

ПУБЛИЧНО-ПРАВОВЫЕ НАУКИ / PUBLIC-LEGAL DISCIPLINES

Редактор рубрики З. У. Гасанов / Rubric editor Z. U. Gasanov

Научная статья



УДК / UDC 341:004

<https://doi.org/10.21202/2782-2923.2026.1.207-225>

Л. В. Терентьева¹

¹ Московский государственный юридический университет имени О. Е. Кутафина (МГЮА), г. Москва, Россия

Трансформация территориальной парадигмы юрисдикции в условиях цифровизации

Терентьева Людмила Вячеславовна, доктор юридических наук, доцент, Московский государственный юридический университет имени О. Е. Кутафина (МГЮА)

E-mail: terentevamila@mail.ru

ORCID: 0000-0002-7152-7454

Web of Science Researcher ID: V-1213-2019

eLIBRARY SPIN-код: 5312-6101

Аннотация

Цель: разработка новых подходов к трансформации территориальной парадигмы юрисдикции в международном публичном и частном праве в условиях цифровизации.

Методы: исследование основано на применении общенаучных методов познания (анализ, синтез, системный подход, моделирование), а также междисциплинарного (конвергентного) подхода, который позволил интегрировать категориальный аппарат международного публичного и частного права.

Результаты: доказана невозможность решения коллизионных и юрисдикционных проблем международного частного права в цифровую эпоху без обращения к базовым категориям международного публичного права (суверенитет, территория и др.). Выявлена и раскрыта причинно-следственная связь между экстратерриториальными претензиями одних государств и ответной протекционистской политикой других (законы о локализации данных), что является ключевым импульсом фрагментации («балканизации») киберпространства. Установлено, что в праве происходит переход от жестких территориальных критериев («место исполнения», «место причинения вреда») к гибким оценочным категориям («тесная связь»). Обосновано, что территориальная парадигма не упраздняется, а адаптируется через формирование правовых фикций, «привязывающих» национальные сегменты киберпространства (доменные зоны, инфраструктуру) к государственной территории. Доказана несостоятельность концепции признания киберпространства глобальным общественным достоянием по аналогии с открытым морем в условиях технологической монополии и геополитического соперничества.

Научная новизна: разработан конвергентный подход, позволяющий исследовать трансформацию юрисдикции как единый процесс, затрагивающий и международное публичное, и международное частное право. Обоснована концепция адаптации территориальной парадигмы, которая проявляется не в ее отмене, а в параллельном развитии двух процессов: «заземления» виртуального пространства через правовые фикции и формирования нового «виртуального контура» экстратерриториальной юрисдикции. Доказана определяющая роль государственно-



центричного подхода и политики цифрового суверенитета в противовес модели мультистейкхолдеризма, а также дана новая оценка тенденции установления юрисдикции на основе «тесной связи» в международном частном праве и выявлены ее риски исходя из правовой определенности.

Практическая значимость: результаты исследования могут быть использованы при разработке национальной и международной политики на основе государственно-центричной модели управления Интернетом, а выявленные тенденции (экстратерриториальные претензии, технологическая монополия) могут быть использованы в целях прогнозирования и предотвращения угроз и разработки превентивных мер, заключающихся в формировании политики стратегического управления киберпространством.

Ключевые слова:

публично-правовые науки, суверенитет, экстратерриториальность, киберпространство, территориальная парадигма, мультистейкхолдеризм

Как цитировать статью: Терентьева, Л. В. (2026). Трансформация территориальной парадигмы юрисдикции в условиях цифровизации. *Russian Journal of Economics and Law*, 20(1), 207–225. <https://doi.org/10.21202/2782-2923.2026.1.207-225>

Scientific article

L. V. Terenteva¹

¹ Kutafin Moscow State Law University (MSAL), Moscow, Russia

Transformation of territorial paradigm of a jurisdiction under digitalization

Lyudmila V. Terentyeva, Dr. Sci. (Law), Associate Professor, Kutafin Moscow State Law University (MSAL)

E-mail: terentevamila@mail.ru

ORCID: 0000-0002-7152-7454

Web of Science Researcher ID: V-1213-2019

eLIBRARY SPIN-code: 5312-6101

Abstract

Objective: to develop new approaches to the transformation of the territorial paradigm of jurisdiction in international public and private law under digitalization.

Methods: the research is based on general scientific methods of cognition (analysis, synthesis, system approach, modeling), as well as an interdisciplinary (convergent) approach, which allowed integrating the categorical apparatus of international public and private law.

Results: the study proved that it is impossible to solve conflict-of-laws and jurisdictional problems of private international law in the digital age without referring to the basic categories of public international law (sovereignty, territory, etc.). The author identified and disclosed a causal relationship between the extraterritorial claims of some states and the retaliatory protectionist policies of others (data localization laws), which is a key impetus for the cyberspace fragmentation (“Balkanization”). It is established that law faces a transition from rigid territorial criteria (“place of execution”, “place of harm”) to flexible assessment categories (“close connection”). The research proved that the territorial paradigm is not abolished, but is adapted by forming legal fictions that “bind” national segments of cyberspace (domain zones, infrastructure) to a state territory. The author showed the inconsistency of recognizing cyberspace as a global public domain similar to the open sea under technological monopoly and geopolitical rivalry.

Scientific novelty: a convergent approach was developed that allows studying the jurisdiction transformation as a consolidated process affecting both public and private international law. The concept of adapting the territorial paradigm was substantiated, which manifests itself not in its abolition, but in the parallel development of two processes: the “grounding” of virtual space through legal fictions and the formation of a new “virtual contour” of extraterritorial jurisdiction. The author proves the decisive role of the state-centric approach and the policy of digital sovereignty as opposed to the model of multistakeholderism. The study also provides a new assessment of the trend of establishing jurisdiction based on “close connection” in private international law and identifies its risks based on legal certainty.

Practical significance: the research results can be used to develop national and international policies based on a state-centered Internet management model; the identified trends (extraterritorial claims, technological monopoly) can be used to predict and prevent threats and develop preventive measures aimed at shaping strategic cyberspace management policies.

Keywords:

public-legal disciplines, sovereignty, extraterritoriality, cyberspace, territorial paradigm, multistakeholderism

For citation: Terenteva, L. V. (2026). Transformation of territorial paradigm of a jurisdiction under digitalization. *Russian Journal of Economics and Law*, 20(1), 207–225. (In Russ.). <https://doi.org/10.21202/2782-2923.2026.1.207-225>

Введение

В начале XXI в. цифровизация стала цивилизационной основой, кардинально трансформировав организацию жизни общества – от политики и экономики до личных отношений. Во многих работах подчеркивается ее непрерывный и незавершаемый характер как системообразующего процесса, представляющего собой механизм внедрения цифровых технологий и платформ во все сферы общественной жизни, что ведет к их технологическому преобразованию.

Казалось бы, процесс технологической трансформации, предполагающий перманентное внедрение инноваций, не может быть прекращен, как не может быть остановлена эволюция общества. Однако это утверждение верно лишь в том случае, если цифровизация несет в себе позитивные смыслы: повышение уровня жизни, комфорт, безопасность. Если же начнут доминировать рискогенные факторы, представляющие угрозу для человека и общества проблемы экономического, социального, этического и психологического характера, нельзя исключать и возможный полный переход к аналоговому укладу жизни.

Однако на сегодняшний момент вопрос принудительного перехода к полностью нецифровому миру в повестке дня не стоит. В этой связи на правовую науку возлагается важная миссия по прогнозированию появления неблагоприятных факторов цифровизации и исключительная задача по разработке адаптивных регуляторных средств для их нейтрализации. Это необходимо для того, чтобы технологии эффективно служили обществу и не выходили из-под контроля.

Ввиду постоянной эволюции цифровизации вопрос о жизнеспособности сложившихся правовых традиций в условиях технологических изменений остается неизменно актуальным. Его острота обусловлена также необходимостью сохранения баланса, диалектического единства между традиционными устоями права, обеспечивающими преемственность и стабильность, и новациями, призванными гарантировать технологический, социальный и экономический прогресс.

Если говорить о традициях науки международного частного права, то ключевая проблема в контексте цифровизации заключается в определенном противоречии между территориальным характером базовых для этой отрасли категорий – коллизионных и юрисдикционных привязок – и внетерриториальной, виртуальной природой киберпространства. Юрисдикционные привязки, закрепленные в основаниях установления международной судебной юрисдикции, позволяют решить проблему выбора надлежащего суда для разрешения спора, вытекающего из трансграничного частноправового отношения. Коллизионные привязки, являясь структурной частью коллизионной нормы, указывают на право, подлежащее применению к частноправовым отношениям, осложненным иностранным элементом. Важно отметить, что формулы прикрепления, лежащие в основе коллизионной привязки, равно как и основания установления международной судебной юрисдикции, изначально пространственно ориентированы.

Так, поиск применимого права осуществляется на основе таких формул прикрепления, как место причинения вреда; место наступления вредоносных последствий; место жительства или основное место деятельности стороны, которая осуществляет исполнение, имеющее решающее значение для содержания договора; право страны места совершения сделки и т. п. Основания подсудности (юрисдикционные привязки) формулируются по схожему принципу: место нахождения ответчика/истца; место исполнения договора; место причинения вреда или наступления вреда и т. п.

