

О взаимосвязи вопросов обеспечения информационного суверенитета Российской Федерации и формирования цифровой среды доверия¹

Аннотация. Статья посвящена исследованию значимости вопроса обеспечения информационного суверенитета для формирования цифровой среды доверия. Автором использовались методы: построение гипотез, идеализация, правовое моделирование, сравнительный правовой метод. Полученные результаты: В условиях глобализации и цифровой трансформации происходит видоизменение форм и механизмов реализации социально-экономических отношений, формирование новых инструментов взаимодействий. Возникающие при этом новые и производные риски, вызовы и угрозы формируют очевидный запрос на формирование среды доверия реализации всего спектра общественных отношений в цифровом пространстве.

В статье обосновывается взаимосвязь обеспечения информационного и технологического суверенитета и формирования цифровой среды доверия в современном государстве. В настоящий момент использование территориального подхода в отношении информационной инфраструктуры при определении сферы действия государственного суверенитета в информационном пространстве является преобладающим подходом в решении данных задач.

В рамках данного подхода реализованы ключевые составные элементы информационного суверенитета, среди которых механизм локализации персональных данных, использования доменных имен на территории Российской Федерации, установления требований к операторам связи, установлены правовые основы деятельности для иностранных лиц, осуществляющих деятельность в сети Интернет.

Ключевые слова: суверенитет, информационный суверенитет, цифровой суверенитет, цифровое пространство, среда доверия, цифровая трансформация.



**Алексей Игоревич
ХИМЧЕНКО,**

старший преподаватель
кафедры информационного
права и цифровых
технологий Университета
имени О.Е. Кутафина
(МГЮА),
кандидат юридических наук
[alekseykhimchenko@
yandex.ru](mailto:alekseykhimchenko@yandex.ru)
125993, Россия, г. Москва,
ул. Садовая-Кудринская, д. 9

DOI: 10.17803/2311-5998.2022.92.4.083-091

¹ Исследование выполнено в рамках программы стратегического академического лидерства «Приоритет-2030».

ALEKSEY I. KHIMCHENKO,

Associate Professor of the Department
of information law and digital technologies
of the Kutafin Moscow State Law University (MSAL),
Cand. Sci. (Law)

alekseykhimchenko@yandex.ru

9, ul. Sadovaya-Kudrinskaya, Moscow, Russia, 125993

**On the interconnection of issues of ensuring the information
sovereignty of the Russian Federation and the formation
of a digital environment of trust**

Abstract. *The study focuses on the importance of information sovereignty for the formation of a digital environment of trust. The author used the following methods: hypothesis building, idealization, legal modeling, and comparative legal method. Results. In the context of globalization and digital transformation, there is a modification of the forms and mechanisms of the implementation of socio-economic relations, the formation of new instruments of interaction. The emerging new and derivative risks, challenges and threats form an obvious request for the formation of an environment of trust for the implementation of the entire spectrum of public relations in the digital space. The article substantiates the relationship between ensuring information and technological sovereignty and the formation of a digital environment of trust in a modern state. The use of a territorial approach in relation to information infrastructure in determining the scope of state sovereignty in the information space is the prevailing approach in solving these tasks.*

Within the framework of this approach, the key components of information sovereignty have been implemented, including the mechanism of localization of personal data, the use of domain names on the territory of the Russian Federation, the establishment of requirements for telecom operators, the legal basis of activity for foreign persons operating on the Internet has been established.

Keywords: *sovereignty, information sovereignty, digital sovereignty, digital space, trust environment, digital transformation, information technology, digital environment of trust, legal regulation, information sovereignty, digital transformation.*

Активные процессы цифровой трансформации как в отдельных сферах экономики, так и в области государственного управления и системе публичной власти в целом оказывают влияние на качество общественных отношений, их содержание и реализацию. Возникающие при этом новые и производные риски, вызовы и угрозы формируют очевидный запрос на формирование среды доверия реализации всего спектра общественных отношений в цифровом пространстве.

