DOI 10.37882/2223–2974.2023.04.27

ВИДЫ ОТРИЦАНИЯ НЕДОБРОСОВЕСТНОГО ПОВЕДЕНИЯ В СФЕРЕ ИСПОЛЬЗОВАНИЯ ЦИФРОВЫХ ПРАВ

TYPES OF DENIAL OF BAD FAITH CONDUCT IN THE FIELD OF DIGITAL RIGHTS

Z. Sedova

Summary. Denial of bad faith conduct as a method of legal regulation of relations develops the principle of good faith. One type of such denial is the inadmissibility of the abuse of digital technologies, the prohibitions of specific types of which are still in the process of forming in the law as court decisions emerge. On the example of existing judicial practice in disputes about the violation of digital rights and causing harm by using the means and capabilities of information and telecommunications network «Internet», the legislator can systematize unfair cyber practices and establish norms-prohibitions for the types of digital misconduct identified in the current historical period even today. One of the most common type of breach in cyberspace is the abuse of consumer personal data, the way to protect which is to create appropriate digital rights management systems. Digitalization of most spheres of life contributes to the emergence of new legal terms: «digital bad faith conduct» or «cyber-bad-faith», «legal escapism» — requiring a clear definition for the purpose of developing new legal remedies against violations of digital rights.

Keywords: principle of good faith, denial of bad faith conduct, digital rights, digital bad faith conduct, cyber-bad-faith, legal escapism.

Седова Жанна Игоревна
Кандидат юридических наук, Российский государственный университет правосудия
Zhanna.sedova@EL5-energo.ru

Аннотация. Отрицание недобросовестного поведения, как метод правового регулирования отношений, развивает принцип добросовестности. Одним из видов такого отрицания является недопустимость злоупотребления цифровыми технологиями, запреты конкретных видов которых в праве еще находятся в стадии формирования по мере появления решений судов. На примере существующей судебной практики по спорам о нарушении цифровых прав и причинении вреда с использованием средств и возможностей информационно-телекоммуникационной сети «Интернет», уже сегодня законодатель может систематизировать недобросовестные киберпрактики и установить нормы-запреты выявленных в текущем историческом периоде видов цифрового недобросовестного поведения. Одним из распространенных видов нарушений в киберпространстве является злоупотребление персональными данными потребителей, способом защиты которых является создание соответствующих систем управления цифровыми правами. Цифровизация большинства сфер жизнедеятельности способствует появлению новых правовых понятий: «цифровое недобросовестное поведение» или «кибернедобросовестность», «правовой эскапизм», — требующих своего чёткого определения для целей разработки новых правовых средств защиты от нарушений цифровых прав.

Ключевые слова: принцип добросовестности, отрицание недобросовестного поведения, цифровые права, цифровое недобросовестное поведение, кибернедобросовестность, правовой эскапизм.

Повсеместная цифровизация общественных отношений приносит их участникам не только такое благо, как быстроту и удобство реализации прав, перенесенных в виртуальное пространство, закрепление новых прав в связи с появлением новых технологий, но также сопряжена с риском цифрового недобросовестного поведения участников. Недобросовестное поведение может быть направлено на нарушение цифровых прав, отнесенных к IV поколению прав человека [1, с. 48], причинение вреда или получение выгоды обманным путем с использованием цифровых технологий.

Среди распространенных форм злоупотребления цифровыми правами можно выделить:

- нарушение авторских и смежных прав (см. пункт 25 Постановления Пленума Верховного Суда РФ от 19.06.2006 № 15 «О вопросах, возникших у судов при рассмотрении гражданских дел, связанных с применением законодательства об авторских и смежных правах»);
- киберсквоттинг (от англ. «cybersquatting») — злонамеренная регистрация доменных имён, содержащих торговую марку, которая принадлежит другому лицу, с целью их дальнейшей перепродажи или недобросовестного использования; регистрации домена третьим лицом, не являющимся владельцем идентичного или сходного товарного знака с целью недобросовестной конкуренции (см. Постановление ФАС Московского округа от 31.12.2010 № КГ-А40/16995–10 по делу № А40–170684/09–26–1231);
- создание против воли заинтересованного лица дип-фейков (от англ. «deepfake») — технология, применяемой при монтаже видео для наложения лица поверх другого [2];

- незаконное содержание размещаемого провайдерами контента [3];
- перехват смс [4];
- использование интернет-ресурсов для распространения запрещенного контента [5, с. 75–77];
- кибератаки [5, с. 60–94].