Тем не менее применение данных понятий к правоотношениям, реализуемым в цифровой среде, связано со значительными сложностями. Ключевая проблема заключается в определении *locus actus* (места совершения действия) в условиях, когда субъекты рассредоточены в пространстве. Возникает вопрос, какое из мест следует считать юридически значимым: территорию, на которой offerent получил акцепт, страну регистрации его предприятия, юрисдикцию нахождения административного центра или место фактического осуществления деловой активности?

Особую актуальность эта дилемма приобретает применительно к деятельности, осуществляемой исключительно в сети Интернет. В подобных случаях возникает правовая неопределенность: каким образом установить юрисдикцию, в пределах которой эта деятельность считается совершенной, и допустимо ли в принципе отнесение сегментов киберпространства к территории какого-либо государства. Еще в 2014 г. британский ученый А. Миллс (2014) в своем исследовании, посвященном вопросам юрисдикции в международном праве, отметил, что «виртуальное присутствие» участников оборота в цифровой среде требует кардинального пересмотра традиционных оснований для установления юрисдикции (Mills, 2014). Но, несмотря на относительную давность постановки указанной проблемы, она до сих пор не получила своего решения.

Противопоставление пространственной природы классических юрисдикционных и коллизионных привязок внетерриториальному характеру цифровой среды порождает комплекс вопросов, требующих разрешения прежде всего в сфере публичного права. Ключ к их решению лежит в области международного публичного и конституционного права, чей категориальный аппарат («юрисдикция», «территория государства») формирует основу для любого правового регулирования. Как точно отметил нидерландский ученый А. Лоддер, применение закона возможно лишь после определения юрисдикции; а если юрисдикция территориальна, то необходимо установить связь между событиями в киберпространстве и конкретной страной, пользователем или компьютером (Lodder, 2013).

Постановка указанных проблем не является новой и освещается в доктрине по сей день (Mueller, 2020; Ryngaert, 2023; Ruohonen, 2021; Sharma, 2025)¹. Однако адекватного решения данная проблема до сих пор не получила.

В этой связи в настоящей статье поставлена цель выявления адаптивных механизмов установления юрисдикции (как в международном публичном, так и в частном праве) в условиях противоречия между территориальным характером государственного суверенитета и внетерриториальной природой киберпространства цифровизации.

Достижение поставленной цели предполагает последовательное решение ряда важных исследовательских задач:

- интегрировать категориальный аппарат международного публичного права (суверенитет, территория, юрисдикция) и международного частного права (коллизионные и юрисдикционные привязки) для комплексного анализа регулирования отношений в киберпространстве;
- выявить многоуровневую структуру киберпространства (физический, логический, социальный уровни) в целях оценки приемлемости распространения суверенитета и юрисдикции государства в отношении каждого уровня;
- оценить модели управления Интернетом (мультистейкхолдеризм и государственно-центричный подход) и их влияние на установление юрисдикции;
- исследовать эволюцию классических территориальных принципов в сторону гибких критериев («тесная связь») в национальном законодательстве и судебной практике, а также выявить связанные с этим риски правовой неопределенности;
- сформулировать правовые фикции, позволяющие «заземлить» виртуальное пространство путем привязки национальных сегментов киберпространства (доменных зон, инфраструктуры) к государственной территории;

¹ Mueller, M. Sovereignty and Cyberspace: Institutions and Internet governance (under review by Regulation and Governance). Internet Governance Forum. <https://www.intgovforum.org/sites/default/files/webform/week13-cyberspace-sovereignty.pdf>; Mueller, M. (2021). Digital sovereignty: What does it mean? Internet Governance Project. <https://www.internetgovernance.org/wp-content/uploads/Digital-sovereignty-IGF2021.pdf>

– сформулировать прогностические выводы о будущем территориальной парадигмы юрисдикции, определив, что она не отменяется, но диалектически адаптируется через параллельное развитие «заземляющих» фикций и нового «виртуального контура» экстратерриториальной юрисдикции.

Результаты исследования

Конвергентный подход

Цифровая трансформация стала универсальным вызовом для всей правовой системы, что породило тезис о стирании границ между отраслями права, высказанный, в частности, Э. В. Талапиной (2018). По мнению автора, поскольку информация и технологии пронизывают каждую отрасль, они, становясь общим знаменателем, определяют единую логику права, что снижает ценность отраслевого деления (Талапина, 2018).

Подобный взгляд, однако, представляется излишне категоричным. В условиях цифровизации скорее наблюдается подвижность границ между отраслями права при сохранении значимости отраслевого деления, основанного на комбинированном использовании предмета и метода. Постановка новых общих вопросов обуславливает необходимость разработки и применения конвергентного подхода, при котором одновременно используются ресурсы различных отраслей права или происходит последовательное обращение к знаниям, представленным в каждой из релевантных отраслей правоведения.

Таким образом, наблюдаемый процесс отражает не упадок отраслевой системы, а ее качественную эволюцию, выраженную во взаимовлиянии и взаимосвязи отраслей права.

Так, пространственная ориентированность юрисдикционных и коллизионных привязок и внетерриториальность цифровой среды обуславливают необходимость исследования, как государственный суверенитет в его территориально обусловленном измерении реализуется в условиях информационно-коммуникационных процессов. По справедливому замечанию А. Миллса, юрисдикция, традиционно рассматриваемая в международном праве как атрибут государственной власти, выполняет важную функцию определения, при каких обстоятельствах конкретное лицо или событие оказывается в сфере действия национального правопорядка, что является весьма значимым вопросом и для смежной дисциплины международного частного права (Mills, 2014). В этом контексте категории «юрисдикция государства» и «территория государства» выступают в качестве системообразующих для определения пространственных пределов действия как норм о подсудности, так и коллизионных норм.

Следовательно, обращение к концептуальному аппарату международного публичного права становится необходимой предпосылкой для корректного разрешения вопросов международного частного права в цифровую эпоху. Без данного фундамента публично-правового анализа любая попытка построить последовательную коллизионную или юрисдикционную модель в киберпространстве оказывается несостоятельной.

Киберпространство и государственный суверенитет: дискуссия о территории

В системе международного публичного права такие категории, как юрисдикция и суверенитет, изначально обладают пространственной, территориальной природой. Это качество породило множество дискуссий, в рамках которых нередко высказываются спекулятивные суждения о неприменимости или утрате актуальности этих классических правовых конструкций в условиях внетерриториального киберпространства.

Трудности объективирования киберпространства физическими параметрами способствовали появлению тезисов о неэффективности географической территориальности в международном праве и ослаблении государственных границ (Ансельмо, 2006; Benyekhlef & Gelinas, 2009; Kobrin, 1997)²; о существенном изменении понятия «территория» и отсутствии совпадения границ государств с границами реализации их власти (Adams & Albakajai, 2016; Matusitz, 2014; Стрельцов, 2017); о невозможности территориальных суверенов управлять киберпространством, для которого должна быть создана своя юрисдикция (или несколько юрисдикций) (Johnson, 1996). Высказывались и предположения о необходимости создания правовой системы, основанной

² Малахов, В. С. (2007). Государство в условиях глобализации: учебное пособие. Москва: Книжный дом Университет. EDN: UXPEFR

на саморегуляции ввиду невозможности осуществления суверенной власти в не имеющем границ киберпространстве (Johnson, 1996; Самарин, 2016).

В современных публикациях 2020-х гг. воспроизводятся похожие тезисы. Так, в работах американского профессора М. Мюллера, сферой исследования которого среди прочих являются также правовые вопросы управления в сети Интернет, отмечено, что идеи о возможности установления территориального суверенитета в условиях цифровых технологий являются весьма упрощенными. Обосновывает автор указанный тезис несоответствием между территорией и управлением, заложенным в структуру Интернета, а именно транснациональным характером организаций, вовлеченных в процесс управления Интернетом (Рабочая группа разработчиков Интернета (IETF), ICANN), и технологической взаимозависимостью инфраструктуры Интернета – стандартов, адресов, доменов, маршрутизаторов (Mueller, 2020)³.

Другие зарубежные ученые: С. Рингаерт (Ryngaert, 2023), С. Шарма (Sharma, 2025), Ю. Рухонен (Ruohonen, 2021) также отметили слабое согласование теоретической концепции суверенитета с цифровой средой и поставили вопрос о необходимости дальнейшей разработки новых теоретических моделей суверенитета.

Примечательно, что идеи о необходимости отнесения киберпространства к территориям с международным режимом, а именно к географическим пространствам, лежащим за пределами территории государств и находящимся в общем пользовании всего человечества, всех государств (Антарктика, космическое пространство, небесные тела, моря за пределами территориальных вод), которые были предложены Д. Ментэ (Menthe, 1998) более 20 лет назад, обрели новое звучание в современных теоретических дискуссиях о правовом регулировании отношений в киберпространстве.

В частности, М. Мюллер обосновывает необходимость признания киберпространства глобальным общественным достоянием, исходя из тезиса о несовместимости классического территориального суверенитета с природой цифровой среды (Mueller, 2020)⁴. Свою позицию автор подкрепляет историко-правовыми аналогиями, а именно существованием пространств, изъятых из-под национального суверенитета. К ним относятся, во-первых, режим открытого моря, сложившийся еще в XVII в., а во-вторых – космическое пространство, включая Луну и небесные тела, которые, в соответствии со статьей II Договора по космосу 1967 г.⁵, не подлежат национальному присвоению.

