

МУНИЦИПАЛЬНОЕ УЧРЕЖДЕНИЕ КУЛЬТУРЫ
«ИЖМОРСКАЯ ЦЕНТРАЛИЗОВАННАЯ БИБЛИОТЕЧНАЯ СИСТЕМА»
Ижморская центральная библиотека им. М.С.Прудникова
Сектор информации, маркетинга и рекламы

СЕТЕВОМУ ОБЩЕСТВУ – СЕТЕВОЕ ПРАВО

Д а й д ж е с т

пгт.Ижморский,2022

Сетевое право — это учение о сетях, представляющих собой систему норм, регулирующую общественные отношения, в электронных сетях различных видов и (или) с помощью электронных сетей, закрепляющих правовое содержание построения и функционирования сети.

Система права, являясь явлением объективного характера, формируется не произвольно, а зависит от сложившейся в государстве системы общественных отношений. Каждому типу государства на определенном этапе развития соответствует свой тип права. Таким образом, усложнение структуры общественно-правовых связей неизбежно влечет и усложнение системы их правовой регламентации.

Последнее десятилетие во всем мире отмечено бурным развитием новых информационных технологий и формированием единого информационного пространства. Количество услуг, получаемых с использованием сети Интернет неуклонно возрастает. Интернет стал средством массовой информации, на серверах сети хранится огромное количество информационных ресурсов (сотни миллионов web-страниц), поиск которых обеспечивают информационно-поисковые системы.

В 2006 году появилась теория сетевого права, в 2010 году многие ее положения были реализованы в Федеральном законе «Об организации предоставления государственных и муниципальных услуг», затем в распоряжении Правительства РФ № 1815р от 2010 года была поставлена задача оценки индекса готовности к созданию сетевого общества, что означало признание существования сетевого общества, а опубликованный 13 апреля 2012 года на официальном сайте Министерства связи и массовых коммуникаций проект «Концепция развития в Российской Федерации механизмов электронной демократии до 2020 года» содержал планы реализации многих идей, которые были описаны в рамках теории сетевого права. Впервые в истории отечественной науки правовая доктрина, предложившая совершенно новое направление юридической науки, реализуется столь быстро, масштабно и эффективно. Наука идет дальше, переходит от частного к общему — от теории сетевого права к обоснованию необходимости создания сетевого общества, назначение которого — решение российских проблем в инновационно-инвестиционной сфере. Строительство так называемой вертикали власти в России объяснялось необходимостью улучшения управления государством. Для улучшения функционирования государства было выдвинуто много разных идей

=====

Какие обязанности возлагаются на блогера при размещении общедоступной информации на сайте в сети Интернет?

При размещении общедоступной информации в сети Интернет блогеры обязаны соблюдать общие требования и ограничения на распространение информации в части ее достоверности, соблюдения прав и законных интересов граждан и организаций, недопустимости размещения информации, распространение которой в РФ ограничивается или запрещается.

Понятие "блогер"

В действующем законодательстве определение понятия "блогер" отсутствует. Ранее блогером признавался владелец сайта и (или) страницы сайта в сети Интернет, на которых размещается общедоступная информация и доступ к которым в течение суток составляет более 3 000 пользователей сети (ч. 1 ст. 10.2 Закона от 27.07.2006 N 149-ФЗ). Однако указанная норма с 30.07.2017 утратила силу (п. 2 ст. 1, ч. 2 ст. 3 Закона от 29.07.2017 N 276-ФЗ; Информация Роскомнадзора).

В настоящее время блогером принято называть человека, который размещает на сайте или странице сайта в сети Интернет регулярно обновляемый контент - тексты, изображения, мультимедиа. Как правило, доступ к данному контенту предоставляется неограниченному кругу лиц.

В данном материале не рассматривается деятельность иностранных граждан в сети Интернет на территории РФ, а также физических лиц, которые могут быть признаны выполняющими функции иностранного агента (в частности, по распространению сообщений и материалов, которые созданы иностранными СМИ, выполняющим функции иностранного агента, в случае получения денежных средств от таких СМИ) (ч. 1 ст. 1, ст. 3 Закона от 01.07.2021 N 236-ФЗ; ч. 3, 7 ст. 6 Закона от 27.12.1991 N 2124-1).

Обязанности и ответственность блогера при размещении общедоступной информации в сети Интернет

При размещении общедоступной информации блогеры обязаны соблюдать установленные законодательством общие требования и ограничения на ее распространение. К числу таковых относятся требования о достоверности информации, соблюдении интеллектуальных прав, недопустимости размещения информации, распространение которой в РФ ограничивается или запрещается, запрет на распространение информации о частной жизни, а также персональных данных лица без его согласия (п. п. 6, 7 ст. 3, ч. 1 ст. 5, ч. 2 ст. 7, ч. 2, 8, 9 ст. 9, ч. 1 ст. 10, ч. 5 ст. 15 Закона N 149-ФЗ; ст. 7 Закона от 27.07.2006 N 152-ФЗ).

Справка. Понятие общедоступной информации

Общедоступная информация - это общеизвестные сведения и иная информация, доступ к которой не ограничен (ч. 1 ст. 7 Закона N 149-ФЗ).

