ПП № 1(70)-2019. с. 91—95

УДК 343.221.51 + 004.056

Савенкова Д. Д.

АКТУАЛЬНЫЕ ВОПРОСЫ РАЗВИТИЯ ИНСТИТУТА ЮРИДИЧЕСКОЙ ОТВЕТСТВЕННОСТИ В СФЕРЕ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В УСЛОВИЯХ ЦИФРОВИЗАЦИИ

Savenkova D. D.

TOPICAL ISSUES OF DEVELOPMENT OF THE INSTITUTION OF LEGAL RESPONSIBILITY IN THE FIELD OF INFORMATION SECURITY IN TERMS OF DIGITALIZATION

Статья посвящена актуальным вопросам юридической ответственности в сфере обеспечения информационной безопасности в условиях цифровизации. В статье рассматриваются механизмы ограничения доступа к сайтам в сети Интернет на примере блокировки сайтов. Анализируется правовая природа блокировки сайтов как превентивной меры и санкции. Поднимается проблема установления границ ответственности провайдеров и пользователей, закрепляемой в пользовательских соглашениях в информационно-телекоммуникационных сетях, а также применяемое право в случае возникновения спора.

Ключевые слова: *информационная безопасность, юридическая ответственность, юрисдикция, блокировка сайтов, пользовательские соглашения, сеть Интернет, принципы.*

The article is devoted to topical issues of legal responsibility in the field of information security in terms of digitalization. The article discusses the mechanisms of restricting access to sites on the Internet on the example of blocking sites. The legal nature of blocking sites as a preventive measure and sanction is analyzed. The problem of establishing the boundaries of responsibility of providers and users, enshrined in user agreements in information and telecommunication networks, as well as the applicable law in the event of a dispute.

Keywords: *information security, legal liability, jurisdiction, blocking sites, user agreements, the Internet, principles.*

Проблемы «цифровизации» и «цифровой экономики» в настоящее время активно обсуждаются в юридической сфере, их развитию уделяется внимание как органами государственной власти, экспертным сообществом, так и обществом в целом. В послании Федеральному Собранию в 2016 г. Президент Российской Федерации В.В. Путин предложил «запустить масштабную системную программу развития экономики нового технологического поколения – цифровой экономики. [1] В утвержденной в июле 2017 года Правительством Российской Федерации программе развития цифровой экономики до 2024 года определены пять базовых направлений – нормативное регулирование, кадры и образование, формирование исследовательских компетенций и технических заделов, информационная инфраструктура и информационная безопасность.

Процесс цифровизации, особенно использование ряда цифровых технологий, вместе с тем несет множество рисков и угроз. В связи с этим вопросы информационной безопасности становятся ключевыми при обеспечении практически всех информационных процессов, как на национальном, так и на международном уровнях. Одним из важнейших компонентов системы обеспечения информационной безопасности является институт юридической ответственности. Он выполняет ряд функций в данной системе – превентивную, охранительную, правовосстановительную и другие. Представляется, что именно данный институт позволяет обеспечивать на данном этапе развития информационного общества выполнение более двух третей требований в сфере обеспечения информационной безопасности на национальном уровне.

Как показывает анализ одним из наиболее актуальных организационно-правовых механизмов в институте юридической ответственности в информационной сфере является ограничение работы (блокировка) сайта или другого сетевого ресурса. Блокировка сайта имеет сложную юридическую природу: это и превентивное средство (обеспечительная мера), и мера защиты от неправомерных действий и информации, причиняющей вред или являющейся противоправной, это и санкция за совершенное правонарушение. Вопросы правового регулирования блокировки сайтов закреплены в Федеральном законе «Об информации, информационных технологиях и о защите информации» (далее – Закон об информации), где содержится целый ряд правовых норм, связанных с «блокировкой сайтов». Так, в ст. 15 Закона об информации регламентируются следующие вопросы ограничений доступа к сайтам в сети «Интернет»: ограничение доступа к информационному ресурсу организатора распространения информации в сети «Интернет»; ограничения доступа к сайтам в сети «Интернет», на которых неоднократно и неправомерно размещалась информация, содержащая объекты авторских и (или) смежных прав, или информация, необходимая для их получения с использованием информационно-телекоммуникационных сетей, в том числе сети «Интернет». А с 2017 г. также определяет Порядок ограничения доступа к копиям заблокированных сайтов.