Все перечисленные нарушения прав и законных интересов участников цифровых отношений относятся к недобросовестному поведению, в связи с чем можно заявить о формировании нового понятия в праве — «цифровое недобросовестное поведение» или «кибернедобросовестность». Случаи кибернедобросовестности характеризуется сложностью их выявления из-за технической составляющей, так как информационно-цифровые технологии быстро развиваются и обогнали правовое регулирование.

Требования добросовестности в отношениях с использованием цифровых технологий обеспечиваются международным и национальным правом, а также формируемым в ходе саморегулирования [6, с. 230–253] киберправом — обыкновениями и обычаями.

В силу того, что законодательство не успевает реагировать на новые формы злоупотребления цифровыми правами, круг которых постоянно расширяется с развитием технологий, в правоприменительной практике формируются способы противодействия (отрицания) недобросовестному поведению. Отрицание представляет собой метод правового регулирования, основанный на принципах справедливости и добросовестности, выраженный в применении участниками правоотношений и судами способов правового регулирования (запретов, обязываний и дозволений) и соответствующих им правовых средств. Отрицание выступает основой реализации правовых механизмов защиты от недобросовестного поведения во всех сферах правоотношений.

Отрицание недобросовестного поведения, будучи универсальным (применимым в любой отрасли права) методом регулирования отношений, служит утверждению права, что проявляется через «позитивный смысл осознания и реализации права (неотъемлемые права и свободы человека, позитивную правовую ответственность, правовую активность, правовую культуру в смысле уважительного отношения к праву» [7, с. 8–9], а также нивелирует правовой эскапизм.

По мнению Л.В. Козыревой, «на сегодняшний день понятие «эскапизм» не признано в качестве юридического термина» [8, с. 211–212]. Однако следует отметить, что в основе кибернедобросовестности лежит именно правовой эскапизм, означающий любые формы юридически значимого поведения, направленные на избегание как в реальной жизни, так и в киберпространстве: известных и принятых в обществе устоев, ценностей; сложившегося в условиях цивилизации отношения к общезначимым образцам культурного и добросовестного поведения. Такое эскапическое поведение [избегание ценностей] является следствием процессов глобализации, цифровизации, создания виртуальной реальности и характеризуется «амбивалентностью», то есть двойственностью (расщеплением) отношения субъекта к своему же поведению: когда такое поведение вызывает у субъекта одновременно два противоположных к своему поведению отношения (позитивное и негативное). Амбивалентность поведения проявляется у «эскапического субъекта» [8, с. 211–212] также в расщеплении личности на: (1) реальную в социуме и (2) цифровую в киберпространстве, правовой статус которой ещё только разрабатывается,— в связи с чем субъект ощущает разную степень дозволенности поведения. Правильную правовую оценку поведения возможно сформировать только через познание видов отрицания недобросовестного поведения.

Термин «киберпространство», возникший в художественной литературе, уже широко используется источниками права. В частности, «киберпространство» определяется как «Интернет и социальные сети» в Рекомендации № CM/Rec (2019) 1 Комитета министров Совета Европы [9], сам термин «киберпространство» используется в утвержденных Правительством РФ «Прогнозе научно-технологического развития Российской Федерации на период до 2030 года», «Основных направлениях деятельности Правительства Российской Федерации на период до 2024 года» и других документах Минкомсвязи и Минфина России.

