УДК 342.7
ББК 67.400.32

ПРАВО НА ДОСТОВЕРНУЮ ИНФОРМАЦИЮ В СЕТИ ИНТЕРНЕТ: ВЫЗОВЫ ФЕЙКОВИЗАЦИИ И ПУТИ РЕШЕНИЯ

А. Е. Канакова
Алтайский государственный университет (Барнаул, Россия)
ORCID: 0000–0003–1912–4575

Современное цифровое пространство, выступая ключевым элементом глобальной коммуникации, трансформирует традиционные правовые институты, создавая беспрецедентные вызовы для реализации фундаментального права на достоверную информацию. Актуальность исследования обусловлена экспоненциальным ростом масштабов фейковизации контента, использованием алгоритмических инструментов манипуляции и отсутствием эффективных механизмов противодействия дезинформации в трансграничном формате. Виртуальная среда, характеризуясь анонимностью, скоростью распространения данных и стиранием географических границ, формирует качественно новые условия для реализации права на информацию, традиционно регулируемого в оффлайн-пространстве. Это требует переосмысления классических правовых подходов и разработки специализированных норм, адаптированных к цифровым реалиям. В статье обосновывается, что виртуальное пространство создает уникальные особенности для права на информацию, связанные с трансграничностью и технологическими угрозами. Автор предлагает регулировать данную сферу через синтез «жестких» и «мягких» мер, обеспечивающих баланс между защитой информационной безопасности и сохранением свободы слова. Отдельное внимание уделяется формированию категории «виртуальная территория государства», которая не может быть ограничена традиционными административными границами. Автор аргументирует, что защита цифрового суверенитета должна осуществляться не через установление запретительных барьеров, нарушающих принципы открытости интернета, а посредством предупредительных и профилактических механизмов.

Ключевые слова: цифровизация, право на информацию, недостоверная информация, виртуальная территория

Финансирование: Исследование выполнено за счет гранта Российского научного фонда, проект № 23–78–01133 «Цифровизация прав и свобод человека и гражданина в Российской Федерации».

THE RIGHT TO RELIABLE INFORMATION ON THE INTERNET: CHALLENGES OF FAKEIZATION AND SOLUTIONS

A. E. Kanakova
Altai State University (Barnaul, Russia)
ORCID: 0000–0003–1912–4575

Modern digital space, acting as a key element of global communication, transforms traditional legal institutions, creating unprecedented challenges to the realization of the fundamental right to reliable information. The relevance of the research is due to the exponential growth of content faking, the use of algorithmic tools of manipulation and the lack of effective mechanisms to counter disinformation in a transboundary format. The virtual environment, characterized by anonymity, the speed of data dissemination and the erasure of geographical boundaries, forms qualitatively new conditions for the realization of the right to information, traditionally regulated in offline space. This requires a rethinking of classical legal approaches and the development of specialized norms adapted to digital realities. The article substantiates that virtual space creates unique features for the right to information related to transboundary nature and technological threats. The author proposes to regulate this sphere through a synthesis of «hard» and «soft» measures, ensuring a balance between the protection of information security and preservation of freedom of speech. Special attention is paid to the formation of the category of «virtual territory of the state»,

which cannot be limited by traditional administrative boundaries. The author argues that the protection of digital sovereignty should be realized not through the establishment of prohibitive barriers that violate the principles of Internet openness, but through preventive and prophylactic mechanisms.

Keywords: digitalization, right to information, inaccurate information, virtual territory

Funding: The research was supported by the Russian Science Foundation, project No. 23–78–01133: Digitalization of human and civil rights and freedoms in the Russian Federation.

Doi: https://doi.org/10.14258/ralj(2025)1.7

Несмотря на программность и невозможность мгновенной реализации многих положений Конституции Российской Федерации 1993 г. (далее — Конституция РФ), содержание прав, свобод и обязанностей, закрепленных в данном акте, отражало объективную реальность того времени. Так, в ст. 29 Конституции РФ закреплены свобода слова (ч. 1) и право на информацию (ч. 4), формулировки которых нацелены исключительно на оффлайн-пространство. Разумеется, данные нормы можно применить к правоотношениям в цифровой и (или) виртуальной сфере, однако в них отсутствует учет специфики данных внешних условий, отчего реализация и защита соответствующих правомочий не будет полноценной.

