

НАУЧНАЯ СТАТЬЯ

УДК 341.231.14

DOI 10.20310/2587-9340-2022-6-2-151-157

Шифр научной специальности 5.1.1

Проблемы реализации охранительной функции государства в сфере защиты прав человека в цифровом пространстве

© КОЛОСОВА Татьяна Евгеньевна,

старший преподаватель кафедры гражданско-правовых дисциплин, Владимирский филиал ФГБОУ ВО «Российская академия народного хозяйства и государственной службы при Президенте Российской Федерации», Российская Федерация, 600017 г. Владимир, ул. Горького, 59а, ORCID: [0000-0001-7774-2991](https://orcid.org/0000-0001-7774-2991), SPIN-код [8793-7341](https://www.spin-код.рф/8793-7341), РИНЦ AuthorID [1051415](https://elibrary.ru/1051415), tat1892@yandex.ru

Аннотация

Цифровизация всех сфер жизни общества и государства актуализировала проблемы, возникающие при реализации государством его охранительной функции в сфере защиты прав человека. Особая значимость указанных вопросов обусловлена закреплением в Конституции Российской Федерации обеспечения безопасности личности, общества и государства при применении информационных технологий, обороте цифровых данных в качестве самостоятельного предмета ведения Российской Федерации в области обороны и безопасности. Целью настоящего исследования явилось обоснование гипотезы о необходимости принятия государством системных мер, направленных на обеспечение цифровой безопасности личности, общества и государства. Методологическую основу исследования составил диалектический метод познания рассматриваемых социально-правовых явлений. Кроме того, при написании статьи применялись: логический метод, который использовался при определении последовательности изложения материала и формулировании выводов, метод системного анализа, метод моделирования, структурно-функциональный метод, а также метод обращения к выводам теории прав человека. Проанализированы основные направления реализации охранительной функции государства в указанной сфере, к которым автор относит: обеспечение сохранности персональных данных граждан, полученных в результате информационного обмена, и исключение их использования в противоправных целях; соблюдение трудовых и других социальных прав граждан в условиях вовлечения их в новые цифровые формы экономической деятельности, в частности, при взаимодействии с цифровыми платформами; поэтапное и разумное введение цифрового документооборота с сохранением его традиционных форм; обеспечение цифрового суверенитета государства и принятие мер по недопущению использования цифрового информационного пространства для дискриминации российских граждан, дезинформации и деструктивной деятельности. Обоснована необходимость конкретных мер, которые государство может и должно предпринять в рамках реализации его охранительной функции по нейтрализации и снижению рисков в сфере обеспечения и защиты прав человека в цифровом пространстве. Результаты проведенного исследования могут найти свое применение в нормотворческой и правоприменительной деятельности в сфере реализации государственной политики по обеспечению цифровой безопасности, а также в дальнейших научных исследованиях в указанной области права.

Ключевые слова

права человека, цифровизация, цифровые права, цифровой суверенитет, охранительная функция государства

Для цитирования

Колосова Т.Е. Проблемы реализации охранительной функции государства в сфере защиты прав человека в цифровом пространстве // Актуальные проблемы государства и права. 2022. Т. 6. № 2. С. 151-157. DOI [10.20310/2587-9340-2022-6-2-151-157](https://doi.org/10.20310/2587-9340-2022-6-2-151-157)

ORIGINAL ARTICLE

DOI [10.20310/2587-9340-2022-6-2-151-157](https://doi.org/10.20310/2587-9340-2022-6-2-151-157)

Problems of implementation of the state protective function in the field of human rights protection in the digital space

© Tatiana E. KOLOSOVA,

Senior Lecturer of the Civil Law Disciplines Department, Vladimir Branch of the Russian Presidential Academy of National Economy and Public Administration, 59a Gor'kogo St., Vladimir 600017, Russian Federation, ORCID: [0000-0001-7774-2991](https://orcid.org/0000-0001-7774-2991), SPIN-code [8793-7341](https://sp.inm.ac.ru/SPIN/0000000177742991), RSCI AuthorID [1051415](https://www.rsci.org/author/1051415), tat1892@yandex.ru