Предлагается выделить следующие виды отрицания недобросовестного поведения в сфере использования цифровых прав:

1. **Общие виды отрицания**, которые свойственны не только сфере цифровых правоотношений, являются общеправовыми, но также могут быть применимы в сфере кибербезопасности:

1.1) принцип добросовестности как автономный нормативный способ отрицания. Закрепление в пункте 5 статьи 10 Гражданского кодекса РФ добросовестности достаточно для реагирования судебными органами на недобросовестное поведение даже в отсутствие в праве чётко сформулированной нормы, запрещающей конкретный вид недобросовестного поведения;

1.2) недопустимость поведения, выходящего за нормативные пределы осуществления гражданских прав. Данный способ противодействия недобросовестному поведению может быть

конкретизирован в качестве требований о недопустимости обхода закона; недопустимости злоупотребления правами; недопустимости осуществления гражданских прав исключительно с намерением причинить вред другому лицу; недопустимости использования гражданских прав в целях ограничения конкуренции; недопустимости злоупотребления доминирующим положением на рынке.

2. **Частные виды отрицания** недобросовестного поведения, которые применимы конкретно в сфере цифровых прав: недопустимость злоупотребления цифровыми технологиями (кибернедобросовестности), правовыми средствами достижения которого выступают: блокирование контента; запрет использования алгоритмов, которые могут приводить к дискриминации людей по каким-то признакам; запрет операций по счетам в случае неординарного поведения клиента банка со смартустройством; блокчейн, позволяющий выявлять, например, признаки антиконкурентных соглашений на торгах в режиме онлайн.

Попытка дать определение злоупотреблению цифровыми правами производилась в доктрине. С точки зрения А.Г. и Н.Г. Столетовых, Р.Б. Головкина, понятие «злоупотребление цифровыми правами» невозможно дать без определения «цифровых обязанностей». Так, авторы предлагают определить цифровые обязанности как «меры должного поведения субъектов правоотношений, выраженные цифровыми кодами или обозначениями на основе и в рамках информационных систем, признаваемых законодательством». Под «злоупотреблением цифровыми правами» авторы предлагают понимать «разновидность субъективно-противоправного поведения, выражающегося в умышленном использовании предусмотренных законом цифровых прав и обязанностей в ущерб интересам других субъектов правоотношений» [8, с. 1710–1723]. Использование категории «субъективно-противоправного поведения» не столь удачно, так как не ясно используется ли она в значении поведения, исходящего от субъекта правоотношения и поэтому являющегося субъективным (то есть свойственным субъекту) или противопоставляется объективной оценке противоправности (по аналогии с субъективным и объективным вменением вины недобросовестному лицу).

Злоупотребление цифровыми правами с использованием сети «Интернет», представляющей собой пространство для реализации прав и свобод человека [9], нарушает основополагающие права и свободы участников цифровых отношений. Европейский Суд по правам человека (далее — «**ЕСПЧ**») рассматривает право на доступ в сеть «Интернет» в контексте свободы выражения мнения и свободы информации [10]. А.А. Антопольский, проанализировав постановления ЕСПЧ по делам, затрагивающим право на доступ в сеть «Интернет», пришел к выводу, что такие дела были инициированы жалобами на нарушение следующих статей Европейской Конвенции о защите прав человека и основных свобод от 04.11.1950 (далее — «**ЕКПЧ**»): статьи 8 (право на уважение частной и семейной жизни, жилища и корреспонденции); статьи 10 (свобода выражения мнения); статьи 1 Протокола 1 к ЕКПЧ со ссылкой на нарушения права собственности (в т.ч. интеллектуальной собственности); статьи 6 (право на справедливое судебное разбирательство), статьи 11 (свобода собраний и объединений) и статьи 14 (запрет дискриминации) [11]. Россия не является стороной ЕКЧП с 16.09.2022 (Резолюция ЕСПЧ от 22.03.2022).