Блогеры обязаны соблюдать права, свободы и законные интересы граждан и юридических лиц, в частности честь и достоинство личности, деловую репутацию. В случае распространения в сети Интернет порочащих, не соответствующих действительности сведений блогер должен будет удалить соответствующую информацию. Кроме того, от него могут потребовать опровержения указанных им сведений, компенсировать моральный вред и возместить убытки. Также предусмотрена ответственность за оскорбление и клевету (п. 1 ст. 150, п. п. 1, 5, 9 ст. 152 ГК РФ; ст. ст. 5.61, 5.61.1 КоАП РФ; ст. 128.1 УК РФ; п. 8 ч. 1 ст. 10.4, п. 4 ч. 1 ст. 10.6, ст. 15.1-2 Закона N 149-ФЗ; п. п. 5, 6, 7, 9 Постановления Пленума Верховного Суда РФ от 24.02.2005 N 3).

Размещение блогерами общедоступной информации ограничивается, в частности, положениями норм, устанавливающих ответственность за действия в информационно-телекоммуникационной сети, в том числе в сети Интернет.

Так, административная ответственность (при отсутствии состава преступления) наступает, например, за распространение в сети Интернет (ч. 5, 9, 10 ст. 13.15 КоАП РФ; ст. 4 Закона от 27.12.1991 N 2124-1):

1) сведений, содержащих инструкции по самодельному изготовлению взрывчатых веществ и взрывных устройств, незаконному изготовлению или переделке оружия, основных частей огнестрельного оружия;

2) заведомо недостоверной общественно значимой информации под видом достоверных сообщений, которое повлекло, в частности, следующие последствия:

- создание угрозы причинения вреда жизни и (или) здоровью граждан, имуществу, угрозы массового нарушения общественного порядка и (или) общественной безопасности либо угрозы создания помех функционированию или прекращения функционирования объектов жизнеобеспечения, транспортной или социальной инфраструктуры, кредитных организаций, объектов энергетики, промышленности или связи;
- создание помех функционированию объектов жизнеобеспечения, транспортной или социальной инфраструктуры, кредитных организаций, объектов энергетики, промышленности или связи.

Публичное распространение заведомо ложной информации в определенных случаях может повлечь уголовную ответственность (ст. ст. 207.1, 207.2 УК РФ). Также на блогеров распространяется запрет на использование сетей связи

общего пользования для осуществления экстремистской деятельности. За публичные призывы в блогах к террористической, экстремистской деятельности, публичное оправдание терроризма или пропаганду терроризма предусмотрена уголовная ответственность (ч. 2 ст. 205.2, ч. 2 ст. 280 УК РФ; ч. 1 ст. 12 Закона от 25.07.2002 N 114-ФЗ).

Кроме того, запрещены публичные призывы к осуществлению действий, направленных на нарушение территориальной целостности РФ, а также распространение в блогах информации, которая направлена на пропаганду войны, нацистской атрибутики или иной запрещенной символики, разжигание национальной, расовой или религиозной ненависти и вражды (ст. ст. 20.3, 20.3.1, 20.3.2 КоАП РФ; ст. ст. 280.1, 282 УК РФ; ч. 6 ст. 10 Закона N 149-ФЗ).

Блогер при размещении общедоступной информации на сайте или странице сайта в сети Интернет должен обеспечивать права несовершеннолетних. Не допускается, например, незаконное распространение информации, указывающей на личность несовершеннолетнего потерпевшего, не достигшего 16-летнего возраста, по уголовному делу либо информации, содержащей описание полученных в связи с преступлением физических или нравственных страданий, повлекшее причинение вреда здоровью несовершеннолетнего, или психическое расстройство несовершеннолетнего, или иные тяжкие последствия (ч. 3 ст. 137 УК РФ).

Дополнительно отметим, что с 01.02.2021 установлены отдельные обязанности для владельца социальной сети. В частности, он не должен допускать ее использование в целях распространения материалов, содержащих нецензурную брань, а также обязан осуществлять мониторинг социальной сети в целях выявления информации, направленной на склонение или иное вовлечение несовершеннолетних в совершение противоправных действий, представляющих угрозу для жизни и (или) здоровья их самих либо иных лиц (п. 1, пп. "е" п. 5 ч. 1 ст. 10.6 Закона N 149-ФЗ; [п. 1 ст. 1](#), [ст. 2](#) Закона от 30.12.2020 N 530-ФЗ).

"Конституционное и муниципальное право", 2021, N 11

ПРАВА ЧЕЛОВЕКА И ГЛОБАЛЬНЫЕ СЕТИ В УСЛОВИЯХ НАРАСТАНИЯ ТЕРРОРИСТИЧЕСКИХ УГРОЗ

В.Г. РОМАНОВСКИЙ

В статье анализируются проблемы противодействия террористическим угрозам в социальных сетях и мессенджерах. Показано, что эффективность противодействия во многом зависит от введения дополнительных ограничений и запретов, поддерживаемых правоохранительными органами. В то же

время при введении правовых новелл в указанной сфере необходимо учитывать технологические особенности распространения информации в сети Интернет. Представлен зарубежный опыт регулирования социальных сетей (Германия, Китай, Великобритания).