Проблема обеспечения доверия является основополагающей при взаимодействии в цифровой среде и достигается посредством набора комплексных

решений, среди которых обеспечение основных прав человека и гражданина в информационной среде, контроля субъектов информационных правоотношений над своими данными за счет прозрачности их оборота, создание качественных решений в части расширения возможностей и способов идентификации².

Решение указанных задач предполагает долгосрочную фундаментальную правовую, технологическую и методологическую работу в широком диапазоне составляющих ее многих дифференцированных задач, ключевой из которых является создание качественной информационно-коммуникационной инфраструктуры и поддержание соответствующего уровня ее функционирования. При этом подходы к решению осложняются самой трансграничной природой информационных технологий и соответствующей территориальной спецификой, формируют вопрос о возможности определения территории и территориальных границ в информационной сфере, что часто становится предметом внимания научного сообщества³.

Однако, как отмечают ученые, к настоящему моменту понимания, что такое государственный суверенитет в цифровом пространстве, в целом так и не появилось⁴.

Вместе с тем общемировые тенденции по изменению глобального государственного устройства, повышение санкционной и ограничительной активности, активная геополитическая и экономическая конкуренция основных игроков и неизбежный переход к многополярному мироустройству, с одной стороны, повышает сложность решаемой задачи, с другой же — вносит определенную методическую ясность, суть которой заключается в очевидности того, что среда доверия в современном (цифровом?) государстве может быть реализована только в условиях соответствующего информационного и технологического суверенитета.

Анализ показывает, что суверенитет в информационном пространстве находится в активном фокусе стратегических и концептуальных правовых актов.

Так, в Стратегии развития информационного общества в Российской Федерации на 2017—2030 годы, утвержденной Указом Президента РФ от 09.05.2017 № 203⁵, содержится положение о необходимости отстаивать 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 1 декабря 2016 г. № 642⁶, установлено, что в условиях значительных ограничений других возможностей развития Российской Федерации риски и угрозы в информационной сфере становятся существенным барьером, препятствующим долгосрочному росту благосостояния общества и укреплению суверенитета России.

² Цифровая среда доверия / В. Наумов, Е. Авакян, А. Чубурков [и др.] // Закон. 2019. № 9. С. 26.

³ Стрельцов А. А. О предмете и методе информационного права // Информационное право. 2019. № 4.

⁴ URL: <https://msal.ru/news/advokatskaya-gazeta-eksperty-obsudili-voprosy-gosudarstvennogo-suvereniteta-v-informatsionnom-pole/> (дата обращения: 01.05.2021).

⁵ СЗ РФ. 2017. № 20. Ст. 2901.

⁶ СЗ РФ. 2016. № 49. Ст. 6887.



В Стратегии развития отрасли информационных технологий в Российской Федерации на 2014—2020 годы и на перспективу до 2025 года, утвержденной распоряжением Правительства РФ от 01.11.2013 № 2036-р⁷, к числу мер долгосрочного характера отнесено обеспечение стабильности развития и суверенности российской отрасли информационных технологий в долгосрочной перспективе.

Доктрина информационной безопасности Российской Федерации, утвержденная Указом Президента РФ от 05.12.2016 № 646⁸, защиту суверенитета Российской Федерации в информационном пространстве относит к основным направлениям обеспечения информационной безопасности.

В Основах государственной политики Российской Федерации в области международной информационной безопасности, утвержденных Указом Президента РФ от 12.04.2021 № 213⁹, использование информационно-коммуникационных технологий в военно-политической и иных сферах в целях подрыва (ущемления) суверенитета отнесено к основным угрозам международной информационной безопасности.

Национальная стратегия развития искусственного интеллекта на период до 2030 года, утвержденная Указом Президента РФ от 10.10.2019 № 490¹⁰, определяет необходимость обеспечения «технологического суверенитета Российской Федерации».

В паспорте национального проекта Национальной программы «Цифровая экономика Российской Федерации»¹¹ достижение суверенитета и устойчивого социально-экономического развития Российской Федерации в условиях цифровой экономики отнесено к целям реализации федерального проекта «Информационная безопасность».