Злоупотребление правами в сети «Интернет» может нарушать конституционные права субъектов правоотношений. Судья Конституционного Суда РФ Н.С. Бондарь проанализировал угрозы нарушения конституционных прав личности, которые несет в себе цифровизация [12, с. 25–42]. Хотя Конституция РФ прямо не устанавливает права на защиту персональных данных, данное право вытекает из других защищаемых Конституцией РФ прав: права на свободу, неприкосновенность частной жизни, право на тайну переписки, запрет сбора, хранения, использования и распространения информации о частной жизни лица без его согласия (часть 1 статьи 22, часть 1 статьи 23, часть 2 статьи 23, часть 1 статьи 24 Конституции РФ).

С точки зрения анализа нарушения основополагающих прав личности недобросовестным поведением, интерес представляет дело «Брейер против Германии» [13]. Предметом рассмотрения ЕСПЧ в данном деле была тайна защиты переписки и нарушение статьи 8 ЕКПЧ в случаях, когда содержание переписки хранится операторами сотовых данных и может в любое время быть предоставлено по запросу правоохранительного органа. С точки зрения заявителя, положения статьи 111 закона Германии о связи не содержат необходимого ограничения возможного последующего использования персональных данных, доступ третьих лиц к которым является автоматическим, то есть информация предоставляется не по запросу правоохранительного органа в отношении, например, подозреваемого за определенный период времени, а ко всему объему частной переписки, что является непропорциональным. ЕСПЧ признал подобное хранение личных данных оператором связи пропорциональным и необходимым в демократическом обществе (параграфы 108–109 указанного решения), и не нарушающим ЕКПЧ, тем самым поддержав хранение всего объема персональных данных независимо от того, существует ли разумное подозрение в отношении их субъекта.

Судья ЕСПЧ К. Ранзони не поддержал позицию, выраженную в данном решении ЕСПЧ, указав на нарушение баланса частных и публичных интересов в пользу последних в своем особом мнении. С точки зрения К. Ранзони, недопустимо хранение всего объема информации, принадлежащей субъекту персональных данных без предварительного выделения информации, необходимой для уголовного преследования, а гарантии защиты нельзя назвать эффективными до тех пор, пока доступ к персональным данным может быть получен автоматически. В противном случае лицо, согласившись на обработку своих данных цифровым способом, заведомо лишалось бы права на конфиденциальность.

Особое мнение судьи Конституционного суда или Европейского Суда по правам человека — это вид отрицания недобросовестного поведения в сфере цифровых отношений на уровне реализации основополагающих, конституционных прав и свобод личности, основанный на индивидуальном регулировании.

Необходимо более подробно рассмотреть виды злоупотребления цифровыми правами и способы противодействия такому недобросовестному поведению в сферах: (1) защиты персональных данных потребителей в цифровой среде; (2) нарушений, осуществленных с использованием цифровых платформ; (3) использования электронной подписи недобросовестными субъектами правоотношений.

В связи с глобальной цифровизацией возникает необходимость защиты прав потребителей в цифровой среде и отрицания злоупотреблений, лишающих потребителей их разумных ожиданий и нарушающих их права. Системы управления цифровыми правами (**УЦП**) — это любые технологии, способные контролировать доступ к цифровому контенту и предотвращающие или ограничивающие действия, не санкционированные правообладателем [14]. Системы УЦП в потребительских отношениях — это программные инструменты, встроенные в приобретаемые потребителем приложение или программу, предназначенные для настройки использования цифровых файлов с целью защиты интересов правообладателей. Технологии УЦП позволяют управлять доступом к данным, возможностью и длительностью их просмотра, изменением, копированием и сохранением.