Межличностные коммуникации в эпоху развития цифровых технологий претерпели за последние двадцать лет значительные изменения. Социальные сети, по сути, видоизменили мир. Именно благодаря им происходит не просто общение между людьми, связанными определенным интересом, но и информационный обмен (а значит, формирование общественного сознания), выстраивание экономических связей (интернет-экономика все больше отвоевывает себе пространство, занимая серьезный объем в ВВП ведущих стран мира), формирование политического пространства (Д. Трамп, например, имел 35 миллионов подписчиков в Facebook и 25 миллионов в Instagram).

Социальные сети трансформировали и содержание многих базовых прав человека, среди которых центральное место занимают право на неприкосновенность частной жизни и право на получение информации. Связано это как минимум со следующими факторами: раскрытие многих сторон частной жизни на страницах собственных аккаунтов; зависимость получения некоторых услуг от раскрытия персональных данных; связь экономической деятельности с личными страницами в социальных сетях самих предпринимателей. Каждый гражданин выкладывает в мировую паутину огромный объем личной информации, причем такой, что для его обработки требуется искусственный интеллект.

Возрастающее влияние социальных сетей на различные аспекты жизни общества не могло не вызвать определенный интерес со стороны преступных элементов. Уже сейчас можно наблюдать увеличение числа преступлений с применением интернет-технологий, среди которых наибольшее внимание вызывает вымогательство и мошенничество. В первом случае происходит шифровка критически важных данных, а ключ для дешифровки становится доступным только после выплаты выкупа. Объем оборота "шифровальщиков" достигает миллиарда долларов (их доля среди всего вредоносного программного обеспечения почти 50%). Интернет-мошенничество приобретает такие извращенные формы, что правоохранительные органы не всегда успевают обновлять рекомендации по предотвращению преступных посягательств.

Террористические организации быстро освоили новые технологии, активно внедряясь в цифровое пространство, используя его для достижения различных целей: вербовка сторонников; сбор финансовых и материальных ресурсов; пропаганда собственной идеологии; планирование атак, кибербуллинг (травля) своих противников и др. К тому же происходит быстрая

адаптация к мерам противодействия. Так, "Аль-Каида" (запрещена в Российской Федерации) в 2011 г. попыталась разместить онлайн-журнал под названием Inspire ("Вдохновляй"), но его распространение было быстро заблокировано. Благодаря социальным сетям появилась возможность мгновенного обмена информацией. Система хэштегов ускоряет и поиск необходимых данных. Благодаря им и быстрой заливке файлов происходит их моментальное тиражирование и распространение. Сайты стали неудобными, поскольку их блокировка весьма эффективна. Иное дело аккаунты в социальных сетях и телеграм-каналы. Хэштег становится своеобразным ключиком доступа для единомышленников террористической идеи. Кроме того, внесение специальных ошибок в хэштег минимизирует их блокировку. Например, вместо всем понятного слова "терроризм" публикуется хэштег "#терроизм", который собирает в считанные минуты значительное число получателей необходимых сведений.

Расширение зависимости экономики, государства и общества от социальных сетей не позволяет вводить жесткие запретительные меры. С другой стороны, использование цифровых технологий международными террористическими организациями заставляет отрабатывать новые меры противодействия преступной деятельности.

Следует выделить несколько значимых факторов в выстраивании системы противодействия террористическим угрозам в социальных сетях.

Цели, установленные законом, могут быть не достижимы в силу технических особенностей передачи информации через Интернет. Ярким примером может служить так называемый Закон о блогерах - Федеральный закон от 5 мая 2014 г. N 97-ФЗ, дополнивший Федеральный закон "Об информации, информационных технологиях и о защите информации" статьей 10.2 "Особенности распространения блогером общедоступной информации".

Показательна также ситуация с мессенджером Telegram П. Дурова. Объявленная блокировка привела к его еще большей популярности, тогда как цели блокировки так и не были достигнуты. В 2020 г. Роскомнадзор объявил, что у ведомства отсутствуют юридические претензии к деятельности компании, что означает отказ от методики запретов.

Аналогичные последствия произошли с запретом нецензурной брани в социальных сетях, который был установлен благодаря Федеральному закону от 30 декабря 2020 г. N 530-ФЗ, дополнившему Федеральный закон "Об информации, информационных технологиях и о защите информации" статьей 10.6 "Особенности распространения информации в социальных сетях". Информангентство РБК в апреле 2021 г. привело показательную

статистику: "В течение двух месяцев, с 1 февраля по 31 марта 2021 года, в соцсетях "ВКонтакте", "Одноклассники", Facebook, Instagram, Twitter, YouTube, Telegram и TikTok русскоязычные пользователи сделали 20.2 млн публикаций с использованием нецензурной лексики.

Приведенные факты указывают на необходимость соотношения вводимых запретов с техническими возможностями их соблюдения. "Штамповка" правил поведения, заранее обреченных на их неисполнение, лишь девальвирует значение закона. Подобная политика в столь специфической сфере только усложняет принципы взаимодействия государства, технологических компаний и пользователей социальных сетей.