Исследуя вопросы информационного суверенитета, ученые Е. В. Виноградова и Т. А. Полякова выделяют тенденцию к локализации сферы действия государственного суверенитета отдельных государств на основе привязки соответствующих информационных пространств к находящейся на территории конкретного государства информационной инфраструктуре. При этом в качестве возможных подходов к определению содержания информационного пространства выделяются территориальный, связывающий соответствующую информационную инфраструктуру и информационные ресурсы с территорией конкретного государства, и экстерриториальный, распространяющий действие правовых норм и деятельность органов государственной власти одного государства на территории других¹².

Очевидно, что решения, формирующие основу цифровой среды доверия, находятся в тесной взаимосвязи с условиями информационно-коммуникационной

⁷ СЗ РФ. 2013. № 46. Ст. 5954.

⁸ СЗ РФ. 2016. № 50. Ст. 7074.

⁹ СЗ РФ. 2021. № 16 (ч. I). Ст. 2746.

¹⁰ СЗ РФ. 2019. № 41. Ст. 5700.

¹¹ Утверждена президиумом Совета при Президенте РФ по стратегическому развитию и национальным проектам (протокол от 04.06.2019 № 7).

¹² Виноградова Е. В., Полякова Т. А. О месте информационного суверенитета в конституционно-правовом пространстве современной России // Правовое государство: теория и практика. 2021. № 1 (63). С. 40.

инфраструктурый. При этом, поскольку состояние соответствующей инфраструктуры влияет на научно-технический, экономический и оборонный потенциал России, эксплуатация и развитие ее осуществляется с учетом актуальной международной повестки.

Законодательство должно реализовать ключевые направления информационного суверенитета по территориальному признаку, информационной инфраструктуре и быть направленным на снижение угроз устойчивости, безопасности и целостности функционирования сети Интернет и сетей связи общего пользования, обеспечение устойчивого и безопасного использования на территории Российской Федерации доменных имен, локализацию персональных данных, организацию выпуска цифровой валюты и др.

Так, ст. 14.2 Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»¹³ определяет порядок обеспечения устойчивого и безопасного использования на территории Российской Федерации доменных имен.

Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных»¹⁴ установлено, что при сборе персональных данных, в том числе посредством информационно-телекоммуникационной сети Интернет, оператор обязан обеспечить запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение персональных данных граждан Российской Федерации с использованием баз данных, находящихся на территории Российской Федерации.

В соответствии с ч. 5.1 ст. 46 Федерального закона от 07.07.2003 № 126-ФЗ «О связи»¹⁵ оператор связи, оказывающий услуги по предоставлению доступа к сети Интернет, обязан обеспечивать установку в своей сети связи технических средств противодействия угрозам устойчивости, безопасности и целостности функционирования на территории Российской Федерации информационно-телекоммуникационной сети Интернет и сети связи общего пользования. Статьей 56.1 определяется организация деятельности по обеспечению устойчивого, безопасного и целостного функционирования на территории Российской Федерации информационно-телекоммуникационной сети Интернет. В соответствии с ч. 3 ст. 5 собственниками или иными владельцами линий связи, пересекающих Государственную границу Российской Федерации, могут являться только российские юридические лица.

В соответствии со ст. 14 Федерального закона от 31.07.2020 № 259-ФЗ «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации»¹⁶ организация выпуска цифровой валюты в Российской Федерации осуществляется с использованием объектов российской информационной инфраструктуры, к которой отнесены «доменные имена и сетевые адреса, находящиеся в российской национальной доменной зоне, и (или) информационные системы, технические средства которых размещены на территории Российской Федерации, и (или) комплексы

¹³ СЗ РФ. 2006. № 31 (ч. I). Ст. 3448.

¹⁴ СЗ РФ. 2006. № 31 (ч. I). Ст. 3451.

¹⁵ СЗ РФ. 2003. № 28. Ст. 2895.

¹⁶ СЗ РФ. 2020. № 31 (ч. I). Ст. 5018.



программно-аппаратных средств, размещенные на территории Российской Федерации».