По мнению М. Мюллера, применение к киберпространству модели общественного достояния обусловлено следующими ключевыми аргументами:

- любые границы в цифровой среде носят прежде всего технологический и договорный характер, определяясь протоколами и программным кодом, а не географией;
- физическая привязка инфраструктуры (серверов, кабелей) к территории конкретного государства не дает автоматических оснований для распространения на все киберпространство принципов территориального суверенитета в их традиционном понимании;
- установление суверенитета неэффективно в отношении глобальной, динамичной и децентрализованной сети (Mueller, 2020)⁶.

Следует отметить, что в условиях современного внешнеполитического курса США, характеризующегося как попытками силовой смены законной власти в Венесуэле, так и обсуждением возможности присоединения Гренландии, попытки формирования международного консенсуса в отношении признания киберпространства глобальным общественным достоянием не имеют успешных перспектив.

Данная проблема усугубляется технологической монополией: ключевые элементы инфраструктуры и управления глобальной сетью сосредоточены под юрисдикцией США и контролем американских корпо-

³ Mueller, M. Sovereignty and Cyberspace: Institutions and Internet governance (under review by Regulation and Governance). <https://www.intgovforum.org/sites/default/files/webform/week13-cyberspace-sovereignty.pdf>; Mueller, M. Digital sovereignty: What does it mean? Internet Governance Project. <https://www.internetgovernance.org/wp-content/uploads/Digital-sovereignty-IGF2021.pdf>

⁴ Там же.

⁵ ООН. (1966, 19 декабря). Договор о принципах деятельности государств по исследованию и использованию космического пространства, включая Луну и другие небесные тела. https://www.un.org/ru/documents/decl_conv/conventions/outer_space_governing.shtml

⁶ Mueller, M. Sovereignty and Cyberspace: Institutions and Internet governance (under review by Regulation and Governance). <https://www.intgovforum.org/sites/default/files/webform/week13-cyberspace-sovereignty.pdf>; Mueller, M. Digital sovereignty: What does it mean? Internet Governance Project. <https://www.internetgovernance.org/wp-content/uploads/Digital-sovereignty-IGF2021.pdf>

раций. Совокупность этих факторов: применение инструментов гибридной войны, демонстрация амбиций в отношении суверенных территорий и концентрация стратегического технологического ресурса – ставит под сомнение саму возможность проведения правовой аналогии между киберпространством и территориями с международным режимом, такими как открытое море или космос.

Дополнительной причиной несостоятельности данной концепции видится существенное отличие в правовой природе отношений. Если режим международных пространств регулируется преимущественно нормами публичного права через межгосударственные соглашения, то киберпространство представляет собой комплексную среду, где одновременно осуществляются как публично-правовые, так и частноправовые отношения.

В то же время тезис М. Мюллера (2020) о конфликте между географией инфраструктуры и классическим суверенитетом является отчасти справедливым. Автор верно обозначает проблему, однако преувеличивает невозможность ее решения путем установления территориального суверенитета в отношении определенной части физической инфраструктуры киберпространства. Как представляется, здесь автором не учитываются целенаправленные усилия государств по развитию технологических и регуляторных механизмов для утверждения своей юрисдикции в цифровой сфере.

Киберпространство представляет собой многоуровневую структуру, интегрирующую логический (виртуальный), физический и социальный уровни. Его материальную основу составляет программно-техническая инфраструктура: телекоммуникационные сети, компьютерные системы, серверы, маршрутизаторы, процессоры, спутники, коммутаторы и кабели. Определение юрисдикции государства над техническими компонентами этой инфраструктуры, физически расположенными на его территории, не вызывает правовых затруднений и осуществляется на основе принципа территориального суверенитета.

Но в то же время проблемы могут быть обнаружены в том, что существенная часть физической инфраструктуры киберпространства имеет транснациональный характер. Так, например, подводные кабели, отвечающие за передачу более 95 % трафика, проходят через территории с международным режимом. Принимая во внимание, что зачастую данные кабели находятся во владении частных корпораций, государства ограничены в осуществлении контроля над ними (Pierucci, 2025).

Основными производителями сетевых компонентов, встраиваемых технологий и сопутствующих услуг для подводных кабелей являются американские фирмы, которые также финансируют строительство новых подводных кабелей, соединяющих все регионы мира. Как отмечено в Стратегии цифровой политики и международного киберпространства США, опубликованной 6 мая 2024 г., Правительство США оказывает поддержку американским и другим поставщикам в установке, эксплуатации, техническом обслуживании и ремонте защищенной инфраструктуры. Также с 2021 г. Государственный департамент США реализует программу по прокладке кабелей на территории Восточной Европы, стран Азиатско-Тихоокеанского региона, Юго-Востока, где используются американские технологии, что говорит о серьезном уровне контроля США в отношении прокладки и эксплуатации подводной кабельной связи⁷.

Логический (виртуальный) уровень представлен операционными системами, стандартами передачи данных, аппаратными приложениями, программным обеспечением, позволяющими передавать данные между частями его физической инфраструктуры.

Что касается социального уровня, где, собственно, и реализуется коммуникация, то здесь у киберпространства, действительно, границы весьма условны.

Таким образом, правовая природа киберпространства раскрывается в диалектическом противоречии. С одной стороны, его физический уровень (географически локализованные серверы, кабели) остается в сфере действия принципа государственной территориальной юрисдикции. С другой – логический (протоколы, программное обеспечение) и социальный (коммуникационный) уровни демонстрируют принципиальную внетерриториальность, что формирует широкий спектр теоретических подходов: от радикальных тезисов о невозможности установления суверенитета до концепций признания киберпространства глобальным общественным достоянием по аналогии с открытым морем или космосом.

⁷ U.S. Department of State. (2024). The United States International Cyberspace & Digital Policy Strategy. https://www.state.gov/wp-content/uploads/2024/07/United-States-International-Cyberspace-and-Digital-Strategy-FINAL-2024-05-15_508v03-Section-508-Accessible-7.18.2024.pdf

Экстратерриториальная юрисдикция в цифровую эру

Условность границ в киберпространстве имеет серьезные последствия, главное из которых – несанкционированное расширение сферы применения законов одного государства в отношении другого. Речь идет в первую очередь о законах публично-правового характера, что свидетельствует о расширении экстратерриториальной юрисдикции одного государства в отношении другого, реализуемой без санкции последнего государства.

Классическим примером служит дело *Yahoo! Inc. v. La Ligue Contre Le Racisme et L'Antisémitisme*, где доступность информации в сети Интернет послужила основанием для принятия юрисдикции французским судом. Истцы – Союз еврейских студентов Франции (*UEJF*) и Лига против расизма и антисемитизма (*LICRA*) – обратились во французский суд с иском к американской компании *Yahoo*, зарегистрированной по законам штата Делавэр. Союз еврейских студентов Франции (*UEJF*) и Лига против расизма и антисемитизма (*LICRA*) потребовали заблокировать доступ французским пользователям к информации о продаже предметов с нацистской символикой и снять с торгов фашистскую атрибутику. В соответствии со ст. R645-1 французского Уголовного кодекса запрещается продажа, обмен или демонстрация нацистских материалов и иных объектов⁸. При этом ст. 113-7 французского Уголовного кодекса позволяет распространять уголовный закон на преступления, совершенные за пределами французской территории любым иностранным гражданином, если пострадавшим лицом является гражданин Франции. Компания *Yahoo* возражала против юрисдикции французского суда, поскольку действия совершались на территории США, а изображения хранились на американских серверах. Суд, однако, счел, что доступность сайта во Франции достаточна для установления юрисдикции.

Многие государства, включая Россию, в ответ на такие вызовы приняли законы, направленные на блокировку негативных последствий деятельности в киберпространстве. В частности, в РФ был принят комплекс законов, которые часто называют обобщенно законами о локализации данных. Так, ФЗ РФ № 152-ФЗ «О персональных данных» 2006 г.⁹ и ФЗ РФ № 126 «О связи» 2002 г.¹⁰ вводят обязанность крупных компаний в сфере информационных технологий (в том числе иностранных) хранить на серверах в России не только данные профилей пользователей, но и всю историю их переписки, звонков, публикаций. ФЗ РФ № 149-ФЗ «Об информации, информационных технологиях и защите информации» 2006 г.¹¹ предусматривает возможность ограничения доступа к информации, распространяемой с нарушением закона.

Однако это не решило проблему экстратерриториального распространения юрисдикции. Следует отметить определенную семантическую неустойчивость понятий «территориальность» и «экстратерриториальность». Как верно отметил нидерландский профессор С. Рингаерт, то, что одно государство считает территориальным проявлением юрисдикции, другое может расценить как экстратерриториальное (Ryngaert, 2016, 2023).

Экстратерриториальная юрисдикция не является принципиально новым феноменом. Тенденция к ее расширению сложилась преимущественно в США, которые играют ведущую роль в распространении своего законодательства за пределы государства. Стоило США сделать первый шаг по распространению своей экстерриториальной юрисдикции, другие страны (Франция, Германия, Великобритания) также включились в соответствующий процесс *me too* (Parrish, 2009). Сейчас этот процесс продолжается, особенно в эпоху введения односторонних ограничений против физических и юридических лиц из других стран (например, России, Ирана, КНДР).

Один из первых экстерриториальных законов США – «Антимонопольный закон» – Закон Шермана (или Акт Шермана)¹², принятый в 1890 г. В соответствии с п. 3 пар. 8 ст. 1 Конституции США, Конгресс США имеет право принимать законы, имеющие сферу действия за пределами территориальных границ Соединенных Штатов¹³.