Своеобразной ответной реакцией на растущее влияние спутникового Интернета можно считать появление проекта Федерального закона "О внесении изменений в статью 71 Федерального закона "О связи", которую предлагается дополнить запретом на ввоз на территорию России абонентских терминалов и земных станций, кроме тех операторов связи, которые имеют соответствующие российские лицензии. Сложность реализации такого запрета заключается в том, что прием сигнала предполагается и на мобильных устройствах. То есть для доступа к спутниковому Интернету будет достаточно скачать специальное приложение.

В настоящее время каждый оператор связи должен внедрить систему технических средств для обеспечения функций оперативно-розыскных мероприятий (сокращенно - СОРМ). Для реализации данной обязанности принят целый комплекс нормативных актов. Постановлением Правительства РФ от 31 июля 2014 г. N 743 утверждены Правила взаимодействия организаторов распространения информации в информационно-телекоммуникационной сети Интернет с уполномоченными государственными органами, осуществляющими оперативно-розыскную деятельность или обеспечение безопасности Российской Федерации. Приказом Минкомсвязи России от 12 декабря 2016 г. N 645 утверждены Правила (часть I) применения оборудования систем коммутации, включая программное обеспечение, обеспечивающего выполнение установленных действий при проведении оперативно-розыскных мероприятий. Часть II утверждена Приказом Минкомсвязи России от 19 ноября 2012 г. N 268, часть III - Приказом Минкомсвязи России от 16 апреля 2014 г. N 83, а часть IV - Приказом Минкомсвязи России от 26 февраля 2018 г. N 86.

Постановлением Правительства РФ от 23 сентября 2020 г. N 1526 утверждены Правила хранения организаторами распространения информации в информационно-телекоммуникационной сети Интернет информации о фактах приема, передачи, доставки и (или) обработки

голосовой информации, письменного текста, изображений, звуков, видео или иных электронных сообщений пользователей информационно-телекоммуникационной сети Интернет и информации об этих пользователях и предоставления ее уполномоченным государственным органам, осуществляющим оперативно-розыскную деятельность или обеспечение безопасности Российской Федерации. Указанные Правила призваны обеспечить 6-месячное хранение метаданных пользователей сети Интернет.

Введение обязательности хранения электронных документов операторами связи и расширение полномочий спецслужб - мировая тенденция. Во многих странах инициируются различные иски, нацеленные на минимизацию требований, затрагивающих право на неприкосновенность частной жизни. В качестве примера можно привести Директиву 2006/24/ЕС от 15 марта 2006 г., которая впервые установила режим обязательного хранения электронных данных на территории Европы. Она подвергалась жесткой критике, в результате в 2014 г. Европейский суд вынес решение о ее недействительности. Нецелевой мониторинг данных всего населения в отсутствие подозрений в совершении преступления был признан недопустимым в демократическом обществе. До этого прокурор Европейского суда П.К. Вильялон рекомендовал отменить Директиву.

Несмотря на указанное решение, в Великобритании был принят специальный Закон от 29 ноября 2016 г. о полномочиях на проведение расследования, устанавливающий еще более широкие полномочия спецслужб, чем которые закреплялись в Директиве (но носящие уточняющий характер в отличие от расплывчатых правил Директивы). Общественная дискуссия вокруг Закона 2016 г. не утихает. Отчасти он скорректирован - под давлением правозащитных организаций. Подобная ситуация наблюдается в США, где споры о допустимости тотального хранения ряда метаданных интернет-пользователей - постоянный предмет сенатских дебатов, что не устраняет сами полномочия американских спецслужб.

Как раз реализация всех указанных нормативных актов и приведенных тенденций может свестись к нулю созданием системы спутникового Интернета. Будет отсутствовать само место установки технических средств контроля. Следует дополнить, что спутниковый Интернет ускоряет процесс передачи данных, что изначально создает фору его пользователям. Есть сферы деятельности, где скорость передачи данных - условие успеха. Кстати, внедрение новых технологий в первую очередь воспринимается Вооруженными силами. Достаточно обратиться на официальную страницу OneWeb, чтобы увидеть предлагаемые преимущества: "Решения OneWeb обеспечивают сухопутным войскам бесперебойную и безопасную передачу голосовых и иных данных, что позволяет личному составу создавать и поддерживать тактическое преимущество на земле". Специально

подчеркивается, что оснащение платформой глобального подключения самолетов, вертолетов и беспилотных летательных аппаратов "изменит правила игры".

Изучение китайского опыта создания "золотого щита" (в зарубежных источниках он именуется как "Великий китайский файрвол" - Great Firewall of China показывает, что его обеспечение происходит благодаря многим технологическим решениям, созданным в течение нескольких лет. В-первых, технологическая база была изначально выстроена исходя из национальных нужд. В нашей стране значительный объем трафика связан с использованием иностранного контента, где продукты компании Google имеют свое преимущество (около половины российского трафика - видео, где почти 2/3 приходится на Youtube). Для облегчения доступа к таким продуктам ключевые провайдеры эксплуатируют установленные серверы Google Global Cache. Это также удешевляет пользование сетями. Отказ от GGC приведет не только к удорожанию услуг связи, но и будет иметь иные негативные последствия. Замена же таких дата-центров не произойдет одномоментно, а также потребует серьезных финансовых вливаний. Во-вторых, основная точка входа в Китае в мировую паутину - мобильный телефон. Эта тенденция становится основной для подавляющего числа стран мира. Исходя из этого, продажа мобильных устройств в Китае происходит либо с предустановкой специальных приложений, ограничивающих свободу поиска, либо с добровольно-обязательной последующей установкой такого программного продукта. В-третьих, Китай разработал альтернативные продукты - национальные социальные сети, доступ к которым максимально персонализирован и лишен анонимности. Все указанные мероприятия имеют свою цену - более 40 млрд долл., что вряд ли может позволить себе наше государство (к тому же имея некоторую технологическую зависимость от иностранных компаний по ряду моментов).