Указанные нормы, способствуя повышению устойчивости и безопасности информационной инфраструктуры, направлены на исключение возможности деструктивного воздействия на ее объекты иностранными бенефициарами, что способствует созданию безопасного инфраструктурного контура для «решений доверия».

Помимо реализованных к настоящему моменту подходов по законодательной реализации информационного суверенитета, отдельного рассмотрения заслуживает норма, установившая правовые основы деятельности иностранных лиц, осуществляющих деятельность в сети Интернет на территории Российской Федерации, на которой стоит остановиться подробно.

Актуальность законодательной инициативы обусловлена существенной долей рынка информационных технологий России, в настоящее время занимаемой зарубежными корпорациями. Так, по данным исследований, поисковую систему Google предпочитают около 56 % российских пользователей, второе и третье место по популярности среди социальных сетей в России занимают Facebook (16 % аудитории) и Twitter (14 % аудитории), а видеохостинг YouTube, бенефициаром которого выступает компания Google LLC, является третьим по популярности в России информационным ресурсом с ежемесячной аудиторией более 44 млн человек.

Не располагая достаточным правовым инструментарием для реализации своих прав в российском правовом поле, пользователь становился заложником иностранных юрисдикций и особенностей их применения.

Так, анализ пользовательских соглашений, таких платформ как eBay, Google, Amazon Web Services, показывает, что указанные в них оговорки о применимом праве демонстрируют инкорпорированный в пользовательские соглашения выбор применимого права при очень условной автономии воли сторон¹⁷ и едва ли позволяют сделать вывод о стремлении платформы к соблюдению прав пользователя.

В сложившейся ситуации активного пользования иностранными информационными продуктами без достаточных механизмов защиты прав пользователей законодателем были предприняты инициативы по регламентации деятельности иностранных юридических лиц, иностранных организаций, не являющихся юридическими лицами, иностранных граждан, лиц без гражданства, осуществляющих деятельность в информационно-телекоммуникационной сети Интернет на территории Российской Федерации.

Федеральным законом от 01.07.2021 № 236-ФЗ «О деятельности иностранных лиц в информационно-телекоммуникационной сети Интернет на территории Российской Федерации»¹⁸ были установлены правовые основы деятельности иностранных юридических лиц, иностранных организаций, не являющихся юридическими лицами, иностранных граждан, лиц без гражданства, осуществляющих деятельность в информационно-телекоммуникационной сети Интернет на

¹⁷ Мажорина М. В. Цифровые платформы и международное частное право, или Есть ли будущее у киберправа? // Lex russica. 2019. № 2.

¹⁸ СЗ РФ. 27 (ч. I). Ст. 5064.

территории Российской Федерации, определены полномочия органов государственной власти Российской Федерации, а также права и обязанности лиц, участвующих в указанной деятельности или пользующихся услугами (результатами) такой деятельности.

Федеральным законом дается определение понятия «иностранное лицо, осуществляющее деятельность в сети Интернет на территории Российской Федерации», а также определяются условия, при которых лицо будет им признано. Под иностранным лицом, осуществляющим деятельность в сети Интернет на территории Российской Федерации, понимается иностранное лицо, осуществляющее любую деятельность, не запрещенную на территории Российской Федерации, осуществляемую при условии, что иностранное лицо является владельцем сайта в сети Интернет, и (или) страницы сайта в сети Интернет, и (или) информационной системы, и (или) программы для электронных вычислительных машин, доступ к которым в течение суток составляет более пятисот тысяч пользователей сети Интернет, находящихся на территории Российской Федерации.

Такие обязанности распространяются на провайдеров хостинга, операторов рекламных систем и организаторов распространения информации в сети Интернет.

Законом устанавливается обязанность указанных лиц, в частности, создать филиал, или открыть представительство, или учредить российское юридическое лицо и обеспечить функционирование на территории Российской Федерации филиала, или представительства, или российского юридического лица в соответствии с предусмотренными требованиями.