Abstract

Digitalization of all spheres of life of society and the state has actualized the problems that arise when the state implements its protective function in the field of human rights protection in conditions. The special significance of these issues is due to the consolidation in the Constitution of the Russian Federation of ensuring the security of the individual, society and the state in the application of information technologies, the circulation of digital data as an independent subject of the Russian Federation in the field of defense and security. The purpose of this study was to substantiate the hypothesis of the need for the state to take systemic measures aimed at ensuring the digital security of the individual, society and the state. The methodological basis of the study was the dialectical method of cognition of the considered socio-legal phenomena. In addition, when writing the article, the following methods were used: the logical method used in determining the sequence of presentation of the material and the formulation of conclusions, the method of system analysis, the method of modeling, the structural and functional method, as well as the method of referring to the conclusions of the theory of human rights. The paper analyzes the main directions of the implementation of the protective function of the state in this area, to which the author refers: ensuring the safety of personal data of citizens obtained as a result of information exchange, and the exclusion of their use for illegal purposes; compliance with labor and other social rights of citizens in the conditions of their involvement in new digital forms of economic activity, in particular, when interaction with digital platforms; gradual and reasonable introduction of digital document management while preserving its traditional forms; ensuring the digital sovereignty of the state and taking measures to prevent the use of the digital information space for discrimination against Russian citizens, disinformation and destructive activities. The author substantiates the need for specific measures that the state can and should take as part of the implementation of its protective function to neutralize and reduce risks in the field of ensuring and protecting human rights in the digital space. The results of the conducted research can be applied in standard-setting and law enforcement activities in the field of implementation of the state policy on ensuring digital security, as well as in further scientific research in this area of law.

Keywords

Human rights, digitalization, digital rights, digital sovereignty, the protective function of the state

For citation

Kolosova T.E. Problemy realizatsii okhranitel'noy funktsii gosudarstva v sfere zashchity prav cheloveka v tsifrovom prostranstve [Problems of implementation of the state protective function in the field of human rights protection in the digital space]. *Aktual'nye problemy gosudarstva i prava – Current Issues of the State and Law*, 2022, vol. 6, no. 2, pp. 151-157. DOI [10.20310/2587-9340-2022-6-2-151-157](https://doi.org/10.20310/2587-9340-2022-6-2-151-157) (In Russian, Abstr. in Engl.)

Введение (постановка проблемы)

Вопросы обеспечения безопасности личности, общества и государства при применении информационных технологий, обращении цифровых данных на протяжении длительного времени привлекают внимание как специалистов, так и широкой общественности. Очевидно, что использование цифровых технологий, глобальный информационный обмен наряду с положительным, общественно полезным эффектом зачастую формирует и серьезные риски для общества и государства, приводит к нарушению прав граждан.

Как отмечается в литературе, в условиях превращения информации в товар в сферу такого товарообмена неизбежно вовлекаются персональные данные и сведения о частной жизни, утрачивается или становится небезупречной сетевая нейтральность, возрастают проблемы кибербезопасности, совместимости и защиты конкуренции, да и просто обеспечения в обществе социальной справедливости [1, с. 97].

Приход «цифры» в нашу жизнь неизбежно затронул право и законодательство [2, с. 6]. Впервые в нашей стране комплексное правовое урегулирование вопросы цифровой безопасности получили в Федеральном законе «Об информации, информационных технологиях и о защите информации» от 27 июля 2006 г. № 149-ФЗ¹. Однако уровень их значимости в настоящее время настолько возрос, что они нашли отражение при работе над изменениями и дополнениями в Конституцию России [3].

Законом Российской Федерации о поправке к Конституции Российской Федерации от 14 марта 2020 г. № 1-ФКЗ «О совершенствовании регулирования отдельных вопросов организации и функционирования публичной власти»² пункт «м» статьи 71 Конституции, очерчивающий предмет ведения Российской Федерации в области обороны и безопасности, был дополнен указанием на то, что в предмет ведения государства в указанной сфере включено обеспечение безопасности личности, общества и государства при применении информационных технологий, обороте цифровых данных.

¹ Российская газета. 2006. 29 июля.