Появление SpaceX в КНР было воспринято настороженно, но и здесь после оценки всех рисков принято решение о создании собственной программы Galaxy Space.

Китай является примером фрагментации Интернета - площадки, которая изначально выстраивалась как зона свободного распространения информации. Следует отметить, что подобная тенденция эксплуатируется некоторыми странами. Есть попытки обоснования концепции суверенитета в цифровом пространстве. Технологические гиганты выступают последовательными противниками такого подхода. И если противодействие терроризму выступает понятным основанием введения дополнительных ограничений для интернет-провайдеров, то некоей дополнительной тенью во всех случаях выступает опасение государств в формирующейся

концентрации рынка, а значит, появлению власти над информационными потоками. К тому же взрывное развитие "экономики-онлайн" способствует новому переделу мирового рынка. Данные аспекты поднимались в Германии в 2017 г. при принятии Закона об улучшении правоприменения в социальных сетях (социальны). Несмотря на продвижение идеи о регулировании социальных сетей в целях ограничения доступа к запрещенному контенту, многие исследователи подчеркивали, что этому Закону предшествовали переговоры государства и представителей технологических гигантов, на которых обсуждались общие "правила игры", где борьба с терроризмом была лишь одной из тем обсуждения.

Подобная последовательность наблюдается сейчас в Великобритании, где в мае 2021 г. опубликован проект Акта о безопасности в Интернете. Показательно, что в 2018 г. была опубликована (в апреле 2019 г. - обновленная версия) Цифровая хартия, в которой можно найти соответствующий посыл, лежащий в основе ее принятия, - "опасения по поводу баланса сил между крупными технологическими платформами, гражданами и иными участниками отношений". При этом подчеркнута, что лидерство в решении обозначенных проблем должно принадлежать государству. Первый опыт регулирования социальных сетей в Великобритании появился в 2017 г. с принятием Акта о цифровой экономике, в соответствии с разделом 103 которого принимается Кодекс поведения в социальных сетях. Однако указанный кодекс не затрагивает меры противодействия терроризму в мессенджерах и различных онлайн-платформах. Многие аналитики настороженно заключают, что инициирование Акта о безопасности в Интернете - предлог для восстановления суверенных полномочий государства в виртуальном пространстве, контролируемом частными компаниями, далекими от защиты национальных интересов.

Приведенные обстоятельства позволяют сформулировать следующие выводы.

1. Социальные сети имеют различный функционал, обеспечивающий коммуникации во всех сферах жизни общества, государства и отдельного человека. Развитие цифровой экономики невозможно без расширения возможностей социальных сетей, что обуславливает к ним особое отношение со стороны современного законодателя.

2. Социальные сети активно используются для достижения преступных целей, где расширение влияния со стороны террористических организаций занимает серьезное место. Простота в использовании не требует от самих террористов глобальных познаний и продвинутой цифровой грамотности. Их переход в виртуальное пространство осложняет работу спецслужбам по

противодействию таким угрозам.

3. Эффективное предотвращение террористических атак невозможно без расширения возможностей мониторинга электронного общения граждан, что, безусловно, влечет за собой введение дополнительных ограничений основных прав человека. Общая тенденция связана в первую очередь с изменением концепции права на неприкосновенность частной жизни. Так, закрепление постоянного доступа к персональным данным со стороны правоохранительных органов, государственного хакерства (как разновидности оперативно-розыскного мероприятия), обязанности хранения метаданных пользователей - устоявшаяся практика современных государств.

4. Реализация вводимых запретов в Интернете во многом зависит от технологических особенностей всемирной паутины. Результаты прогресса указывают, что в этой сфере необходимо достижение консенсуса по формированию единых правил поведения: а) между самими государствами, чтобы запрет в одном государстве не преодолевался в либеральной практике другого (стремление некоторых стран к фрагментации Интернета не решит проблему, лишь приведет к технологическому отставанию инициатора); б) между государствами и гигантами данной отрасли (только сорегулирование, формирование партнерских отношений могут иметь положительный результат).

"Судья", 2020, N 10

О НЕКОТОРЫХ ВОПРОСАХ ЗАЩИТЫ АВТОРСКИХ И СМЕЖНЫХ ПРАВ В ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННОЙ СЕТИ ИНТЕРНЕТ

Д.А. ЛЕПЕШИН

Отсутствие привычной объективизированной материальной формы у объектов защиты авторских и смежных прав выявляет и обосновывает необходимость защиты таких прав в информационно-телекоммуникационной сети Интернет. Авторские и смежные права могут быть нарушены путем незаконного размещения произведения, его распространения без согласия правообладателя. При рассмотрении дел, связанных с защитой авторских и смежных прав, имеется ряд проблемных вопросов, которые перечисляет и анализирует автор настоящей статьи.