⁸ Penal Code (France) (по состоянию на июль 2025). <https://www.wipo.int/wipolex/en/legislation/details/23309>

⁹ О персональных данных. № 152-ФЗ от 27.07.2006 (последняя редакция). КонсультантПлюс. https://www.consultant.ru/document/cons_doc_LAW_61801/

¹⁰ О связи. № 126-ФЗ от 07.07.2003 (последняя редакция). КонсультантПлюс. https://www.consultant.ru/document/cons_doc_LAW_43224/

¹¹ Об информации, информационных технологиях и о защите информации. № 149-ФЗ от 27.07.2006 (последняя редакция). КонсультантПлюс. https://www.consultant.ru/document/cons_doc_LAW_61798/

¹² Sherman Antitrust Act, 15 U.S.C. <https://www.law.cornell.edu/uscode/text/15/chapter-1>

¹³ The Constitution of the United States. <https://constitutionus.com/>

В цифровую эпоху, когда существенным образом упростились механизмы трансграничной передачи данных, список экстра TERRИТОРИАЛЬНЫХ американских законов пополнил «Акт, разъясняющий законный доступ к данным, находящимся за рубежом (Облачный акт)» 2018 г.¹⁴ Предыстория принятия данного акта началась с постановления суда Манхэттена по делу *Microsoft Corp. v. United States Department of Justice*, в котором суд, руководствуясь Законом 1986 г. «О конфиденциальности электронной связи» (*Electronic Communication Privacy Act*), обязал компанию «Майкрософт» предоставить свободный доступ к данным электронной почты правоохранительным органам США в любых частях планеты независимо от того, находятся ли они под американской юрисдикцией или нет¹⁵. В частности, власти потребовали от «Майкрософта» передать сообщения, хранящиеся в ирландском дата-центре, следователям из американских правоохранительных органов. В апелляции, поданной в Окружной суд Нью-Йорка, компания «Майкрософт» выступила против ордера на разглашение данных, поскольку судебное постановление нарушает суверенитет Ирландии в силу того, что запрашиваемые данные находятся в Дублине и, соответственно, американский суд не имеет юрисдикции над информацией в других странах.

Судьи Верховного суда США высказались о невозможности экстра TERRИТОРИАЛЬНОГО доступа к данным в силу того, что Закон 1986 г. «О конфиденциальности электронной связи» не распространялся на данные, находящиеся за пределами США. В феврале 2018 г. в Конгресс был представлен «Акт, разъясняющий законный доступ к данным, находящимся за рубежом» (далее – Облачный акт), а в марте этого же года он был подписан президентом США Д. Трампом.

Облачный акт предусматривает доступ правоохранительных органов США к данным интернет-пользователей за рубежом и допускает возможность заключения двухсторонних соглашений с иностранными государствами, позволяя их правоохранительным органам напрямую запрашивать данные у американских компаний, минуя традиционные механизмы договоров о взаимной правовой помощи. В соответствии с п. 2713 данного Акта провайдеры услуг электронной связи или провайдеры удаленного вычислительного обслуживания обязаны сохранять, осуществлять резервное копирование, раскрывать содержание беспроводной или электронной коммуникации, а также любую запись или иную информацию клиента или абонента провайдера независимо от того, находится ли такая коммуникация, запись или другая информация в пределах или за пределами Соединенных Штатов¹⁶. Правоохранительные органы США могут направить запрос на получение данных интернет-пользователей, которые хранятся за пределами американской юрисдикции, в связи с проводимым расследованием. Запрос направляется непосредственно в компанию, обладающую такой информацией, которая вне зависимости от того, где она находится, обязана предоставить по запросу соответствующую информацию. При этом запрет передачи данных местонахождения этих компаний законодательством не может являться единственным основанием для непредоставления данных американским властям.

Основную тревогу Облачный акт вызывает в тех юрисдикциях, преимущественно это страны Европы и Северной Америки, где широко используются услуги крупных облачных провайдеров, инкорпорированных в США. Так, например, в противоречие с Облачным актом вступает ст. 48 Регламента Европейского Парламента и Совета ЕС 2016 г. о защите физических лиц при обработке персональных данных и о свободном обращении таких данных, а также об отмене Директивы 95/46/ЕС (далее – Регламент)¹⁷, которая предусматривает, что передача или раскрытие персональных данных может осуществляться, только если они основаны на международном соглашении, таком как договор о взаимной правовой помощи, действующий между запрашивающей третьей страной и Евросоюзом. Облачный закон, таким образом, серьезно подрывает требования Регламента, позволяя США потенциально получить доступ к данным, которые хранятся на европейской территории или поступают от европейских граждан и компаний, при условии, что эти данные управляются поставщиком в соответствии с американским законодательством.

В Стратегии цифровой политики и международного киберпространства США 2024 г. также была обозначена проблема напряженности в отношениях с торговыми партнерами США относительно облачных сервисов

¹⁴ H.R.4943 – 115th Congress (2017–2018). <https://www.congress.gov/bill/115th-congress/house-bill/4943/text>

¹⁵ In Re Warrant to Search a Certain Email Account Controlled & Maintained by Microsoft Corp., 15 F. Supp. 3d 466 (S.D.N.Y. 2014). (Harvard Law Review, 2015, 128(3), 1019–26).

¹⁶ H.R.4943 – 115th Congress (2017–2018). <https://www.congress.gov/bill/115th-congress/house-bill/4943/text>

¹⁷ General Data Protection Regulation (GDPR). GDPR Archives. GDPR.eu

и центров обработки данных, вылившаяся в то, что ряд партнеров США пригрозили исключить американских облачных провайдеров со своих рынков из-за опасений по поводу доступа к данным и контроля над ними¹⁸. Как указано в Стратегии, Государственный департамент США стремится достичь общего понимания со своими международными партнерами в отношении справедливого и безопасного использования облачных ресурсов. С этой целью Государственный департамент совместно с Министерством юстиции работает над разъяснением законности применения Облачного акта в отношении данных, находящихся за рубежом, и над заключением двусторонних соглашений в соответствии с этим Актом.

Для стран, предусмотревших обязательную локализацию данных (Россия, Китай), риски, связанные с подобными законами, снижены. В этой связи одним из инструментов против устранения юрисдикционных барьеров в киберпространстве является определенная цифровая изолированность или четкая фрагментация цифрового пространства по линии национальных границ.

В то же время экстратерриториальная сфера действия законов о персональных данных стала общей мировой практикой. В ст. 3 Регламента ЕС раскрываются как территориальная, так и экстратерриториальная сферы его распространения в зависимости от того, учреждены ли контролер или лица, обрабатывающие персональные данные, в Европейском союзе.

В РФ «Закон о персональных данных» 2006 г. применяется к обработке персональных данных граждан РФ, осуществляемой иностранными юридическими лицами или иностранными физическими лицами, на основании договора, стороной которого являются граждане РФ. Китайское законодательство о персональных данных обладает четко выраженным экстратерриториальным действием, которое выражается в защите данных китайских граждан независимо от того, где находится компания, их обрабатывающая (Закон КНР о защите персональной информации 2021 г.)¹⁹.

Таким образом, условные границы киберпространства стали катализатором до сих пор не решенной юрисдикционной проблемы, проявлением которой является экспансия экстратерриториального действия национальных законов. В этом контексте обоснованной представляется позиция, сформулированная в российской правовой доктрине, что при существующем многообразии национальных законодательств и принципиально различных подходов к регулированию сценарий достижения универсальной юрисдикционной модели для киберпространства не имеет реалистичных перспектив (Razmetaeva et al., 2021).

Односторонние претензии на трансграничное применение права одной страны закономерно встречают противодействие в форме ответного законодательства других государств, что ведет к эскалации правовых конфликтов и фрагментации цифровой среды, подтверждая точное наблюдение М. Мюллера (Mueller, 2020) о «мести» глобализма сети, когда суверенные государства пытаются ее уничтожить²⁰.

Попытка разрешить фундаментальное противоречие между трансграничной природой сети и территориальным характером суверенитета через экстратерриториальное расширение законов не решает проблему, а лишь переводит ее в новую плоскость, а именно к поиску баланса между экстратерриториальностью и четкой фрагментацией цифрового пространства по линии национальных границ.

Переосмысление понятия «территория»

Тенденция расширения экстратерриториальной юрисдикции в условиях цифровизации ставит вопрос о допустимых пределах ее распространения. Оправданной в этой связи представляется позиция, согласно которой современное международное право функционирует на основе устаревшей пространственной па-

¹⁸ U.S. Department of State. (2024). The United States International Cyberspace & Digital Policy Strategy. https://www.state.gov/wp-content/uploads/2024/07/United-States-International-Cyberspace-and-Digital-Strategy-FINAL-2024-05-15_508v03-Section-508-Accessible-7.18.2024.pdf

¹⁹ Всекитайское собрание народных представителей. <http://www.npc.gov.cn/npc/c30834/202108/a8c4e3672c74491a80b53a172bb753fe.shtml>

²⁰ Mueller, M. Sovereignty and Cyberspace: Institutions and Internet governance (under review by Regulation and Governance). Internet Governance Forum. <https://www.intgovforum.org/sites/default/files/webform/week13-cyberspace-sovereignty.pdf>; Mueller, M. Digital sovereignty: What does it mean? Internet Governance Project. <https://www.internetgovernance.org/wp-content/uploads/Digital-sovereignty-IGF2021.pdf>

радикалы (Lithgoe, 2024). Однако говорить о «конце территории государства» преждевременно, поскольку физическая территория сохраняет свое фундаментальное правовое значение.