Часто договоры, защищенные УЦП, имеют недобросовестным образом «скрытые» и неочевидные потребителю положения (например, гиперссылки, расположенные неочевидным образом на веб-странице с использованием мелкого шрифта). Многие программы, защищенные УЦП, являются предметом лицензионных соглашений с конечным пользователем и потребитель часто не читает такие лицензионные условия, так как имеет дело с договором присоединения. Подобное использование УЦП без надлежащего информирования субъекта персональных данных о возможном использовании предоставленных им данных можно рассматривать как навязывание односторонних договорных условий. Пользователи, с одной стороны, получают доступ к цифровому контенту, защищенному технологической мерой защиты, но поставщик контента на практике навязывает договорное положение посредством click-wrap-соглашения, заключаемого путем щелчка мышью по клавише «я согласен», если это сопровождается текстом такого договора и описанием ценовых и иных условий сделки [15], (то есть получения согласия субъекта персональных данных с применяемой политикой), что может повлечь использование персональных данных, на которое потребитель не дал бы осознанного согласия [16].

Э.В. Талапина выявила вызванную развитием цифровых технологий тенденцию стирания граней между отраслями права: в условиях глобальной сетевой структуры современного общества различия между публичным и частным международным правом нивелируются. Э.В. Талапина считает, что поскольку информация и технологии содержатся в каждой отрасли права, то они, как общий знаменатель, определяют единую логику права и снижают ценность отраслевого деления в принципе [17]. Развитие мировой Интернет-сферы, по сути, поставило право перед необходимостью адаптации всей системы и структуры права к цифровым технологиям. Объективные изменения, за которыми правовое регулирование не успевает, связаны в первую очередь с началом вытеснения категории «территория» термином «пространство», а также с массовым заключением внешнеэкономических и внутринациональных сделок нажатием («кликаньем») одной кнопки в компьютере или телефоне («one click» технологии). Даже цифровая подпись, вытесняющая собственноручную подпись физического лица, уже тоже устарела по сравнению с «one click» технологиями.

Необходимость урегулирования защиты персональных данных потребителей в цифровой среде была поставлена на повестку Европейского Союза в 2015 году, в ходе обсуждения Директивы о некоторых аспектах, касающихся контрактов на поставку цифрового контента (далее — «**Директива**») [20]. Директива посвящена фундаментальному праву на защиту персональных данных, предусмотренному в Уставе Европейского Союза (статья 8 Устава, ст. 1 (2) Директивы), и обеспечению того, чтобы обработка персональных данных происходила «законно, справедливо и прозрачно» (статья 5 (1) (a) Директивы).

Использование персональных данных ограничено «правомерным основанием» такого использования (см. статьи 6 (1) (a), 6 (1) (b) и 6 (1) (f) Директивы), к которому Директива относит, в том числе, необходимость исполнения договора, законный интерес и наличие согласия субъекта персональных данных. При этом основания законности не должны наличествовать кумулятивно в каждом конкретном случае использования данных, а владелец персональных данных может их обрабатывать без получения предварительного согласия, если эта обработка необходима для исполнения договора с субъектом данных. Таким образом, перечень законных оснований использования информации, принадлежащей субъекту данных, необходимо сделать если не кумулятивным, то хотя бы признать необходимость совместного удовлетворения критериев «необходимости исполнения договора» и дачи согласия субъекта данных на их использование. Если в случае с основанием «законный интерес в использовании данных» можно предположить, что законный интерес в использовании данных будет иметь орган государственной власти или лицо, считающее свое право нарушенным, что является достаточным для доступа к данным, то использование основания «необходимость исполнения договора» в качестве единственно достаточного для использования персональных данных является необоснованным и влечет риски для потребителя цифрового контента.

В связи с этим Директива ввела принцип информированного согласия (статья 6 (1) (a) Директивы), который выступает правовой основой законной обработки персональных данных. При этом информация о форме использования персональных данных должна быть легко доступной и ясной [21]. В преамбуле Директивы рекомендуется предоставлять информацию о потенциальном использовании персональных данных потребителя наглядным образом через веб-сайт, чтобы не допускать использование неочевидных гиперссылок поставщиками цифровых услуг и отсутствия ясности в отношении того, кем и с какой целью собираются персональные данные, например, в случае онлайн-рекламы [20].