² Российская газета. 2020. 16 марта.

Переоценить значимость указанного решения вряд ли возможно, поскольку риски для граждан с точки зрения прав человека, связанные с цифровизацией, развитием информационных технологий и их проникновением во все сферы жизни человека, с каждым годом неизменно повышаются, и, соответственно, актуализируется вопрос их снижения, повышения уровня технологической и юридической защиты цифровых данных, а также роли в этом государства [4, с. 57].

С учетом изложенного, чрезвычайно важным направлением реализации охранительной функции современного российского государства является обеспечение «цифровой» безопасности граждан, а также защита их прав в цифровом пространстве.

Результаты исследования

В современной юридической литературе под охранительной функцией государства понимают публично-властную деятельность государства, обусловленную его сущностью, проявляющую его ценность и социальное назначение, осуществляемую в целях предотвращения и нейтрализации угроз безопасности общества [5, с. 13-14].

При этом не вызывает никаких сомнений, что одним из ключевых компонентов в структуре указанной функции государства является охрана и защита прав и свобод личности.

Учитывая, что процессы цифровизации проникают абсолютно во все сферы социальных отношений, в современной литературе в качестве относительно обособленной группы прав человека все чаще выделяют «цифровые» права, под которыми понимают права человека, связанные с использованием современных цифровых технологий и функционированием в цифровой среде [6, с. 12-13].

К ключевым «цифровым» правам граждан следует отнести право на доступ к сети Интернет, которое, в свою очередь, складывается из права на свободный доступ к содержащейся в ней информации, а также права на обеспечение необходимой для этого инфраструктурой и информационно-коммуникационными технологиями; право на неприкосновенность персональных данных, предоставляемых, передаваемых и хранящихся в цифровой форме, право на защиту от кибератак, право на «цифровое забвение».

В настоящей работе мы попытаемся обозначить основные риски, с которыми сталкивается государство, реализуя охранительную функцию в сфере обеспечения прав и свобод человека в цифровой сфере, а также наметить основные направления их нейтрализации.

Одним из главных рисков в указанной сфере, с которыми столкнулся современный мир вообще и Россия в частности, является неконтролируемый сбор информации о гражданах, которые в условиях тотальной цифровизации неизбежно становятся участниками информационного обмена. Так, современные технологии позволяют в кратчайшие сроки аккумулировать и анализировать колоссальные объемы информации, касающиеся абсолютно всех сфер жизни человека: места проживания, работы, маршрутов передвижения, социальных связей, финансовых активов, склонностей и взглядов, состояния здоровья, биометрических данных и т. д.

Очевидно, что в случае бесконтрольного обращения указанные массивы данных могут быть использованы в абсолютно любых целях. Самая безобидная из них – персонализированная реклама, навязывание товаров и услуг на основе выявленных личных предпочтений. При этом, разумеется, субъекты экономической деятельности, использующие указанные данные, руководствуются отнюдь не интересами и благополучием граждан-потребителей, а преследуют исключительную цель получения максимальной прибыли.

В то же время все чаще имеют место факты использования таких данных в криминальных целях, при совершении, прежде всего, корыстных преступлений, связанных с хищением денежных средств, находящихся на банковских счетах граждан, обслуживаемых электронным способом. Так, согласно экспертным данным, только за 2021 г. ущерб от так называемых «киберпреступлений» составил 90 млрд рублей³.

Наряду с посягательствами на имущественные права граждан, собранные цифровые

данные активно используются и для других противоправных действий – цифровой дискриминации, нарушения неприкосновенности частной жизни, посягательств на половую свободу и неприкосновенность, в том числе несовершеннолетних, деятельности деструктивных сект и сообществ и т. д.

При этом в литературе обоснованно отмечается, что регулирование государством исключительно сбора данных не сможет остановить получение и применение персональных данных для манипуляции и цифровой дискриминации. Необходима четко выработанная государственная политика по регламентации способов использования «чувствительных» типов персональных данных, например, запрет на использование любых данных о болезнях, психических отклонениях, беременности, личных семейных и родственных обстоятельствах, запрет на любой анализ поведения и использование личных данных несовершеннолетних и т. д.