1. Подсудность споров, связанных с защитой авторских и смежных прав в информационно-телекоммуникационной сети Интернет

Потенциал развития передачи данных через информационно-телекоммуникационные сети усугубляет проблему защиты авторских прав в

сети Интернет. В то же время необходим баланс между защитой авторских прав и свободой распространения и получения информации.

В связи с началом деятельности новых кассационных и апелляционных судов общей юрисдикции с 1 октября 2019 г. и изменением подсудности споров, связанных с защитой авторских и (или) смежных прав, кроме прав на фотографические произведения и произведения, полученные способами, аналогичными фотографии, с применением предварительных обеспечительных мер в порядке, предусмотренном ст. 144.1 Гражданского процессуального кодекса Российской Федерации (далее - ГПК РФ), проведен анализ правоприменительной практики рассмотрения этой категории дел.

В зависимости от существа заявленных требований и объекта защиты споры по авторским и смежным правам, а также по охране и защите иных интеллектуальных прав могут рассматриваться в первой инстанции Московским городским судом и иными судами общей юрисдикции, арбитражными судами, в частности Судом по интеллектуальным правам.

В силу ч. 3 ст. 26 ГПК РФ к подсудности Московского городского суда отнесены гражданские дела, которые связаны с защитой авторских и (или) смежных прав, кроме прав на фотографические произведения и произведения, полученные способами, аналогичными фотографии, в информационно-телекоммуникационных сетях, в том числе в сети Интернет, и по которым им приняты предварительные обеспечительные меры в соответствии со ст. 144.1 Гражданского процессуального кодекса Российской Федерации. Согласно п. 3 ст. 320.1 ГПК РФ в редакции Федерального закона от 28 ноября 2018 г. N 451-ФЗ "О внесении изменений в отдельные законодательные акты Российской Федерации" апелляционные жалобы на решения Московского городского суда и частные жалобы на определения по вышеуказанной категории гражданских дел рассматриваются Первым апелляционным судом общей юрисдикции как апелляционной инстанцией. В кассационном порядке эти дела рассматриваются Вторым кассационным судом общей юрисдикции.

В рамках упомянутой категории дел могут заявляться следующие требования:

- о пресечении действий, нарушающих право или создающих угрозу его нарушения (ст. 12, п. 2 ч. 1 ст. 1252 Гражданского кодекса Российской Федерации; далее - ГК РФ) (например, обязать прекратить создание технических условий, обеспечивающих размещение, распространение и иное использование кинофильма, сообщений телепередач, аудиокниги на определенном сайте);

- об оспаривании права, о признании права (ст. 12, п. 2 ч. 1 ст. 1252 ГК РФ);

- о принятии предварительных обеспечительных мер, направленных на прекращение нарушения (ст. 144.1 ГПК РФ);

- о взыскании ущерба, компенсации, морального вреда в связи с допущенным нарушением права (ст. 1252 ГК РФ).

Арбитражные суды рассматривают споры, связанные с нарушением авторских и (или) смежных прав в сети Интернет, если заявителем (истцом) не было подано заявление о принятии предварительных обеспечительных мер в порядке, предусмотренном ст. 144.1 ГПК РФ, или предварительные обеспечительные меры отменены.

2. Отдельные аспекты, связанные с защитой авторских и смежных прав в информационно-телекоммуникационной сети Интернет

За последнее время резко возросло количество рассмотренных дел, связанных с защитой авторских и смежных прав, так как потенциал развития передачи данных через информационно-телекоммуникационные сети усугубляет проблему защиты этих прав в сети Интернет. Как уже отмечалось, необходимо найти баланс между авторским правом и свободой распространения и получения информации.

Именно отсутствие привычной объективизированной материальной формы объектов защиты вызывает определенные трудности в разрешении вопроса о том, является ли тот или иной объект, размещенный в сети Интернет, объектом защиты авторского или смежного права. Немаловажен вопрос об аспекте установления виновного лица, разместившего информацию об объекте защиты исключительного права. При этом особенности определения субъектного состава правонарушения обусловлены трансграничностью и экстерриториальностью самой сети Интернет.

С изменением технических возможностей передачи данных, способов объективизации тех или иных объектов авторских прав повышается роль судов и контролирующих органов по идентификации способа размещения информации в сети Интернет как нарушающего авторские и смежные права. Например, избегая непосредственного размещения на странице сайта произведения - литературного, аудиовизуального, видеовизуального и др., - владелец сайта может разместить ссылку, по которой будет осуществляться его скачивание на носитель потребителя.

При рассмотрении дел, связанных с защитой авторских и смежных прав в сети Интернет, следует выделить ряд проблемных вопросов, к которым можно отнести, в частности, следующие:

- удаление или прекращение доступа к объектам авторского права и смежных прав, находящимся в облачных хранилищах;

- установление в судебном решении общего запрета на создание технических условий, обеспечивающих размещение, распространение и иное использование объекта авторского права или смежных прав в сети Интернет.