В соответствии с постановлением Правительства РФ от 5 июня 2018 г. № 651 «О внесении изменений в постановление Правительства Российской Федерации от 26 октября 2012 г. № 1101» еще одним основанием для включения решения в единый реестр доменных имен и (или) указателей страниц сайтов в сети «Интернет», а также сетевых адресов, позволяющих идентифицировать сайты в сети «Интернет», содержащие запрещенную информацию, являются решения Федеральной службы по регулированию алкогольного рынка - в отношении распространяемой посредством сети «Интернет» информации, содержащей предложения о розничной продаже дистанционным способом алкогольной продукции, и (или) спиртосодержащей пищевой продукции, и (или) этилового спирта, и (или) спиртосодержащей непищевой продукции, розничная продажа которых ограничена или запрещена законодательством Российской Федерации о государственном регулировании производства и оборота этилового спирта, алкогольной и спиртосодержащей продукции и об ограничении потребления (распития) алкогольной продукции. При этом правовая природа ограничения доступа (блокировки) к сайтам, ресурсам или информации неоднородна. С одной стороны, это может являться мерой превентивного характера (предупредительная мера – временная блокировка), с другой стороны, как санкция за нарушение установленных Законом об информации правил и норм, а в-третьих, выполняет функцию защиты личности от вредоносной информации.

Кроме того, как показывает исследование в Уголовном кодексе Российской Федерации содержится 17 составов преступлений, где использование сети Интернет является квалифицирующим признаком и за это предусмотрена более строгая ответственность. Вместе с тем важно отметить, что проведенный анализ свидетельствует о том, что в Законе об информации и других нормативных правовых актах отсутствует определение понятия «ограничение доступа к сайту». Полагаем, что данное определение необходимо закрепить указанном Федеральном законе, и под ограничением доступа к сайту представляется целесообразным понимать осуществление на основании решения уполномоченного органа или суда комплекса мер для обеспечения невозможности использования информации, сайта или веб-сервиса. Вопросы ограничения доступа к сайтам являются крайне важными и для развития системы международной информационной безопасности. Блокировка сайтов в настоящее время является универсальным механизмом, который активно используется

в России, Китае, США, Великобритании, Франции, Канаде, Турции и многих других странах.

Особого внимания заслуживает сотрудничество в сфере профилактики терроризма и экстремизма в сети Интернет, а также информационной среде и цифровом пространстве, поскольку такие информационные ресурсы имеют огромную потенциальную опасность и могут являться источниками для распространения противоправных, антигуманных идей. Учитывая, что ИКТ активно используются террористическими и экстремистскими организациями, предлагается в рамках региональных общественных объединений государств: Евразийского экономического союза, а также БРИКС и ШОС создать правовой механизм мониторинга киберинцедентов и нарушений информационной безопасности и ведение межнационального реестра экстремистских и иных запрещенных законодательством материалов, которые будут блокироваться на территории стран участников.

Еще одной исключительно важной и актуальной проблемой развития института юридической ответственности в информационной сфере, которая возникает в условиях цифровизации современного общества и все более активного использования сети Интернет, является установление границ ответственности провайдеров и пользователей, устанавливаемых в пользовательских соглашениях в информационно-телекоммуникационных сетях, а также применяемое право в случае возникновения спора. Так, например, пользовательские соглашения в Facebook и Instagram имеют практически идентичные нормы относительно ответственности следующего содержания: «Если вы являетесь потребителем, к любым претензиям, искам и спорам между пользователями и другой стороной возникающим из Условий или Продуктов, или в связи с ними «спор»), применяются законы страны вашего проживания, и вы можете решить спор в любом компетентном суде такой страны, которому он подсуден. Во всех прочих случаях вы соглашаетесь, что спор должен решаться исключительно в федеральном окружном суде Северного округа штата Калифорния или в суде штата, находящемся в округе Сан-Матео, что вы подчиняетесь персональной юрисдикции любого из этих судов в целях рассмотрения любого такого спора и что настоящее Пользовательское соглашение и любой спор регулируются законодательством штата Калифорния без учета его коллизионных норм». [2] Также интересная формулировка содержится в соглашении ICANN из которой следует, что: споры, возникающие в ходе исполнения или в связи с не согласием, в том числе споры, вызванные отказом ICANN в продлении аккредитации Регистратора и требования о реальном выполнении отдельных положений, будут рассматриваться в суде компетентной юрисдикции или, по решению любой из сторон, в арбитражном суде согласно положениям настоящего подраздела 5.8 в соответствии с правилами международного арбитража Американской арбитражной ассоциации. Заседания должны проводиться на английском языке в округе Лос-Анджелес, штат Калифорния, США. [3]

Так, Н. Руйе отмечал, что частная процедура спора по Uniform Domain Name Dispute Resolution Policy проводится в четырех организациях, из которых самыми известными являются: Центр ВОИС по арбитражу и посредничеству, Североамериканский Национальный арбитражный форум и Азиатский Центр. Центр ВОИС, который с момента начала деятельности по разрешению доменных споров в 1999 г. рассмотрел более 30 тыс. споров, что составляет около 3 тыс. споров в год; Американский форум – около 20 тыс. споров, т.е. примерно 2 тыс. споров в год. [4]