Обоснованные опасения вызывают и процессы так называемой «уберизации» (от наименования фирмы “Uber”) экономики, которые состоят в том, что работник, который с точки зрения трудового законодательства выступает в роли свободного агента, самозанятого, вступает в фактические трудовые отношения не с конкретным работодателем, а с определенной цифровой платформой, которая по существу выступает лишь информационным посредником между заказчиками и поставщиками услуг. Подобная система создает колоссальные риски нарушения трудовых прав граждан, по сути, полностью лишая работников, вовлеченных в подобные экономические отношения, социальных гарантий, предусмотренных трудовым законодательством.

С учетом изложенного полагаем, что в рамках реализации охранительной функции государства законодателю следует предпринять безотлагательные меры по внесению изменений в трудовое законодательство, направленных на урегулирование отношений работников с информационными посредниками в целях обеспечения трудовых прав и социальных гарантий граждан, занятых в указанной сфере.

Заслуживает упоминания и проблема тотальной цифровизации документооборота

³ Эксперт оценил ущерб от киберпреступлений в России в 2021 году. URL: <https://ria.ru/20211222/kiberprestupleniya-1764832102.html> (дата обращения: 18.02.2022).

и, особенно, личных документов граждан, предоставляющих либо подтверждающих их права. У нас не вызывает сомнений тот факт, что человечество рано или поздно придет к полному отказу от изготовления документов на материальных носителях, однако, мы также убеждены и в том, что существующий в настоящее время уровень защиты цифровых данных не позволяет принять такое решение не только незамедлительно, но и в обозримом будущем. Обусловлено это целым рядом факторов. Во-первых, легкостью тиражирования и фальсификации электронных документов, что существенно увеличит возможность их использования в вышеприведенных противоправных целях. Во-вторых, как программная, так и материальная составляющие электронных хранилищ информации на данный момент не обладают необходимым уровнем долговечности и надежности. Так, существующие физические носители цифровой информации крайне недолговечны и редко служат дольше 10–15 лет, в то время как программы обработки и хранения информации обновляются еще быстрее. Что же касается «облачных» технологий, за которыми, безусловно, будущее, то и они в настоящее время далеко несовершенны. При этом с учетом складывающейся в последние годы геополитической обстановки следует учитывать, что подавляющее большинство дата-центров, обеспечивающих хранение таких данных, расположены за пределами нашей страны, что, в случае неблагоприятного развития международной обстановки, может привести к полной утрате доступа к ним российских обладателей и пользователей хранящейся в них информации.

С учетом изложенного, на современном этапе нам представляются разумными предложения по обязательному сохранению в среднесрочной перспективе «гибридного» электронно-бумажного хранения и оборота документов, особенно в части документов, содержащих персональные данные граждан, с признанием подлинником таких документов исключительно их исполнения на материальном носителе.

Наконец, наиболее острой и актуальной в условиях все нарастающего санкционного давления на нашу страну и все обостряющейся внешнеполитической обстановки ста-

новится проблема обеспечения национального цифрового суверенитета, под которым понимают исключительную прерогативу государств самостоятельно и независимо определять внутренние и внешние интересы в цифровой сфере и проводить соответствующую информационную политику; распоряжаться национальными информационными ресурсами и формировать собственную инфраструктуру информационного пространства; гарантировать электронную и информационную безопасность российских граждан, общества и государства. При этом в качестве необходимых средств достижения такого рода суверенитета может быть рекомендовано создание соответствующих регулятивных механизмов, прежде всего, национальных технических стандартов и специального правового режима, создание и использование защищенных от внешнего воздействия аппаратных и программных средств связи отечественного производства, в том числе создание отечественной системы дата-центров, а также способов доведения информации до конечного потребителя, государственно-частное партнерство, которое особенно важно для контроля над сбором, обработкой, хранением и использованием больших массивов данных отечественных пользователей. Кроме того, важнейшей составляющей цифрового суверенитета государства, который бы обеспечивал соблюдение соответствующих прав российских граждан, должно стать создание эффективного механизма «очистки» внутренней виртуальной среды от нежелательной или вредоносной информации, а также инструментов противодействия интегрированным в импортируемый информационный продукт враждебным социально-политическим, историческим, религиозным, нравственно-культурным и другим идеологическим установкам⁴.