Таким образом, современные информационные технологии позволяют размещать и хранить информацию не только на устройствах пользователей, но и на удаленных серверах, в так называемых облачных хранилищах, которые могут принадлежать третьим лицам (не являющимся правообладателями произведения, пользователями или распространителями соответствующего контента).

Описанные технологии используются и при отправке электронных сообщений, когда файлы (в частности, большого объема) загружаются и направляются в виде адресной ссылки, позволяющей осуществить доступ к ним. Сервисы, предоставляющие услуги по облачному хранению, доступны при использовании почтовых сервисов на сайтах www.yandex.ru, www.mail.ru и др. Размещение экземпляра объекта авторского права или смежных прав в облачном хранилище фактически является действием по воспроизведению произведения, которое осуществляется в личных целях. В соответствии со ст. 1273 и 1306 ГК РФ оно допускается без согласия автора или иного правообладателя и без выплаты вознаграждения, за исключением случаев, предусмотренных ст. 1273 ГК РФ.

Исходя из общего принципа добросовестности лица, предоставляющие услуги по хранению информации в облачных хранилищах, не устанавливают правомерность использования такой информации и размещения ее в хранилище.

Ситуация изменяется, когда ссылка на адрес размещения файла, содержащего произведение, размещается на сайтах, к которым может обратиться любой представитель общественности. В этом случае доступ к произведению, размещенному в облачном хранилище, предоставляется неограниченному кругу лиц. И таким образом, помимо воспроизведения произведения или объекта смежных прав, будет иметь место такой вид использования, как доведение до всеобщего сведения произведения или объекта смежных прав, который не предусмотрен ст. 1273 и 1306 ГК РФ.

3. Информационный посредник в гражданских спорах по защите авторских и смежных прав

Установлены условия, при соблюдении которых информационный посредник, предоставляющий возможность размещения материала в сети Интернет, не несет ответственности за нарушение интеллектуальных прав, произошедшее в результате размещения материала третьим лицом или по его указанию. Согласно п. 3 ст. 1253.1 ГК РФ это ситуации, когда:

1) информационный посредник не знал и не должен был знать о том, что использование соответствующих результата интеллектуальной деятельности или средства индивидуализации, содержащихся в таком материале, является неправомерным;

2) информационный посредник в случае получения в письменной форме заявления правообладателя о нарушении интеллектуальных прав с указанием страницы сайта и (или) сетевого адреса в сети Интернет, на которых размещен такой материал, своевременно принял необходимые и достаточные меры для прекращения нарушения интеллектуальных прав.

Выполнение вышеперечисленных условий информационными посредниками, предоставляющими услуги облачного хранения материалов, должно освобождать их от применения мер гражданско-правовой ответственности. В то же время к ним могут быть предъявлены требования, не связанные с применением таких мер, в том числе об удалении информации, нарушающей исключительные права, или об ограничении доступа к ней. Представляется, что подобные требования могут быть предъявлены к информационным посредникам, которые предоставляют услуги облачного хранения объектов авторского права и смежных прав, если доступ третьих лиц к таким объектам осуществляется с разрешения их правообладателей.

Из положений ст. 1253.1 ГК РФ следует, что к информационным посредникам относятся:

- лицо, осуществляющее передачу материала в информационно-телекоммуникационной сети, в том числе в сети Интернет;

- лицо, предоставляющее возможность размещения материала или информации, необходимой для его получения с использованием информационно-телекоммуникационной сети;

- лицо, предоставляющее возможность доступа к материалу в информационно-телекоммуникационной сети или информации,

необходимой для его получения с использованием информационно-телекоммуникационной сети.

В тех случаях, когда имеет место неправомерное использование произведения или объекта смежного права, размещенного в облачном хранилище, целесообразно проанализировать действия лиц, задействованных в процессе. Здесь имеется несколько правоотношений.

Первое - правоотношение, в рамках которого предоставляется сервис по хранению материала. Владелец обычного хранилища предоставляет свою площадку для размещения информации и материалов. Это образно напоминает услуги складского хранения. Пользователь сервиса облачного хранилища размещает в нем объект интеллектуальной собственности.

Второе - правоотношение, в рамках которого обеспечивается техническая возможность доступа к объекту через адресную ссылку. Так, на сайте в сети Интернет лицо размещает ссылку, которая позволяет представителю общественности осуществить доступ к объекту интеллектуальной собственности, размещенному в облачном хранилище без согласия на то правообладателя объекта интеллектуальной собственности. Неправомерным следует считать именно действие по размещению ссылки на сайте в сети Интернет.

При этом фактически информационным посредником будет владелец того информационного ресурса, на котором размещена ссылка. Именно информационный посредник, предоставляющий возможность по размещению ссылки, по которой осуществляется доступ к объекту интеллектуальной собственности без согласия правообладателя, должен ее удалить или ограничить к ней доступ по заявлению лица, чье право нарушено.