В то же время признание данного факта не отменяет озвученные проблемы, поставленные перед международным правом в отношении необходимости дополнительной организации пространства как основы, построенной вокруг стабильных, фиксированных единиц государственной территории, «над которыми» осуществляется суверенитет.

Когда речь идет о территории государства, подразумевается не абстрактная географическая единица, а пространство, в отношении которого устанавливается государственный суверенитет.

В соответствии с ч. 1 ст. 67 Конституции РФ под территорией понимается территория субъектов РФ, внутренние воды и территориальное море, воздушное пространство над ними. В ст. 4 Конституции говорится, что суверенитет РФ распространяется на всю территорию. Таким образом, установление суверенитета государства в отношении информационно-коммуникационного пространства в Конституции РФ не предусмотрено.

Определенная территориализация, или «заземление», киберпространства может быть усмотрена в российских нормативных актах. Так, в Приказе Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 29 июля 2019 г. № 216 предложена концепция доменных имен, входящих в российскую, национальную, доменную зону: (а) домен верхнего уровня .RU; б) домен верхнего уровня .RF; в) домен верхнего уровня .SU; г) иные домены верхнего уровня, управление которыми осуществляется зарегистрированными на территории РФ юридическими лицами, являющимися зарегистрированными владельцами баз данных указанных доменов в международных организациях распределения сетевых адресов и доменных имен²¹.

В судебной практике также определенным сегментам киберпространства придается значение территории.

В соответствии с п. 19 Постановления Пленума Верховного Суда РФ от 27 июня 2017 г. № 23 «О рассмотрении арбитражными судами дел по экономическим спорам, возникающим из отношений, осложненных иностранным элементом», при применении п. 9 ч. 1 ст. 247 АПК РФ под спорами, возникшими из отношений, связанных с государственной регистрацией имен и других объектов и оказанием услуг в международной ассоциации информационно-телекоммуникационной сети Интернет на территории Российской Федерации, следует понимать в том числе споры, связанные с защитой прав на результаты интеллектуальной деятельности и средства индивидуализации юридических лиц, осуществляющих предпринимательскую и иную экономическую деятельность, товаров, работ, услуг и предприятий, использованные при регистрации доменных имен в российской доменной зоне (национальные домены первого уровня и доменные зоны второго уровня, ориентированные на российскую аудиторию либо включающие сайты на кириллице), а если регистрация осуществлена на территории Российской Федерации (регистратором выступает российское лицо), то и в иных доменных зонах.

Возможность дальнейшего переосмысления содержания понятия «территория» в доктрине международного публичного права обусловлена тем, что по мере исторического развития содержание данного понятия не являлось статичным. В результате воздействия политических, экономических, географических, а также технологических факторов понимание территории эволюционировало. Еще в начале XX в. определение территории ограничивали исключительно земной поверхностью. Территорию как «пространство земли и воды, подчиненное исключительно верховной власти государства», определял Ф. Ф. Мартенс²².

На последующих этапах пространственной динамики территория государства стала охватывать воздушное пространство, пространство континентального шельфа, а также пространства, которые достаточно трудно объективировать. Были определены правовые основания пользования территорий с международным режимом (водные пространства за пределами исключительных экономических зон, Антарктида), со специальным международным режимом на основе международного договора (Антарктика, открытое море, космическое пространство) и т. п. Так, уникальными по своей природе объектами, приравненными по статусу к территории РФ, являются космические объекты. Положение о юрисдикции в международном космическом праве зафик-

²¹ Приказ Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 29 июля 2019 г. № 216. Гарант. <https://base.garant.ru/72626866/>

²² Мартенс, Ф. Ф. (2014). Современное международное право цивилизованных народов. Т. 1. Москва: Зерцало. С. 252.

сировано в Договоре о принципах деятельности государств по исследованию и использованию космического пространства, включая Луну и другие небесные тела 1967 г.²³

В трудах по международному праву правовое значение понятию «территория государства» придается в связи с тем, что территориальные единицы (морские и воздушные суда, территориальное море и посольства) в юридическом контексте означают конкретную сферу правовой компетенции, а не географическую категорию²⁴. Принадлежность территории определенному государству и территориальное верховенство, осуществляемое государством, являются двумя основными признаками государственной территории²⁵. При этом правовое значение понятия «территория государства» заключается в определении границ, в рамках которых реализуются суверенитет и полная юрисдикция государства.

Киберпространство как сфера реализации социальных, экономических и политических отношений не может находиться между рамками суверенитета и юрисдикции государства (Терентьева, 2019). Фактическая реализация в нем общественных отношений не позволяет относить его к утопии, «месту, которого нет».

Таким образом, устойчивая связь национальных сегментов киберпространства (например, национальных доменных зон, инфраструктуры) с территорией государства вполне может быть положена в основу юридической фикции, в рамках которой предполагается включение определенной части киберпространства в содержание понятия «территория».

В то же время проблема юрисдикции в киберпространстве на сегодняшний день получает преимущественно научное осмысление и в международно-правовой повестке не стоит. В связи с чем очерчивание юрисдикционных контуров происходит преимущественно на национальном уровне каждого отдельного государства.

Вызовы децентрализованного управления и новые подходы к юрисдикции

Сложности установления полной юрисдикции государств в отношении киберпространства связаны с децентрализованным принципом управления сети Интернет, в который вовлечены негосударственные национальные организации (Общество Интернета (*Internet Society (ISOC)*), некоммерческая организация по управлению доменными именами и IP-адресами (*ICANN*), Рабочая группа по проектированию Интернета (*Internet Engineering Task Force (IETF)*) и др.

В результате критики со стороны многих государств возможности прямого участия США в управлении киберпространством, которая особенно обострилась в результате скандальных разоблачений Эдварда Сноудена, в октябре 2016 г. технические функции по ведению баз данных (реестра) доменов верхнего уровня структуры, подконтрольной Министерству торговли США IANA (Администрация адресного пространства Интернет), перешли под контроль дочерней организации Корпорации ICANN, публичной некоммерческой корпорации «Публичные технические идентификаторы» (*Public Technical Identifiers (PTI)*). Таким образом, как было обозначено советом директоров ICANN, схема управления глобальной сетью выстраивается в соответствии с принципом мультистейкхолдеризма, а именно с участием всех заинтересованных сторон из разных стран мира (Терентьева, 2019).

Сомнения в успешной реализации такого управления были высказаны в западной научной литературе. Так, М. Мюллером была отмечена неуместность риторики о мультистейкхолдеризме ввиду того, что ключевой особенностью этой модели является не наличие множества заинтересованных сторон, а повышенный статус негосударственного субъекта, который вытесняет суверенное государство (Mueller, 2020)²⁶.

²³ Договор о принципах деятельности государств по исследованию и использованию космического пространства, включая Луну и другие небесные тела (Москва – Вашингтон – Лондон). (1967). Ведомости Верховного Совета СССР, 44. Ст. 588.

²⁴ Броунли, Я. (1977). Международное право (в двух книгах). Кн. 1. Москва: Прогресс. С. 185–187; Лукашук, И. И. (2001). Международное право. Общая часть. Москва: Волтерс Клувер. С. 165–176.

²⁵ Гасанова, К. К., Шалягина, Д. Д. (ред.). (2012). Международное право: учебник. Москва: ЮНИТИ-ДАНА: Закон и право. С. 172.

²⁶ Mueller, M. Sovereignty and Cyberspace: Institutions and Internet governance (under review by Regulation and Governance). Internet Governance Forum. <https://www.intgovforum.org/sites/default/files/webform/week13-cyberspace-sovereignty.pdf>; Mueller, M. Digital sovereignty: What does it mean? Internet Governance Project. <https://www.internetgovernance.org/wp-content/uploads/Digital-sovereignty-IGF2021.pdf>

Следует также отметить, что, несмотря на исключение в 2016 г. прямого участия подконтрольных США организаций в структуре ICANN, компании, осуществляющие ключевые функции по управлению сетью Интернет, находятся в юрисдикции США, что позволяет говорить о сохранении доминирующего положения данного государства в процессе управления.

По всей видимости, именно этим объясняется, что в Стратегии цифровой политики и международного киберпространства США 2024 г. поддерживается модель мультистейкхолдеризма и практически стигматизируются Россия, КНР и другие страны, которые в противовес концепции мультистейкхолдеризма продвигают концепцию глобального управления Интернетом, которая сосредоточена на большем вовлечении государств в процесс управления, не исключая при этом возможность привлечения к участию в управлении других заинтересованных сторон²⁷. Как отмечено в Стратегии, Россия, КНР и другие страны стремятся изменить нормы, регулирующие киберпространство, подрывают техническую основу Интернета и ослабляют ответственность за злонамеренное использование авторитарными странами возможностей киберпространства.

Между тем прошедшая в 2016 г. либерализация в управлении инфраструктурой Интернета не освободила корпорацию от определенной политической ангажированности.