Возникает вопрос: каковы механизмы противодействия (отрицания) злоупотреблению в сфере обработки персональных данных потребителей цифровых услуг? Директивой ЕС о цифровом контенте от 20.05.2019 (далее — «**Директива 2019/770**») [22] в качестве таковых установлены право на замену товара или возмещение уплаченных денежных средств. Эти средства защиты применяются в случае, если раскрытая продавцом информация о цифровом контент-продукте, обрабатывающем персональные данные, не совпадает с фактическими характеристиками проданного товара, например, если приложение собирает и делится с третьими лицами информацией в большем объеме, нежели об этом был предупрежден покупатель, или не обеспечивает достаточный уровень безопасности информации потребителя (статьи 6 и 12 Директивы 2019/770).

Защищенность персональных данных пользователей цифрового контента также подвергается угрозе воздействия парсинга — автоматизированного сбора информации (в том числе, персональных данных) с интернет-ресурса с помощью роботизированной программы (бота). Ключевой вопрос заключается в законности и необходимости получения согласия на такой сбор информации из общедоступной базы данных. В силу части 4 статьи 7 Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (далее — «**Закон № 149-ФЗ**»), если часть базы данных размещена ее изготовителем в открытом доступе в сети «Интернет», то она признается «общедоступной информацией, размещаемой в форме открытых данных». Согласно части 2 статьи 7 Закона № 149-ФЗ ограничивается только распространение такой информации, но не ее использование. Стоит учитывать, что правовой режим баз данных, определенный параграфом 5 главы 71 Гражданского кодекса РФ, распространяет правовую защиту только на базу данных, являющуюся результатом интеллектуальной деятельности, а не на любую базу данных в техническом смысле. Перенос части содержания защищаемой базы данных на другой информационный носитель и последующее ее использование признается нарушением смежных прав правообладателя (пункт 1 статьи 1334 Гражданского кодекса РФ).

Дело «ВКонтакте против Дабл» [23] было основано на предполагаемом нарушении компанией ООО «Дабл» прав на базу данных, принадлежащую компании ООО «В Контакте». Нарушение состояло якобы в том, что ООО «Дабл» парсило данные социальной сети, размещенные в открытом доступе, и использовало их в собственных коммерческих целях. ООО «В Контакте» основывало свои требования о недопустимости сбора информации о пользователях соцсети и использования их персональных данных на том, что база данных ООО «В Контакте» «является результатом существенных финансовых, материальных, организационных или иных вложений (инвестиций) изготовителя базы в их создание», соответственно, подлежит защите как объект смежных прав. Девятый арбитражный апелляционный суд на основании заключения о функционировании базы данных пришел к выводу о доказанности факта понесенных существенных затрат на создание спорной базы данных и признал базу данных объектом смежных прав, защищаемым статьями 1334, 1335.1 Гражданского кодекса РФ, а требования истца обоснованными (см. Постановление Девятого арбитражного апелляцион-

ного суда от 06.02.2018 № 09АП-61593/2017-ГК по делу № А40–18827/17). Ответчик решение апелляционного суда оспорил, но дело завершилось подписанием мирового соглашения, утвержденного Судом по интеллектуальным правам, часть 3 которого предусматривает, что: «стороны совместно обязуются соблюдать права пользователей социальной сети «ВКонтакте» и выстраивать свою деятельность с учетом принципов добросовестности в коммерческих отношениях и уважения прав участников гражданского оборота» (см. Постановление Суда по интеллектуальным правам от 23.09.2022 № С01–201/2018 по делу № А40–18827/2017).