Особую тревогу вызывает все возрастающее влияние транснациональных цифровых корпораций, которые в своей деятельности преследуют не только экономические, но и, зачастую, политические цели, связан-

⁴ Цифровая трансформация и защита прав граждан в цифровом пространстве: доклад Совета при Президенте Российской Федерации по развитию гражданского общества и правам человека. М., 2021. С. 49-50.

ные с оказанием идеологического воздействия на население различных государств в целях изменения их мировоззрения, системы ценностей и, в итоге, приведение к власти лояльных им политических сил. Так, крупнейшие зарубежные глобальные цифровые платформы и социальные сети, оперирующие в нашей стране, – Google, Meta** (признана в России экстремистской организацией и запрещена) (Facebook* (социальная сеть, признанная экстремистской и запрещенная на территории Российской Федерации)), Twitter, Instagram* (социальная сеть, признанная экстремистской и запрещенная на территории Российской Федерации), TikTok, YouTube все чаще становятся инструментом деструктивного идеологического воздействия на российских граждан, доведения до них недостоверной информации, а также дискредитации нашей страны и ее граждан в глазах мирового сообщества.

Подобные вопиющие действия являются несомненным открытым посягательством на цифровой суверенитет нашей страны и требуют незамедлительного применения ответных мер со стороны государства в рамках реализации его охранительной функции.

Так, в ответ на беспрецедентные действия компания Meta** (признана в России экстремистской организацией и запрещена), которая в свете проводимой Российской Федерацией специальной военной операции в связи с ситуацией в Луганской Народной Республике и Донецкой Народной Республике разрешила призывы к насилию в социальных сетях Facebook* и Instagram* (социальные сети, признанные экстремистскими и запрещенные на территории Российской Федерации) в отношении российских граждан, Роскомнадзор принял решение об ограничении доступа к социальной сети Instagram* (социальная сеть, признанная экстремистской и запрещенная на территории Российской Федерации)⁵.

Указанные меры, принимаемые государством, в определенной степени ограничивают «цифровые» права граждан – пользователей указанной социальной сети, одна-

ко, безусловно, являются соразмерными и необходимыми в целях обеспечения безопасности государства, общества, а также права российских граждан на защиту от дискриминации. Более того, полагаем, что в условиях информационной войны, которая по существу была развязана в отношении нашей страны со стороны США и ряда примкнувших к ним государств, подобные меры должны стать системными, а основания и порядок их применения должны получить четкое урегулирование на законодательном уровне.

Заключение

Резюмируя вышеизложенное, отметим, что на сегодняшнем сложнейшем этапе развития российского государства в условиях проникновения процессов цифровизации во все сферы жизнедеятельности общества одним из ключевых направлений реализации охранительной функции государства становится принятие исчерпывающих мер, направленных на обеспечение прав человека в цифровом пространстве. Полагаем, что основными точками приложения государством таких усилий должны стать обеспечение сохранности персональных данных граждан, полученных в результате информационного обмена, и исключение их использования в противоправных целях; соблюдение трудовых и других социальных прав граждан в условиях вовлечения их в новые цифровые формы экономической деятельности; поэтапное и разумное введение цифрового документооборота с сохранением его традиционных форм; обеспечение цифрового суверенитета государства и принятие мер по недопущению использования цифрового информационного пространства для дискриминации российских граждан, дезинформации и деструктивной деятельности. При этом, учитывая взрывные темпы развития процессов цифровизации, не вызывает сомнений тот факт, что проблематика их воздействия на сферу прав человека призвана стать важнейшим направлением научного поиска в области права.

⁵ Об ограничении доступа к социальной сети Instagram*. URL: <https://rkn.gov.ru/news/rsoc/news74180.htm> (дата обращения: 18.03.2022).