Еще в 2022 г. Международный регулятор в сфере доменных имен и IP-адресов ICANN отказал Украине на запрос ограничить работу российского сегмента Интернета, заявив, что миссия регулятора «...не предполагает применение мер наказания, введение санкций или ограничение доступа к сегментам Интернета»²⁸. Но уже в 2024 г. ICANN сделала отчет обсуждения проекта правил приема заявок на новые домены верхнего уровня (*New gTLD*), согласно которым заявителей обязывают соблюдать санкции США²⁹. Тем самым от участия в новом раунде подачи заявок в 2026 г. может быть отрезан ряд подсанкционных российских компаний.

Следовательно, частные корпорации, находящиеся под юрисдикцией США, фактически обладают полномочиями по установлению правил и политик при осуществлении ключевых функций по управлению инфраструктурой Интернета.

Иллюстрацией данной проблемы служит решение организации *Public Technical Identifiers (PTI)*, ответственной за функции управления по присвоению номеров в Интернете при ICANN, объявившей в марте 2025 г. о поэтапном прекращении работы домена .su (предназначенного для СССР) к 2030 г. Данное решение формально основано на политике ICANN 2022 г. об упразднении национальных доменов верхнего уровня (*ccTLD*) после исключения соответствующей страны из стандарта *ISO 3166-1*³⁰. При этом домен .su, где зарегистрировано около 100 тыс. имен, продолжает функционировать под управлением Российского института развития общественных сетей (РосНИИРОС), который отвергает планы его ликвидации, отмечая отсутствие формальных действий со стороны ICANN³¹. Это создает неопределенность, учитывая, что ICANN ранее, в 2014 г., отказывалась блокировать домены Сирии, Ирана и КНДР, аргументируя это тем, что домены не являются собственностью государств³².

Подобные действия воспринимаются как часть негативной тенденции, отмеченной в п. 53 Стратегии национальной безопасности РФ 2021 г., где указано на стремление транснациональных корпораций закрепить

²⁷ U.S. Department of State. (2024). The United States International Cyberspace & Digital Policy Strategy. https://www.state.gov/wp-content/uploads/2024/07/United-States-International-Cyberspace-and-Digital-Strategy-FINAL-2024-05-15_508v03-Section-508-Accessible-7.18.2024.pdf

²⁸ В марте 2022 г. украинский вице-премьер и министр цифровой трансформации М. Федоров обратился с письмом генеральному директору корпорации ICANN Йорану Марби с просьбой отключить корневые серверы DNS в России и отозвать российские домены, такие как .ru, .rf и .su. Ответное письмо было подготовлено исполнительным советом RIPE NCC – одним из пяти региональных регистраторов, в котором было гарантировано бесперебойное предоставление услуг вне зависимости от внутриполитических споров, международных конфликтов, войн. RIPE NCC Executive Board Resolution on Provision of Critical Services. (2022, March). <https://www.ripe.net/ripe/mail/archives/ripe-list/2022-March/002462.html>

²⁹ Санкции вышли на верхний уровень. (2024, 10 сентября). Коммерсантъ. <https://www.kommersant.ru/doc/7032586?ysclid=mgs2f779vq311122903>

³⁰ ICANN планирует прекратить поддержку домена СССР .su к 2030 году. (2025, 13 марта). Интерфакс. <https://www.interfax.ru/digital/1013441>

³¹ РосНИИРОС заявил об отсутствии оснований для закрытия домена СССР. (2025, 13 марта). РБК. https://www.rbc.ru/technology_and_media/13/03/2025/67d2d9d49a79472dd69757d2

³² Что будет если отключат Интернет по всему миру. <https://fakt.vot-tac.ru/articles/chto-budet-esli-otklyuchat-internet-po-vsemu-miru.html>

свое монопольное положение в сети Интернет и контролировать все информационные ресурсы путем введения такими корпорациями (при отсутствии законных оснований и вопреки нормам международного права) цензуры и блокировки альтернативных интернет-платформ³³.

В ответ на эти вызовы Россия последовательно реализует политику цифрового суверенитета. В 2019 г. был принят так называемый Закон о суверенном Интернете³⁴, предоставивший Роскомнадзору технические средства для управления маршрутизацией трафика и ограничения доступа к запрещенному контенту. Дальнейшим шагом стало Постановление Правительства № 1667 от 27.10.2025³⁵, расширившее полномочия Роскомнадзора, ФСБ и Минцифры по централизованному управлению сетью, включая возможность полной изоляции российского сегмента Интернета в случае экстремальных угроз.

По словам координатора Центра безопасного Интернета У. Парфентьева, полное изолирование российского сегмента киберпространства является лишь технически возможной опцией на случай чрезвычайного масштаба угроз³⁶. Но, как можно заключить из вышеприведенного, ответом на риски, порождаемые децентрализованным управлением и экстратерриториальными претензиями, становится активная территориализация киберпространства со стороны национальных государств. Это ведет к закономерной фрагментации глобальной Сети на национальные сегменты, где в условиях кризиса доступной остается лишь информация, размещенная на внутренних серверах.

Хотя полная изоляция рассматривается как крайняя и экономически болезненная мера против экзистенциальных угроз, текущее регулирование развивается по пути усиленного контроля трафика, блокировок цифровых сервисов и создания автономной инфраструктуры. Постоянное усложнение технологий будет требовать и дальнейшей эволюции правовых механизмов, закрепляющих цифровой суверенитет в условиях глобальной технологической конкуренции.

Таким образом, в информационную эпоху классическая территориальная парадигма не упраздняется, но подвергается глубокой трансформации. Актуальным становится тезис не об исчезновении границ, а о построении дополнительного к территориальному виртуального контура. Цифровые границы выстраиваются по линиям проявления экстратерриториальной юрисдикции государств, в рамках которой возможен контроль над данными и реализация политики технологической зависимости государства, устанавливающего данную юрисдикцию. Как верно отмечено С. Рингаертом, в современную эпоху экстерриториальная правоприменительная юрисдикция больше не регулируется простыми бинарными правилами (разрешено и не разрешено), а становится проблемой, которая требует детальной тщательной контекстуальной оценки.

При этом прямая территориализация киберпространства через изоляцию национального сегмента хотя и является инструментом обеспечения цифрового суверенитета, но включает в себя значительные экономические издержки, что не становится эффективным направлением развития государства. Успешная политика в цифровой сфере заключается не в простом контроле территорий, а в стратегическом управлении киберпространством. Такое управление может заключаться в возможностях продвижения собственных конкурентноспособных приложений и платформ; создании правовых и технических стандартов; формировании цифровых альянсов с дружественными юрисдикциями и т. п.

Тенденции установления судебной юрисдикции в отношении трансграничных споров в условиях цифровизации

Тенденция пространственной трансформации юрисдикции в международном публичном праве отражается и в специфике установления судебной юрисдикции по рассмотрению споров, вытекающих из частно-право-

³³ Указ Президента РФ от 02.07.2021 № 400. (2021). СЗ РФ, 27(ч. II). Ст. 5351. КонсультантПлюс. https://www.consultant.ru/document/cons_doc_LAW_389271/

³⁴ В ноябре 2019 г. были приняты поправки в федеральные законы РФ «О связи» 2003 г. и «Об информации, информационных технологиях и о защите информации» 2006 г., более известные как Закон о суверенном Интернете.

³⁵ Постановление Правительства РФ от 27.10.2025 № 1667. (2025). КонсультантПлюс. https://www.consultant.ru/document/cons_doc_LAW_518235/

³⁶ Это возможно: как и почему в России могут отключить интернет. (2025, 28 ноября). Рамблер/новости. <https://news.rambler.ru/tech/55681996-eto-vozmozhno-kak-i-pochemu-v-rossii-mogut-otklyuchit-internet/>

вых отношений с иностранным элементом. На сегодняшний день различия между традиционными системами международной подсудности, устанавливаемой исходя из специфики того или иного территориального критерия, постепенно нивелируются. Традиционно в науке международного частного права международная подсудность рассматривалась в трехчастной системе: германская, основным принципом которой является определение судебной юрисдикции на основе места жительства ответчика для физических лиц и места нахождения ответчика для юридических лиц; латинская система, где при определении судебной юрисдикции имеет значение гражданство физических лиц или местонахождение органов управления юридических лиц; англо-американская система, принципы установления которой основаны на возможности установления юрисдикции судов при условии, что ответчику было вручено исковое заявление (Англия) и минимальных контактах ответчика со штатом суда (США). Имеющиеся отличия основных систем установления судебной юрисдикции (континентальная, латинская, англо-американская) в ряде случаев нивелируются ввиду того, что свойственное странам общего права гибкое правило тесной связи становится общим знаменателем установления судебной юрисдикции.

Практически во всех юрисдикциях гибкие критерии установления подсудности, в основе которых лежит судебное усмотрение, приобретают первостепенное значение по отношению к жестким территориальным привязкам в виде «место нахождения», «место исполнения», «место причинения вреда» и т. п.

Так, ст. 11 Закона Бельгии о введении в действие Кодекса международного частного права 2004 г. (*Law of 2004 holding the code of Private International law Belgium*) предусматривает возможность установления юрисдикции бельгийских судов, если дело имеет тесную связь с Бельгией и рассмотрение дела за границей представляется невозможным; или когда неразумно требовать рассмотрения дела за границей³⁷. Согласно ст. 3135 Гражданского кодекса Квебека 1991 г. (*Quebec civil code of Quebec 1991*), если какой-либо орган власти Квебека обладает юрисдикцией рассматривать спор, он может в качестве исключения и на основании ходатайства стороны спора отказаться от юрисдикции, если сочтет, что органы власти другого государства лучше подходят для разрешения этого спора. В ст. 3136 Гражданского кодекса Квебека предусмотрено обратное правило, а именно, если орган власти Квебека не обладает юрисдикцией рассматривать спор, он может тем не менее рассмотреть его при условии, что спор имеет достаточную связь с Квебеком, в случае когда разбирательство не может быть проведено за границей или когда неразумно требовать возбуждения такого разбирательства³⁸. В Общем законе о международном частном праве Уругвая 2020 г. (*General law on private international law 2020 Uruguay*) в п. (3) ст. 57 также предусмотрено установление юрисдикции суда республики, если дело имеет соответствующие связи с республикой³⁹.