Важной задачей современного общества является обеспечение кибербезопасности и вопросы защиты прав человека в цифровой сфере. Цифровое недобросовестное поведение или кибернедобросовестность — это поведение, направленное на нарушение цифровых прав и (или) причинение вреда другим участникам цифровых правоотношений с использованием средств и возможностей информационно-телекоммуникационной сети «Интернет». При этом цифровыми средствами защиты от недобросовестного поведения при использовании цифровых технологий являются: (1) блокчейн или его аналог «Мастерчейн» как инструменты защиты от недобросовестных действий при выдаче цифровых банковских гарантий (в Республике Беларусь принят ряд нормативных правовых актов, регулирующих использование технологий блокчейна) [24, с. 39–47]; (2) использование таких средств идентификации субъекта цифровых прав для устранения «негативных качеств поведения субъектов цифрового общения», как наделение субъекта кодом идентификации, «введение процедуры верификации с ограничительными мерами по отношению к субъектам, которые отказываются предоставлять свои данные интернет-провайдеру» [25, с. 1034]; (3) регулирование цифрового поведения пользователей интернет-сети и ограничение «антисоциального цифрового поведения», а также влияния с помощью цифровых технологий на поведение больших групп людей, используя информацию, адаптированную к психологическим потребностям целевых аудиторий [5, с. 75–77]; (4) пределы использования Больших данных («Dig data»). Указанные цифровые средства защиты от кибернедобросовестности требуют срочного надлежащего правового закрепления.

ЛИТЕРАТУРА

1. Азаров А.Я. Введение в теорию прав человека // Азаров А., Ройтер В., Хюфнер К. Права человека: Международные и российские механизмы защиты. М.: Московская школа прав человека. 2003.
2. Что такое DeepFake? Стоит ли беспокоиться? / Сайт: TechStation. 04.09.2019. URL: https://zen.yandex.ru/media/id/5d6948212f1e4400ae5a62fc/chto-takoe-deepfake-stoit-li-bespokoitsia-5d6f6f9baad43600adce96c8.
3. Сулейманов М. Ответственность провайдеров за правонарушения в киберпространстве. // Сайт: Zakon.ru. 28.02.2012. URL: https://zakon.ru/blog/2012/2/28/otvetstvennost_provajderov_za_pravonarusheniya_v_kiberprostranstve.
4. Бунина В. Перехватят SMS, заберут деньги: хакеры готовят атаку на счета россиян // Сайт: Газета.ru. 09.04.2021. URL: https://www.gazeta.ru/tech/2021/04/09/13552070/may_attack.shtml.
5. Погожина И.Н., Подольский А.И., Идобаева О.А., Подольская Т.А. Цифровое поведение и особенности мотивационной сферы интернет-пользователей: логико-категориальный анализ. Обзор зарубежных исследований. // Вопросы образования/Educational Studies Moscow. 2020. № 3. С. 60–94.
6. Мажорина М.В. Киберпространство и методология международного частного права // Право. Журнал Высшей школы экономики. 2020. № 2. С. 230–253.
7. Бирюков С.В. Отрицание права как теоретико-правовая категория / Дис. на соискание ученой степени кандидата наук: 12.00.01. Омский государственный университет имени Ф.М. Достоевского. 2009. С. 8–9.
8. Козырева Л.В. Правовой взгляд на реальности эскапического субъекта. // Евразийский юридический журнал № 7 (74) 2014. С. 211–212.
9. Рекомендация № CM/Rec (2019) 1 Комитета министров Совета Европы «О предотвращении сексизма и борьбе с ним» (принята 27.03.2019 на 1342-м заседании представителей министров) // Бюллетень Европейского Суда по правам человека. Российское издание. 2019. № 10.
10. Толстик В.А. Обзор Международной научно-практической конференции «Противодействие злоупотреблению правом: теория, практика, техника (X Бабаевские чтения)» (г. Нижний Новгород, 23–24 мая 2019 г.) // Актуальные проблемы экономики и права. 2019. Т. 13, № 4. С. 1710–1723. DOI: http://dx.doi.org/10.21202/1993–047X.13.2019.4.1710–1723.
11. Саликов М.С., Несмеянова С.Э. К постановке проблемы об особенностях реализации и защиты прав и свобод человека в сети Интернет // Российское право: образование, практика, наука. 2019. // URL: https://cyberleninka.ru/article/n/k-postanovke-problemy-ob-osobennostyah-realizatsii-i-zaschity-prav-i-svobod-cheloveka-v-seti-internet.
12. Постановление ЕСПЧ от 09.02.2021 по делу «Рамазан Демир против Турции» («Ramazan Demir v. Turkey») (жалоба № 68550/17) // Бюллетень Европейского Суда по правам человека. Российское издание, 2021, № 8; Постановлении ЕСПЧ от 18.06.2019 по делу «Мехмет Решит Арслан и Орхан Бингел против Турции» («Mehmet Resit Arslan and Orhan Bingol v. Turkey») (жалоба № 47121/06 и другие жалобы) // Бюллетень Европейского Суда по правам человека. Российское издание, 2020, № 1.
13. Антопольский А.А. Права человека и Интернет: практика Европейского суда по правам человека // Труды Института государства и права Российской академии наук. 2019. URL: https://cyberleninka.ru/article/n/prava-cheloveka-i-internet-praktika-evropeyskogo-suda-po-pravam-cheloveka.