Список источников

1. Архипов В.В., Наумов В.Б. Сквозные правовые проблемы Интернета вещей и пределы права: российская перспектива // Труды Института государства и права РАН. 2018. Т. 13. № 6. С. 94-123.
2. Грудцына Л.Ю. Цифровое будущее права: к вопросу об аддитивных технологиях // Журнал российского права. 2021. № 7. С. 5-14.
3. Лебедева Ю.Н. Новое в разграничении вопросов ведения России // Государственная власть и местное самоуправление. 2021. № 9. С. 20-21.
4. Хабриева Т.Я., Клишас А.А. Тематический комментарий к Закону Российской Федерации о поправке к Конституции Российской Федерации от 14 марта 2020 г. № 1-ФКЗ «О совершенствовании регулирования отдельных вопросов организации и функционирования публичной власти». М.: Норма, ИНФРА-М, 2020. 240 с.
5. Пожарский Д.В. Охранительная функция государства: теоретико-методологические проблемы: дис. ... д-ра юрид. наук. М., 2014. 418 с.
6. Варламова Н.В. Цифровые – новое поколение прав человека? // Труды Института государства и права РАН. 2019. Т. 14. № 4. С. 9-46.

References

1. Arkhipov V.V., Naumov V.B. Skvoznnyye pravovyye problemy Interneta veshchey i predely prava: rossiyskaya perspektiva [Cross-cutting Legal Problems of the Internet of Things and the Limits of Law: Russian Perspective]. *Trudy Instituta gosudarstva i prava RAN* [Works of the Institute of State and Law of the Russian Academy of Sciences], 2018, vol. 13, no. 6, pp. 94-123. (In Russian).
2. Grudtsyna L.Y. Tsifrovoye budushcheye prava: k voprosu ob additivnykh tekhnologiyakh [Digital future of law: to a question on additive technologies]. *Zhurnal rossiyskogo prava – Journal of Russian Law*, 2021, no. 7, pp. 5-14. (In Russian).
3. Lebedeva Y.N. Novoye v razgranichenii voprosov vedeniya Rossii [New in differentiation of questions of competence of Russia]. *Gosudarstvennaya vlast' i mestnoye samoupravleniye* [State Power and Local Self-Government], 2021, no. 9, pp. 20-21. (In Russian).
4. Khabriyeva T.Y., Klisshas A.A. *Tematicheskiy kommentariy k Zakonu Rossiyskoy Federatsii o popravke k Konstitutsii Rossiyskoy Federatsii ot 14 marta 2020 g. № 1-FKZ «O sovershenstvovanii regulirovaniya ot-del'nykh voprosov organizatsii i funktsionirovaniya publichnoy vlasti»* [Thematic Comment to the Russian Federation Law on Amendment of the Constitution of the Russian Federation on March 14, 2020, № 1-FKZ “On Improvement of Regulation of Individual Issues of Organization and Functioning of Public Authorities”]. Moscow, Norma Publ., INFRA-M Publ., 2020, 240 p. (In Russian).
5. Pozharskiy D.V. *Okhranitel'naya funktsiya gosudarstva: teoretiko-metodologicheskiye problemy: dis. ... d-ra yurid. nauk* [Protective Function of the State: Theoretical and Methodological Problems. Dr. law sci. diss. abstr.]. Moscow, 2014, 418 p. (In Russian).
6. Varlamova N.V. Tsifrovyye – novoye pokoleniye prav cheloveka? [Digital – a new generation of human rights?]. *Trudy Instituta gosudarstva i prava RAN* [Works of the Institute of State and Law of the Russian Academy of Sciences], 2019, vol. 14, no. 4, pp. 9-46. (In Russian).

* Социальные сети Facebook* и Instagram* (принадлежат Meta**) признаны экстремистскими и запрещены на территории Российской Федерации. 21 марта 2022 г. компания Meta** признана экстремистской организацией, деятельность холдинга в России запрещена.

Статья поступила в редакцию / The article was submitted 21.03.2022
Одобрена после рецензирования / Approved after reviewing 23.05.2022
Принята к публикации / Accepted for publication 27.05.2022



Работа доступна по лицензии [Creative Commons Attribution \(«Атрибуция»\) 4.0](https://creativecommons.org/licenses/by/4.0/) Всемирная