Предусмотренное в ч. 4 ст. 29 Конституции РФ наполнение права на информацию в рамках оффлайн-пространства является вполне контролируемым. Так, производителем информации не мог стать абсолютно любой человек, распространение данных занимало определенное, иногда продолжительное время, причем нередко на конкретную территорию или ее часть, попытки незаконного получения сведений предполагали нахождение нарушителя в непосредственной территориальной близости к объекту или субъекту, а полная анонимность, особенно для производителя и распространителя информации, являлась невозможной.

В рамках реального мира уже устоялись основные механизмы поиска баланса между правами и свободами, в части ненарушения чужих прав и свобод при реализации собственных (ч. 3 ст. 17 Конституции РФ). Однако стремительное развитие технологий внесло серьезные коррективы в данный процесс, разрушив некоторые привычные парадигмы. В частности, в современных условиях абсолютно каждый человек может примерить на себя роль производителя информации, разница между производителем и распространителем стерлась, скорость передачи данных приблизилась к мгновенной, а возможность полного сокрытия личности нарушителя стала вполне реализуемой.

Интернет, как глобальное информационное пространство, стал неотъемлемой частью жизни современного общества. Однако доступность и скорость распространения информации породили новую проблему — фейковизацию [1; 2], т. е. сознательное искажение фактов и создание ложных нарративов. Указанная ситуация обусловила необходимость переосмысления конституционных положений сквозь призму их соответствия текущей объективной реальности, в частности, смещения фокуса внимания с самого факта возможности облекать свое мнение в форму, доступную для восприятия другими субъектами, на характер данных сведений, очерчивая их границы посредством учета всех иных существующих прав и свобод. Условно правомочие, учитывающее баланс между разными правами и свободами, а также специфику сети Интернет, можно обозначить как право на достоверную информацию.

Разумеется, данное исследование не подразумевает необходимости внесения изменений в конституционный текст, так как характеристика достоверности является объективно предполагаемой и лишь формально не закрепленной. Право на достоверную информацию необходимо как условная категория, позволяющая сквозь ее призму рассмотреть масштабы фейковизации, ее последствия, а также меры по цифровизации права на информацию, изначально созданного и закрепленного для реализации в оффлайн-пространстве.

Фейковизация охватывает все сферы жизнедеятельности общества. В качестве примера политической манипуляции можно указать массовое распространение мифов о вакцинации в период пандемии COVID-19, что спровоцировало волну отказов от прививок [3]. В 2023 г. deepfake-видео с «обращением президента о мобилизации» вызвало панику среди населения [4]. В 2020 г. ложные со-

общения о введении «полного карантина» в Москве [5] создали социальную дестабилизацию, а распространение слухов о дефолте банков в 2022 г. привело к оттоку вкладов [6].

Рост числа фейковых новостей стал глобальным трендом. Медиахолдинг Rambler&Co провел опрос 262 374 интернет-пользователей, 93% которых сталкивались с недостоверной информацией (социальные сети и мессенджеры — 64%, телевидение — 16%, интернет-издания — 15%) [7]. С начала СВО и до апреля 2023 г. Роскомнадзор заблокировал уже свыше 157 тыс. ресурсов, где размещались фейки о ходе спецоперации наряду с антироссийской пропагандой [8]. За 2024 г. было удалено или заблокировано 26,9 тыс. материалов, содержащих фейки о СВО [9]. Суммарно за два года за фейки о ВС РФ или их дискредитацию в России осудили 132 человека [10].

Дефиниции категорий «фейк» и «фейковизация» в российском законодательстве отсутствуют. В рамках юридической доктрины [11–16] содержание данных категорий выводится посредством теоретических осмыслений и толкования действующих нормативных правовых актов, закрепляющих ответственность за совершение определенных действий, наименование которых не является унифицированным.