14. Бондарь Н.С., Информационно-цифровое пространство в конституционном измерении: из практики Конституционного Суда Российской Федерации // Журнал российского права, 2019, № 11, С. 25–42.
15. Breyer v. Germany, no. 50001/12, 30 January 2020 // URL: https://www.statewatch.org/media/documents/news/2020/feb/echr-breyer-v-germany-sim-card-privacy-judgment-30–1–20.pdf.
16. Stefan Bechtold. From Copyright to Information Law: Implications of Digital Rights Management, in Security And Privacy In Digital Rights Management, 213, 214–15 (Tomas Sander ed., 2002). // URL: http://www.jura.uni-tuebingen.de/bechtold/pub/2002/DRM_Information_Law. pdf.
17. Талапина Э.В. Право и цифровизация: новые вызовы и перспективы // Журнал российского права. 2018. № 2. // URL: https://cyberleninka.ru/article/n/pravo-i-tsifrovizatsiya-novye-vyzovy-i-perspektivy.
18. Об особенностях click-wrap-соглашений. // Сайт: Роспотребнадзор. 05.11.2020. URL: https://www.rospotrebnadzor.ru/about/info/news/news_details.php? ELEMENT_ID=15893.
19. Jacques de Werra, Moving Beyond the Conflict Between Freedom of Contract and Copyright Policies: In Search of a New Global Policy for On-Line Information Licensing Transactions: A Comparative Analysis Between U.S. Law and European Law, 25 COLUM.J.L.&ARTS 239, 244 (2003).
20. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (GDPR).
21. Directive 93/13 on unfair terms in consumer contracts, O.J. 1993, L 95/29). The GDPR refers to the Unfair Contract Terms Directive in Recital 42.
22. Directive (EU) 2019/770 of the European Parliament and of the Council of 20 May 2019 on certain aspects concerning contracts for the supply of digital content and digital services.
23. Брезгулевская Л. ВКонтакте & Дабл: дело о запрете продажи данных пользователей базы данных соцсети // Сайт: Закон.Ру, 2018. URL: https://zakon.ru/blog/2018/7/12/v_kontaktedabl_delo_o_zaprete_prodazhi_dannyh_polzovatelej_bazy_dannyh_socseti.
24. Михеева И.Е. Блокчейн как инструмент защиты от недобросовестных действий при выдаче цифровых банковских гарантий. // Актуальные проблемы российского права. 2020. Т. 15. № 17 (116) июль. С. 39–47.
25. Жемеров В.В. Цифровые права человека: теоретические и практические проблемы. // Российская юстиция в XXI веке: реалии, проблемы, перспективы. С. 1026–1036.

Российский государственный университет правосудия