4. Алгоритм защиты авторских и смежных прав в информационно-телекоммуникационной сети Интернет

При размещении объекта в облачном хранилище доступ появляется только одновременно со ссылкой, причем она должна быть открытой. И эта ссылка появляется не по инициативе владельца облачного хранилища. Раскрытие доступа и последующее использование осуществляется без его участия. Он не является непосредственным участником действий, связанным с предоставлением доступа к произведению или объекту смежных прав.

В то же время владелец облачного хранилища способен пресечь действия по дальнейшему неправомерному использованию материала, размещенного у него в хранилище, посредством ограничения к нему доступа

или удаления. В связи с этим в соответствии с подп. 2 п. 1 ст. 1252 ГК РФ к нему может быть предъявлено требование о прекращении действий, нарушающих исключительное право, как к лицу, которое может пресечь такое действие.

Можно предположить, что владелец облачного хранилища также может быть рассмотрен в качестве особого вида информационного посредника. Однозначное урегулирование вопроса в данном случае возможно посредством внесения изменений в ст. 1253.1 ГК РФ ввиду появления новых способов предоставления доступа к объектам авторских и смежных прав, а также таких участников соответствующего процесса, как владелец облачного хранилища.

Порядок ограничения доступа к информации, распространяемой с нарушением авторских и (или) смежных прав, определен в ст. 15.2 Федерального закона от 27 июля 2006 г. N 149-ФЗ "Об информации, информационных технологиях и о защите информации". Для ограничения доступа к объектам авторского права и смежных прав, используемым с нарушением исключительных прав, в соответствии с этим Законом требуется:

- указание наименования произведения, его автора, правообладателя, доменного имени и сетевого адреса, позволяющих идентифицировать сайт в сети Интернет, на котором размещена информация, содержащая объекты авторских и (или) смежных прав (кроме фотографических произведений и произведений, полученных способами, аналогичными фотографии), или информация, необходимая для их получения с использованием информационно-телекоммуникационных сетей, без разрешения правообладателя или иного законного основания;

- указание страниц сайта в сети Интернет, позволяющих идентифицировать такую информацию.

Положения п. 3 ст. 1253.1 ГК РФ также свидетельствуют о необходимости указания в заявлении правообладателя страницы сайта и (или) сетевого адреса в сети Интернет, на котором размещен материал.

Следовательно, законодатель исходит из того, что для ограничения доступа должно быть определено местонахождение в информационно-телекоммуникационной сети конкретного произведения (экземпляра или оригинала) или объекта смежных прав.

Ограничение доступа или удаление должно осуществляться в отношении конкретных экземпляров или оригиналов произведений или объектов смежных прав, использование которых осуществляется неправомерно. В то же время правоприменительная практика показывает, что чаще всего в решениях суда о запрете на создание технических условий,

обеспечивающих размещение, распространение и иное использование объекта авторского права или смежных прав в сети Интернет, указывается доменное имя сайта, а не адрес страницы. В связи с этим возникает вопрос: является ли в достаточной степени обоснованным и достаточным для исполнения судебного решения указание в судебном решении только доменного имени сайта (или сетевого ресурса), поскольку на сайте или ресурсе могут размещаться и произведения, использование которых является правомерным?

Как правило, на момент вынесения судебного акта о запрете создания технических условий, обеспечивающих размещение, распространение и иное использование объекта авторского права или смежных прав в сети Интернет, на указанной истцом странице сайта спорный объект уже отсутствует. То есть информационный посредник удалил или же заблокировал доступ к нему в связи с его использованием с нарушением авторских и/или смежных прав.

Однако это не влияет на возможность рассмотрения заявленных правообладателем требований по существу, их удовлетворение судом и установление запрета на создание технических условий, обеспечивающих размещение, распространение и иное использование на сайте информационно-телекоммуникационной сети Интернет объекта авторского права и/или смежных прав без получения согласия правообладателя. Иной подход приведет к невозможности защиты заявителями принадлежащих им исключительных прав на результаты интеллектуальной собственности, так как удаление пользователями каждого повторно размещенного произведения с сайта на момент рассмотрения исковых требований повлекло бы отказ в удовлетворении заявленных требований и при этом не исключало возможности размещения соответствующего объекта вновь.

Таким образом, требование о пресечении действий, нарушающих право или создающих угрозу его нарушения, может быть удовлетворено только в том случае, если противоправное поведение конкретного лица еще не завершено или имеется угроза нарушения права, что подтверждается п. 57 Постановления Пленума Верховного Суда Российской Федерации от 23 апреля 2019 г. N 10 "О применении части четвертой Гражданского кодекса Российской Федерации".

Требования об общем запрете конкретному лицу на будущее использовать результат интеллектуальной деятельности (например, о запрете размещения информации в информационно-телекоммуникационных сетях, в том числе сети Интернет) не подлежат удовлетворению, поскольку такой запрет установлен непосредственно законом, что регулируется абз. 3 п. 1 ст. 1229 ГК РФ.

Дайджест по теме составлен на основе обзора статей из СПС «КонсультантПлюс»

Сетевому обществу – сетевое право: дайджест / МУК «Ижморская ЦБС», Ижморская центральная библиотека им. М.С.Прудникова, сектор информации, маркетинга и рекламы; сост. Н.Стручкова. – пгт.Ижморский, 2022. – 20 с.