В Федеральном законе «Об информации, информационных технологиях и о защите информации» говорится о недостоверной информации в контексте требований по ее удалению с сетевых изданий и социальных сетей или ограничению доступа к ней. В ст. 13.15 Кодекса Российской Федерации об административных правонарушениях, посвященной злоупотреблению свободой массовой информации, предусматривается ответственность за распространение заведомо ложных сведений и заведомо недостоверной информации. Уголовный кодекс Российской Федерации касается ответственности за публичное распространение заведомо ложной информации (ст. 207.1, 207.2, 207.3).

Таким образом, законодатель использует отчасти синонимичные, но формально отличающиеся категории. Размытость данных понятий порождает сложности оценки соответствия совершенных действий критериям нарушения законодательства.

Проблема определения умысла и степени осознания недостоверности распространяемой информации усугубляется тем, что значительная часть трафика в сети Интернет приходится на боты: в 2022 г. 40,5% трафика в российском интернете генерировали боты [17]. Поэтому не исключены ситуации, когда поиск нарушителя приведет к не-субъекту [18] и к необходимости предпринимать правозащитные действия исключительно в отношении распространяемых данных.

Немаловажным является момент того, кто и по каким критериям определяет фейковый характер соответствующей информации. На данный момент субъектами, участвующими в процессе принятия подобного решения, являются Роскомнадзор и прокуратура, что порождает ряд социальных феноменов, негативно сказывающихся на уровне доверия к власти: патернализм (государство или платформы решают за пользователя, что ему можно читать), эффект Стрейзанд (блокировка контента повышает интерес к нему), подозрения в манипуляции (власть может злоупотреблять критериями «недостоверности», удаляя неудобные мнения).

На сегодня в сфере распространения информации очевидной является тенденция к расширению и уточнению списка тем и вопросов, режим оборота которых предполагает ограничение или запрет. Закрытие доступа к определенному ресурсу в сети Интернет можно рассматривать как один из способов формирования виртуальной территории государства, исключая возможность существования правоотношений посредством сайтов, отказывающихся подчиняться российской юрисдикции. Однако при распространении российского законодательства на виртуальное пространство главным является вопрос соразмерности ограничений.

Право на достоверную информацию требует в первую очередь не запретов, а создания экосистемы доверия. Это возможно через синтез «жестких» мер (технологии, законы) и «мягких» (образование, негосударственные организации). Критически важно избежать крайностей: избыточная регуляция превратит интернет в «стерильное» пространство, а ее отсутствие — в цифровой Вавилон, в котором смешаются не языки, а правда, ложь, фейки и факты. Решение — в балансе, где государство, бизнес и граждане совместно отвечают за чистоту информационной среды.

Механизм полной блокировки сайта имеет ряд серьезных недостатков. Во-первых, блокирование доступа ко всему ресурсу в случае наличия на нем отдельных материалов, незаконных с позиции Российской Федерации, влияет на право на информацию населения России, ограничивая его, что ста-

вит вопрос о соразмерности этой меры, когда иные данные на ресурсе с ограниченным доступом являются социально полезными или нейтральными.

Во-вторых, технологии продолжают развиваться, и реализуемые на данный момент методы ограничения доступа могут в дальнейшем стать неэффективными. В качестве примера можно указать неудачную попытку блокировки приложения Telegram: данный мессенджер использует распределенную инфраструктуру с тысячами IP-адресов, привязанных к серверам по всему миру (например, Amazon, Google). Блокировка этих адресов приводила к сопутствующему ущербу: страдали сторонние сервисы, такие как YouTube, Google и другие. Роскомнадзор не смог полностью изолировать Telegram без массовых отключений интернет-трафика, что было невыгодно экономически и политически [19–21]. На данный момент развитие получают децентрализованные технологии IPFS, Mastodon, Nostr [22–24], размещающие данные на разных узлах, отчего блокировка одного из них не закрывает возможность получения данных из других источников.

Таким образом, государству необходимо прорабатывать новые подходы к распространению фейковых данных. Например, установить для всех цифровых платформ (соцсети, мессенджеры, поисковики), доступных на территории России, обязанность внедрить механизм оперативного удаления контента, признанного российскими органами недостоверным. И только в случае неисполнения — блокировка сервиса на территории Российской Федерации.