Ярким примером также являются изменения Гражданского процессуального закона Китая (далее – ГПЗ Китая) 2023 г., которые существенным образом коснулись вопросов установления юрисдикции китайских судов в отношении споров, возникающих из отношений, осложненных иностранным элементом. Так, в 2023 г. впервые было введено новое основание установления юрисдикции – надлежащая связь (*appropriate connection*) между трансграничным спором и территорией Китая. Основание надлежащей связи также используется при решении вопроса о косвенной судебной юрисдикции иностранных судов при решении вопроса о признании и приведении в исполнение иностранных судебных решений (ст. 301 ГПЗ Китая). Таким образом, китайские суды должны решить вопрос о наличии юрисдикции иностранных судов и согласии с ней китайского суда в отношении конкретного спора в целях решения вопроса о признании и приведении в исполнение соответствующего решения иностранного суда (Huang, 2023).

ГПЗ Китая не определяет понятия надлежащей связи (*appropriate connection*), но, как отмечено в китайской доктрине, понятие «надлежащая связь» должно иметь более широкое толкование по сравнению с понятием «тесная связь» (*the closest connection*), которое предусмотрено в китайском законе в связи с применением права к трансграничным отношениям (Huang, 2023).

Тесная связь отмечена в Принципах транснационального гражданского процесса *ALI/UNIDROIT* (2004). Согласно п. 2.1 Принципов, юрисдикция в отношении стороны может быть осуществлена: во-первых, по

³⁷ Плеханов, В. (сост. и ред.). (2021). Международное частное право: сборник национальных кодификаций. Москва. С. 114.

³⁸ Там же. С. 385–386.

³⁹ Там же. С. 898–899.

согласию сторон на передачу спора в арбитраж, во-вторых, когда существует существенная связь между государством суда и стороной или сделкой или событием, являющимся предметом спора⁴⁰.

С одной стороны, гибкие правила в виде тесной связи дают правоприменительным органам возможность оперативного реагирования на изменения, связанные с развитием информационно-коммуникационных процессов. С другой стороны, отсутствие четкого содержания этого понятия повышает риски как необоснованного установления юрисдикции, так и необоснованного отказа в ней.

Отсутствием определенности содержания тесной связи объясняется то, что такое основание установления международной судебной юрисдикции отсутствует в международных договорах с участием РФ.

В этой связи вряд ли можно согласиться, что в международных договорах всегда закрепляются наиболее совершенные правовые конструкции (Бахин, 2002). Создание единых правовых моделей с неизбежностью носит компромиссный характер, учитывающий специфику стран, которые присоединяются к международным договорам. Тогда как задачи по пути достижения компромисса не во всех случаях коррелируют с задачами по выработке наиболее прогрессивных механизмов правового регулирования.

В то же время критерий «существенной связи» предусмотрен в Гаагской конвенции о признании и приведении в исполнение иностранных судебных решений по гражданским и торговым делам 2019 г. (Россия не участвует) в качестве основания косвенной подсудности. Так, одним из условий признания и приведения в исполнение судебного решения является то, что предметом судебного решения является договорное обязательство, и оно вынесено судом государства, в котором исполнение данного обязательства имело место или должно было иметь место в соответствии с (I) соглашением сторон, или (II) правом, применимым к договору, при отсутствии согласованного места исполнения, если только деятельность ответчика в отношении сделки явно не формировала намеренную и существенную связь с данным государством (ст. 5. ч. 1 (g)).

В результате при признании и приведении в исполнение решения суд государства, где испрашивается соответствующее исполнение, будет проверять, имела ли существенную связь деятельность ответчика в отношении сделки с государством, в котором вынесено соответствующее решение. При этом в Конвенции не указано, по какому праву должна быть произведена оценка тесной связи: по праву государства вынесения решения или по праву государства, где испрашивается исполнение.

Заключение

Результаты исследования подтверждают тезис о невозможности решения юрисдикционных и коллизионных проблем в цифровой среде в рамках одной отрасли права. Установлено, что их разрешение наиболее целесообразно в условиях системной интеграции категориального аппарата международного публичного права (суверенитет, территория) и инструментов международного частного права (коллизионные и юрисдикционные привязки).

Анализ многоуровневой структуры киберпространства (физический, логический, социальный уровни) показал диалектический характер его правовой природы: если физическая инфраструктура подпадает под действие традиционного территориального суверенитета, то логический и социальный уровни демонстрируют принципиальную внетерриториальность. Это противоречие опровергает концепции признания киберпространства глобальным общественным достоянием по аналогии с открытым морем, которые игнорируют геополитическую реальность и комплексный характер регулируемых в сети отношений.

Проведенный анализ доказывает, что территориальная парадигма юрисдикции не упраздняется, но подвергается глубокой и диалектической адаптации. Она эволюционирует по двум основным направлениям. Государства формируют юридические конструкции, позволяющие условно «привязать» национальные сегменты киберпространства (национальные доменные зоны, физическую инфраструктуру) к своей территории. Эта тенденция находит выражение в политике цифрового суверенитета и законах о локализации данных. Параллельно наблюдается активное расширение экстратерриториальной юрисдикции, особенно со стороны технологически доминирующих государств, что порождает «виртуальный контур» границ, выстроенный по

⁴⁰ ALI/UNIDROIT Principles of Transnational Civil Procedure. <https://www.unidroit.org/english/principles/civilprocedure/ali-unidroitprinciples-e.pdf>

линиям контроля над данными и возможностью установления технологической зависимости. Данный процесс, в свою очередь, вызывает ответную протекционистскую политику других государств, выступая ключевым драйвером фрагментации («балканизации») глобального киберпространства.

Тенденция пространственной трансформации юрисдикции в международном публичном праве отражается и в специфике установления судебной юрисдикции по рассмотрению споров, вытекающих из частно-правовых отношений с иностранным элементом. В международном частном праве наблюдается тенденция перехода от жестких территориальных критериев подсудности («место исполнения», «место причинения вреда») к гибким оценочным категориям («тесная связь»). Данная тенденция прослеживается в современном национальном законодательстве государств (Бельгия, Квебек, Китай). Однако эта гибкость связана с рисками правовой неопределенности, особенно в условиях семантической неустойчивости самих понятий «территориальности» и «экстратерриториальности», где минимальные связи могут быть расценены судом как существенные.

Установлено, что в условиях технологической монополии и геополитического соперничества определяющей является не модель мультистейкхолдеризма, а государственно-центричный подход к управлению Интернетом. Практическим следствием проведенного исследования является необходимость разработки сбалансированной политики цифрового суверенитета, сочетающей защиту национального сегмента с активным формированием международных цифровых альянсов и продвижением собственных технологических стандартов.

Таким образом, устойчивость территориальной парадигмы в цифровую эпоху подтверждается через ее диалектический синтез. Территориальный принцип установления юрисдикции не утрачивает своего фундаментального значения ввиду расширения содержания понятия «территория», путем формирования новых правовых фикций, которые позволяют связывать определенные национальные сегменты киберпространства (доменные зоны, физическую инфраструктуру) с юрисдикцией конкретного государства, фактически «заземляя» виртуальное пространство. И в то же время в условиях необходимости регулирования трансграничных потоков данных существенное распространение в условиях цифровизации получает экстратерриториальная юрисдикция государств в пределах так называемого виртуального контура, в рамках которого осуществляется контроль над данными и реализация политики технологической зависимости.

Список литературы

- Ансельмо, Э. (2006). Киберпространство в международном законодательстве: опровергает ли развитие Интернета принцип территориальности в международном праве? *Экономические стратегии*, 2, 24–31.
- Бахин, С. В. (2002). Правовые проблемы договорной унификации. *Московский журнал международного права*, 1, 129–143. EDN: HSIVQQ. DOI: 10.24833/0869-0049-2002-1-129-143
- Самарин, А. А. (2016). *Экстратерриториальное действие права*: автореф. дис. ... канд. юрид. наук. Нижний Новгород. 2016. EDN: ZQAIH
- Стрельцов, А. А. (2017). Суверенитет и юрисдикция государства в среде информационно-коммуникационных технологий в контексте международной безопасности. *Международная жизнь*, 2, 87–106. EDN: XVLADB
- Талапина, Э. В. (2018). Право и цифровизация: новые вызовы и перспективы. *Журнал российского права*, 2. EDN: YNJEIF. DOI: 10.12737/art_2018_2_1
- Терентьева, Л. В. (2019). Территориальный аспект юрисдикции и суверенитета государства в киберпространстве. *Lex Russica*, 4. EDN: WAYQRS. DOI: 10.17803/1729-5920.2019.149.4.139-150
- Терентьева, Л. В. (2019). Управление киберпространством по модели мультистейкхолдеризма. *Право и Экономика*, 3. EDN: UGGQPC
- Adams, J., & Albakajai, M. (2016). Cyberspace: A New Threat to the Sovereignty of the State. *Management Studies*, 4(6). <https://doi.org/10.17265/2328-2185/2016.06.003>
- Benyekhlef, K., & Gelinis, F. (2009). The International Experience in regard to Procedures for Settling Conflicts relating to Buxbaum H.L. Territory, Territoriality, and the Resolution of Jurisdictional Conflict. *American Journal of Comparative Law*, 57. Copyright in the Digital Environment. (2001). *UNESCO Copyright Bulletin*, XXXV(4).
- Huang, J. (2023). Developing Chinese Private International Law for Transnational Civil and Commercial Litigation: The 2024 New Chinese Civil Procedure Law. *Netherlands International Law Review*, 70. <https://doi.org/10.1007/s40802-023-00243-3>
- Johnson, D., & Post, D. (1996). Law And Borders: The Rise of Law in Cyberspace. *Stanford Law Review**, 1367.
- Kobrin, S. (1997). Electronic cash and the end of national markets. *Foreign Policy*, 107(4), 65–77. <https://doi.org/10.2307/1149333>
- Lithgoe, G. (2024). *The Rebirth of Territory*. Cambridge University Press.