Определяются полномочия федерального органа исполнительной власти, осуществляющего функции по контролю и надзору в сфере средств массовой информации, массовых коммуникаций, информационных технологий и связи (Роскомнадзор), по размещению на своем официальном сайте в сети Интернет перечня иностранных лиц, осуществляющих деятельность в сети Интернет на территории Российской Федерации, и поддержанию его в актуальном состоянии.

Устанавливаются виды мер понуждения к исполнению иностранными лицами, осуществляющими деятельность в сети Интернет на территории Российской Федерации, законодательства Российской Федерации:

- информирование пользователей информационного ресурса иностранного лица о нарушении иностранным лицом, осуществляющим деятельность в сети Интернет на территории Российской Федерации, законодательства Российской Федерации;
- запрет на распространение рекламы иностранного лица, осуществляющего деятельность в сети Интернет на территории Российской Федерации и (или) его информационного ресурса в качестве объекта рекламирования;
- запрет на распространение рекламы на информационном ресурсе иностранного лица;
- ограничение осуществления переводов денежных средств и приема платежей физических и юридических лиц в пользу иностранного лица, осуществляющего деятельность в сети Интернет на территории Российской Федерации;
- запрет на поисковую выдачу;
- запрет на сбор и трансграничную передачу персональных данных;



— частичное или полное ограничение доступа к информационному ресурсу иностранного лица.

По прогнозам, в первую очередь закон коснется таких ресурсов, как Facebook, Instagram, Twitter, TikTok, Google, YouTube, WhatsApp, Viber, Telegram, World of Tanks¹⁹.

Установление обязанности для иностранных лиц, осуществляющих деятельность в сети Интернет на территории Российской Федерации, соблюдать требования, запреты и ограничения, предусмотренные законодательством РФ, способствует обеспечению информационного суверенитета, расширению правовых возможностей по защите пользователями своих прав, повышению доверия пользователей к используемым сервисам, что благоприятствует формированию среды доверия.

А установление равных условий деятельности для российских и иностранных лиц способствует повышению конкуренции на технологическом рынке, что, в свою очередь, стимулирует повышение потребительских характеристик информационных продуктов.

В развитие указанного Закона постановлением Правительства РФ от 14.01.2022 № 6²⁰ утверждены правила взаимодействия Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций с лицами, указанными в п. 3 ч. 9 ст. 14 Федерального закона «О деятельности иностранных лиц в информационно-телекоммуникационной сети Интернет на территории Российской Федерации».

Таким образом, можно отметить, что на сегодня использование территориального подхода в отношении информационной инфраструктуры при определении сферы действия государственного суверенитета в информационном пространстве является преобладающим подходом в решении соответствующих задач.

С использованием данного подхода реализованы ключевые составные элементы информационного суверенитета, среди которых механизм локализации персональных данных, использование доменных имен на территории Российской Федерации, установление требований к операторам связи, установление правовых основ деятельности иностранных лиц, в сети Интернет.

Указанные законодательные решения в условиях возрастающего количества уязвимостей и рисков направлены на снижение вызовов и угроз устойчивости, безопасности и целостности функционирования российской информационной инфраструктуры, способствуют всесторонней эффективной защите прав и законных интересов участников информационных правоотношений, стимулируют формирование соответствующей среды доверия в информационном пространстве.

¹⁹ URL: <http://duma.gov.ru/news/53199/>.

²⁰ URL: <http://pravo.gov.ru>. 18.01.2022.

БИБЛИОГРАФИЯ

1. *Виноградова Е. В., Полякова Т. А.* О месте информационного суверенитета в конституционно-правовом пространстве современной России // Правовое государство: теория и практика. — 2021. — № 1 (63). — С. 32—50.
2. *Мажорина М. В.* Цифровые платформы и международное частное право, или Есть ли будущее у киберправа? // Lex russica. — 2019. — № 2. — С. 107—120.
3. *Стрельцов А. А.* О предмете и методе информационного права // Информационное право. — 2019. — № 4. — С. 4—11.
4. Цифровая среда доверия / В. Наумов, Е. Авакян, А. Чубурков [и др.] // Закон. — 2019. — № 9. — С. 25—38.