Для реализации подобной инициативы необходимо выполнение определенных последовательных мероприятий.

Во-первых, создание Единого реестра недостоверной информации (далее — ЕРНИ). Роскомнадзор формирует реестр фейков на основе решений судов или межведомственной экспертной комиссии, где каждая запись будет в себя включать URL-адрес материала, цифровой отпечаток контента (хэш), краткое описание ложных фактов и опровержение (данные Росстата, Минздрава, судебные решения и т. п.).

Во-вторых, необходимо подключить платформы (например, с аудиторией от 100 тысяч пользователей с территории Российской Федерации) к системе, позволяющей разным приложениям общаться между собой (Application programming interface (далее — API)), т. е. к API ЕРНИ. В таком случае при загрузке пользователем контента система автоматически проверяет его на соответствие хэшам из реестра и блокирует совпадения.

Подобная технология работы с недостоверным контентом доступна для масштабирования в рамках соглашений различных стран, автоматизирует процесс, снизив нагрузку на модераторов, устранив необходимость «ручного» решения проблемы, и уменьшит проблему анонимности в сети, так как методы воздействия будут направлены на информацию, а не на субъект.

Однако пока подобные технологии существуют только в рамках возможных перспектив внедрения, технологический и правовой аспекты могут быть скорректированы иным способом для соблюдения баланса между властными возможностями и правами и свободами человека и гражданина, а именно установлением градации общественной опасности недостоверной информации. Так, в случае невозможности публично опровергнуть определенную информацию (например, на основе военной тайны) или при высокой социальной полезности иных частей сайта, содержащего недостоверную информацию, необходимо использовать «мягкие» методы. В частности, предлагается не закрывать доступ к данному ресурсу, а предусмотреть посредством взаимодействия с операторами связи появление предупреждения пользователя о том, что он собирается посетить ресурс, достоверность данных которого ставится под сомнение. В данном случае пользователь будет предупрежден о недостоверности информации, но все равно будет иметь возможность продолжить просматривать соответствующий сайт, что значительно снизит уровень негативной реакции общества, которая возникает в условиях установления полного запрета.

Данный подход можно реализовать не только в отношении недостоверной информации, но и информации, оборот которой запрещен или ограничен. В частности, провести градацию информации по уровню опасности (без злого умысла, с низким уровнем риска и угрожающая жизни и безопасности) и степени воздействия (повествовательный характер данных, позволяющий человеку сделать самостоятельные выводы, или информация прямого воздействующего влияния, побуждающая человека к определенным действиям). Таким образом, закрытие доступа должно осуществляться только в отношении данных, недостоверность которых подтверждена в рамках открытого источника и при-

чиняющих непосредственный вред. В иных случаях следует ограничиться предупреждением, выдаваемым оператором связи при направлении запроса на сайт с соответствующей информацией.

Подобный подход, во-первых, снизит уровень социальной напряженности, так как в качестве основного критерия общественного недовольства можно указать желание индивида, как дееспособного субъекта, самостоятельно принять решение о характере распространяемых данных. Во-вторых, выступит в роли профилактического механизма: ознакомившись с информацией, о недостоверности которой человек был предупрежден, с большой степенью вероятности индивид с аналогичной настороженностью отнесется к этой же или похожей информации, перед которой подобного предупреждения не было, так как закрытие доступа не является абсолютным — с помощью средств обхода блокировок люди могут получить эти данные и распространить их либо в рамках живого общения, либо на иных доступных сайтах.

Наряду с этим к «мягким» механизмам регулирования данной сферы можно отнести использование цифровых меток для информации от официальных источников (например, QR-код Минцифры), маркировка контента («Проверено: информация опровергнута Росстатом»; «Источник не подтвержден» и т. п.), популяризация фактчекинга [25] (например, проект «Проверено. Медиа» [26]).