- Lodder, A. R. (2013). Ten Commandments of Internet Law Revisited: Basic Principles for Internet Lawyers. *Information & Communications Technology Law*, 22(3). <https://doi.org/10.1080/13600834.2013.852769>
- Matusitz, J. (2014). Intercultural perspectives on cyberspace: An updated examination. *Journal of Human Behaviour in the Social Environment*, 24(7), 713–724. <https://doi.org/10.1080/10911359.2013.849223>
- Menthe, D. C. (1998). Jurisdiction in Cyberspace: A Theory of International Spaces. *Michigan Telecommunications and Technology Law Review*, 4(1), 69–103. <https://repository.law.umich.edu/cgi/viewcontent.cgi?article=1163&context=mttlr>
- Mills, A. (2014). Rethinking Jurisdiction in International Law. *British Yearbook of International Law*, 84(1), 187–239. <https://doi.org/10.1093/bybil/bru003>
- Mueller, M. L. (2020). Against sovereignty in cyberspace. *International Studies Review*, 22(4), 779–801. <https://doi.org/10.1093/isr/viz044>
- Parrish, A. (2009). Reclaiming International Law from Extraterritoriality. *Minnesota Law Review*, 93. <https://doi.org/10.2139/ssrn.1013740>
- Pierucci, F. (2025). Sovereignty in the Digital Era: Rethinking Territoriality and Governance in Cyberspace. *Digital Society*, 4(27). <https://doi.org/10.1007/s44206-025-00189-4>
- Razmetaeva, Y., Ponomarova, H., & Bylya-Sabadash, I. (2021). Jurisdictional issues in the digital age. *Ius Humani. Law Journal*, 10(1), 167–183. <https://doi.org/10.31207/ih.v10i1.240>
- Ruohonen, J. (2021). The treachery of images in the digital sovereignty debate. *Minds and Machines*, 31(3), 439–456. <https://doi.org/10.1007/s11023-021-09566-7>
- Ryngaert, C. (2016). Introduction: Port State Jurisdiction: Challenges and Potential. *The International Journal of Marine and Coastal Law*, 31, 379–394. <https://doi.org/10.1163/15718085-12341405>
- Ryngaert, C. (2023). Extraterritorial Enforcement Jurisdiction in Cyberspace: Normative Shifts. *German Law Journal*, 24, 537–550. <https://doi.org/10.1017/glj.2023.24>
- Sharma, S. (2025). International law jurisdiction in cyberspace: Navigating legal frontiers in the digital domain. *International Journal of Law*, 11(7), 90–99.

References

- Adams, J., & Albakajai, M. (2016). Cyberspace: A New Threat to the Sovereignty of the State. *Management Studies*, 4(6). <https://doi.org/10.17265/2328-2185/2016.06.003>
- Anselmo, E. (2006). Cyberspace in International legislation: does the Internet development rejects the territoriality principle in international law? *Economicheskie strategii*, 2, 24–31. (In Russ.).
- Bakhin, S. V. (2002). Legal issues of Contract Unification. *Moscow Journal of International Law*, 1, 129–143. (In Russ.). <https://doi.org/10.24833/0869-0049-2002-1-129-143>
- Benyekhlief, K., & Gelinas, F. (2009). The International Experience in regard to Procedures for Settling Conflicts relating to Buxbaum H.L. Territory, Territoriality, and the Resolution of Jurisdictional Conflict. *American Journal of Comparative Law*, 57. Copyright in the Digital Environment. (2001). *UNESCO Copyright Bulletin*, XXXV(4).
- Huang, J. (2023). Developing Chinese Private International Law for Transnational Civil and Commercial Litigation: The 2024 New Chinese Civil Procedure Law. *Netherlands International Law Review*, 70. <https://doi.org/10.1007/s40802-023-00243-3>
- Johnson, D., & Post, D. (1996). Law And Borders: The Rise of Law in Cyberspace. *Stanford Law Review*, 1367.
- Kobrin, S. (1997). Electronic cash and the end of national markets. *Foreign Policy*, 107(4), 65–77. <https://doi.org/10.2307/1149333>
- Lithgoe, G. (2024). *The Rebirth of Territory*. Cambridge University Press.
- Lodder, A. R. (2013). Ten Commandments of Internet Law Revisited: Basic Principles for Internet Lawyers. *Information & Communications Technology Law*, 22(3). <https://doi.org/10.1080/13600834.2013.852769>
- Matusitz, J. (2014). Intercultural perspectives on cyberspace: An updated examination. *Journal of Human Behaviour in the Social Environment*, 24(7), 713–724. <https://doi.org/10.1080/10911359.2013.849223>
- Menthe, D. C. (1998). Jurisdiction in Cyberspace: A Theory of International Spaces. *Michigan Telecommunications and Technology Law Review*, 4(1), 69–103. <https://repository.law.umich.edu/cgi/viewcontent.cgi?article=1163&context=mttlr>
- Mills, A. (2014). Rethinking Jurisdiction in International Law. *British Yearbook of International Law*, 84(1), 187–239. <https://doi.org/10.1093/bybil/bru003>
- Mueller, M. L. (2020). Against sovereignty in cyberspace. *International Studies Review*, 22(4), 779–801. <https://doi.org/10.1093/isr/viz044>
- Parrish, A. (2009). Reclaiming International Law from Extraterritoriality. *Minnesota Law Review*, 93. <https://doi.org/10.2139/ssrn.1013740>
- Pierucci, F. (2025). Sovereignty in the Digital Era: Rethinking Territoriality and Governance in Cyberspace. *Digital Society*, 4(27). <https://doi.org/10.1007/s44206-025-00189-4>
- Razmetaeva, Y., Ponomarova, H., & Bylya-Sabadash, I. (2021). Jurisdictional issues in the digital age. *Ius Humani. Law Journal*, 10(1), 167–183. <https://doi.org/10.31207/ih.v10i1.240>

- Ruohonen, J. (2021). The treachery of images in the digital sovereignty debate. *Minds and Machines*, 31(3), 439–456. <https://doi.org/10.1007/s11023-021-09566-7>
- Ryngaert, C. (2016). Introduction: Port State Jurisdiction: Challenges and Potential. *The International Journal of Marine and Coastal Law*, 31, 379–394. <https://doi.org/10.1163/15718085-12341405>
- Ryngaert, C. (2023). Extraterritorial Enforcement Jurisdiction in Cyberspace: Normative Shifts. *German Law Journal*, 24, 537–550. <https://doi.org/10.1017/glj.2023.24>
- Samarin, A. A. (2016). *Exterritorial action of law*: abstract of a Cand. Sci. (Law) thesis. Nizhny Novgorod. (In Russ.).
- Sharma, S. (2025). International law jurisdiction in cyberspace: Navigating legal frontiers in the digital domain. *International Journal of Law*, 11(7), 90–99.
- Strelcov, A. A. (2017). Sovereignty and jurisdiction of a state in the information-communication technologies environment in the context of international security. *Mezhdunarodnaya Zhizn*, 2, 87–106. (In Russ.).
- Talapina, E. (2018). Law and Digitalization: New Challenges and Prospects. *Journal of Russian Law*, 2. (In Russ.). https://doi.org/10.12737/art_2018_2_1
- Terenteva, L. V. (2019). Cyberspace governance according to the multistakeholder model. *Pravo i Ekonomika*, 3. (In Russ.).
- Terenteva, L. V. (2019). Territorial aspect of state jurisdiction and sovereignty in cyberspace. *Lex Russica*, 4. (In Russ.). <https://doi.org/10.17803/1729-5920.2019.149.4.139-150>

* Принадлежит нежелательной организации в РФ / Belongs to an undesirable organization in the Russian Federation.

Вклад автора

Автор подтверждает, что полностью отвечает за все аспекты представленной работы.

Author's contribution

The author confirms sole responsibility for all aspects of the work.

Информация об использовании искусственного интеллекта

AI was not used.

Information about the use of artificial intelligence

ИИ не использовался.

Конфликт интересов / Conflict of Interest

Автором не заявлен / No conflict of interest is declared by the author

История статьи / Article history

Дата поступления / Received 24.11.2025

Дата одобрения после рецензирования / Date of approval after reviewing 21.01.2026

Дата принятия в печать / Accepted 25.02.2026