Предложенная модель решает ключевой конфликт между свободой доступа к информации и защитой общества от дезинформации, устанавливая баланс и не превращая регулирование в цензуру. Эффективность данного подхода обусловлена свободой выбора (пользователь сам решает, доверять ли помеченной информации), прозрачностью (причины блокировки ресурса или информации находятся в открытом доступе) и снижением вреда (даже при доступе к фейкам пользователь видит предупреждение и опровержение). Ключевое правило в представленной схеме сводится к идее: не скрывать, а объяснять. Такой подход защищает и общество от фейков, и права граждан на доступ к информации.

Проведенный анализ позволяет сделать вывод, что действия, совершаемые индивидом в виртуальном пространстве, не порождают новое правомочие, не создают отдельное цифровое право, а лишь продолжают конституционные положения, так как у них единая правовая основа, общие принципы (например, о достоверности СМИ) и общая цель (защита общества от вреда, вызванного дезинформацией).

При этом важно отметить, что движение информации стало иметь волнообразную динамику: например, данные, полученные из источника в сети Интернет, передаются в формате обсуждения в реальном пространстве, а после вновь уходят в виртуальную сферу посредством написания комментария и т. п. Иными словами, одна и та же информация не может условно по секундам менять право, в рамках которого она распространяется, поэтому создание права на цифровую информацию или цифрового права на информацию будет излишним. Наличие оффлайн-аналога в виде права на информацию предопределяет лишь уточнение его содержания под специфику внешней среды реализации.

Вместе с этим учет особенностей сети Интернет выявляет важную проблему построения виртуального пространства соответствующего государства: не имея возможности провести регулирование всех сайтов, государства пытаются очертить зону собственной юрисдикции в сети Интернет посредством закрытия доступа к ресурсам, отказавшимся подчиняться их законам. Несомненно, на данный момент реализация указанного подхода позволяет государству обозначить границы собственного влияния на правоотношения, связанные с виртуальным пространством, тем самым дифференцируя территорию на зоны, где человек может рассчитывать на применение норм российского права и где это исключено (так как фактически человек будет использовать ресурс, запрещенный на территории России). Однако такая методика имеет временный характер (развитие технологий, направленных на изменение структуры сети Интернет, и создание способов обхода блокировок) и негативные социальные последствия (повышения уровня недоверия к власти из-за ограничения права на информацию). На основе этого можно предположить, что в дальнейшем используемые ныне блокировки потеряют собственную эффективность, дискредитировав властные структуры по критерию неспособности реализовать вынесенные запреты. В целях недопущения подобной ситуации при регулировании категории «виртуальная территория государства» Российской Федерации следует обозначить границы данной зоны посредством «мягких мер» предупреждающего характера, информируя пользователя о недостоверности данных, размещенных на определенном

ресурсе, о наличии на сайте информации, запрещенной к распространению на территории Российской Федерации и способной причинить вред индивиду, о том, что индивид не сможет прибегнуть к защитным механизмам, предусмотренным законодательством Российской Федерации, в случае нарушения его прав и свобод на просторах соответствующего сайта вследствие отказа владельцев сайта сотрудничать с Россией. При этом возможность использования «жестких мер» (как полная блокировка доступа к ресурсу) останется доступной, но реализовываться она должна только в четко оговоренных законом случаях.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Королёв И. А. Практики верификации и фактчекинга в контексте фейковизации медиапространства // Вестник Гродненского государственного университета имени Янки Купалы. Сер. 3. Филология. Педагогика. Психология. 2022. Т. 12, № 2. С. 51–64.

2. Наконечный И. С. Фейковизация медиапространства как фактор искажения «повестки дня» // Медиасреда. 2024. № 2. С. 20–23.

3. Немцева М. Печаль интеллекта: лучшие фейки о вакцине // Известия. 2022. URL: https://iz.ru/1143868/mariia-nemtceva/pechal-intellekta-luchshie-feiki-o-vaktcine (дата обращения: 09.01.2025).

4. Дипфейк с «обращением» Путина сделали при помощи технологии замены лица // ТАСС. Эксперт. 2023. URL: https://tass.ru/obschestvo/17933053 (дата обращения: 09.01.2025).

5. Власти Москвы опровергли сведения СМИ о введении полного карантина в столице // Газета. Ru. 2020. URL: https://www.gazeta.ru/social/news/2020/03/17/n_14171899. shtml (дата обращения: 09.01.2025).

6. Что будет с вкладом в банке в случае дефолта? // Сравни. ру. 2022. URL: https://www.sravni.ru/vklady/info/chto-budet-s-vkladom-v-banke-v-sluchae-defolta/ (дата обращения: 09.01.2025).

7. Исследование: более 90% опрошенных россиян сталкивались с фейками // РИА Новости. 2023. URL: https://ria.ru/20231214/feyki-1915671398.html (дата обращения: 09.01.2025).

8. Роскомнадзор заблокировал 157 тыс. фейков и призывов к митингам с начала СВО // ТАСС. 2023. URL: https://tass.ru/obschestvo/16665411 (дата обращения: 09.01.2025).

9. Роскомнадзор: официальный Telegram-канал. 2023. URL: https://t.me/rkn_tg/1345 (дата обращения: 09.01.2025).

10. В России за два года за фейки о ВС РФ или их дискредитацию осудили 132 человек // ТАСС. 2024. URL: https://tass.ru/obschestvo/20586579 (дата обращения: 09.01.2025).

11. Дорофеева В. В. Фейковые новости в современном медиапространстве // Вопросы теории и практики журналистики. 2019. Т. 8, № 4. С. 774–786.

12. Иоселиани А. Д., Бунина М. А. Фейк и фейк-ньюс как инструменты влияния на формирование общественного мнения // Век глобализации. 2023. № 2. С. 125–135.

13. Симонова Е. В. Фейк как вызов цифрового медиапространства // Образование и наука без границ: фундаментальные и прикладные исследования. 2022. № 15. С. 65–69.

14. Сегал Н. А., Мищенко А. Н., Уварова И. В. Новые слова и значения в русском языке XXI века (на примере языковой единицы «фейк») // Вестник Южно-Уральского государственного университета. Сер.: Лингвистика. 2022. Т. 19, № 3. С. 35–41.

15. Чернышева А. В., Радомысльский М. С. Фейк: идентичность личности в рамках сетевой культуры или игровая мистификация? // Научный потенциал. 2022. № 3. С. 106–111.

16. Шестак Л. А. Политическая лингвистика: фрейм события и фейк-ньюс // Cross-Cultural Studies: Education and Science. 2018. Т. 3, № 3. С. 194–199.

17. Боты приблизились к россиянам по генерации трафика в интернете // Газета. Ru. 2023. URL: https://www.gazeta.ru/tech/news/2023/06/15/20670158.shtml (дата обращения: 09.01.2025).

18. Чуйко А. А. Проблемы установления административной ответственности за правонарушения в сфере распространения фейк-ньюс // Современный юрист. 2022. № 4. С. 74–83.

19. Почему Telegram не заблокировали за год // Рамблер. 2023. URL: https://news.rambler.ru/internet/42111935-pochemu-rossiyskie-vlasti-za-tselyy-god-ne-smogli-zablokirovat-telegram/ (дата обращения: 09.01.2025).

20. Роскомнадзор решил снять ограничения на работу Telegram в России // РБК. 2020. URL: https://www.rbc.ru/society/18/06/2020/5eeb378c9a7947208c4e62e3 (дата обращения: 09.01.2025).

21. История блокировки Telegram в России // ТАСС. 2023. URL: https://tass.ru/info/8761201 (дата обращения: 09.01.2025).

22. What is IPFS? // BeInCrypto. 2023. URL: https://beincrypto.com/learn/what-is-ipfs/ (дата обращения: 09.01.2025).

23. Что такое Nostr? // IShosting. 2023. URL: https://blog.ishosting.com/ru/what-is-nostr (дата обращения: 09.01.2025).

24. Join Mastodon: официальный сайт. URL: https://joinmastodon.org/ (дата обращения: 09.01.2025).

25. Поздняков Е. И. Гражданское общество как субъект противодействия фейк-ньюс в системе информационной безопасности России и Китая // Гражданин. Выборы. Власть. 2022. № 4. С. 170–178.

26. Проверено. Медиа : официальный сайт. URL: https://provereno.media/ (дата обращения: 09.01.2025).