Таким образом, при использовании различных сервисов, социальных сетей и медиа продуктов, существует риск ограничения ответственности компаний, а также сложности, связанные с трансграничной юрисдикцией при судебном разбирательстве и ограничение в защите своих прав и законных интересов. Полагаем, что решением такого вопроса может быть закрепление общей правовой нормы, о том, что, если одним из субъектов телекоммуникационных правоотношений является гражданин РФ либо лицо, временно проживающее на территории РФ, а также, если сервис или услуга предоставляется на территории РФ, то пользователь такого сервиса имеет возможность обратиться в российские суды для защиты своих прав, свобод и законных интересов, за исключением случаев прямого указания коллизионных норм, закреплённых в российском законодательстве или в международных правовых нормах. При этом как показывает анализ аналогичных пользовательских соглашений крупнейших российских интернет-компаний или сервисов, то в них вопрос юрисдикции решается путем определения подсудности спора судам российской юрисдикции.

Относительно юрисдикции при привлечении к уголовной ответственности за преступления в сфере информационной безопасности, как составляющей национальной безопасности, следует отметить, что вопрос трансграничной юрисдикции по сути определен в ст. 12 УК РФ. Кроме того, важное теоретико-правовое значение для развития института юридической ответственности в области обеспечения информационной безопасности имеет вопрос оптимизации системы принципов. Для правового регулирования отношений, связанных с юридической ответственностью важна унификация, как общепризнанных, общеправовых, так и закрепленных в отдельных законодательных актах отраслевых принципов правового регулирования информационного права отношений в сфере информации, информационных технологий и защиты информации. [5]

Следует согласиться с Т.А. Поляковой, которая отмечает важность сохранения принципа государственного суверенитет, а также выделяет такие важнейшие принципы, необходимые для дальнейшего развития информационного общества и обеспечения информационной безопасности, как доверие и безопасность в использовании ИКТ, вытекающие из необходимости поощрять, формировать, развивать и активно внедрять устойчивую глобальную культуру кибербезопасности [6]. Очевидно, что процессы информатизации и цифровизации, активно происходящие в настоящее время в России, касаются всех сфер нашей жизни, включая экономику, социальную сферу, здравоохранение, образование направлены на развитие информационного общества, но вместе с тем влекут новые риски, вызовы и угрозы информационной безопасности в информационном пространстве и цифровой среде. В связи с этим обеспечение устойчивого развития современного мира, информационного пространства возможно лишь при условии объединения усилий всех государств в создании новых правовых инструментов и механизмов для развития эффективной системы международной информационной безопасности и совершенствования национального законодательства, укрепления международного сотрудничества.

Литература

1. Послание Президента Федеральному Собранию от 1 декабря 2016 г. Официальный сайт Президента Российской Федерации URL: http://kremlin.ru/events/president/news/53379 (дата обращения 27 января 2019 г.)
2. Пользовательское соглашение Facebook // Официальный сайт Facebook URI: https://www.facebook.com/legal/terms?locale=ru_RU (дата обращения 25 августа 2018 г.); Условия использования Instagram // Официальный сайт Instagram // URL: https://help.instagram.com/581066165581870 (дата обращения 27 декабря 2018 г.)
3. Соглашение об аккредитации регистраторов // Официальный сайт ICANN URL: https://www.icann.org/resources/unthemed-pages/approved-with-specs-2013-10-31-ru(дата обращения 28 августа 2018 г.)
4. Руйе Н. Споры о доменных именах: выбор между частными процедурами (udrp и прочими) и разбирательством в государственном суде // Право в сфере Интернета. Сборник статей / Рук. авт. кол. и отв. ред. д.ю.н. М.А. Рожкова. – М.: Статут, 2018. – 528 с.
5. Минбалеев, А. В. Принципы информационного права / А. В. Минбалеев // Вестник ЮУрГУ. Серия «Право». – 2015. – Т. 15. № 1. – С. 79-84.
6. Полякова Т.А. Базовые принципы как основные начала правового обеспечения информационной безопасности // Труды Института государства и права РАН. – 2016. – № 3 (55). –С. 17-40.

References

1. Poslanie Prezidenta Federal'nomu Sobraniyu ot 1 dekabrya 2016 g. Oficial'nyj sajt Prezidenta Rossijskoj Federacii URL: http://kremlin.ru/events/president/news/53379 (data obrashcheniya 27 yanvarya 2019 g.)
2. Pol'zovatel'skoe soglashenie Facebook // Oficial'nyj sajt Facebook URI: https://www.facebook.com/legal/terms?locale=ru_RU (data obrashcheniya 25 avgusta 2018 g.); Usloviya ispol'zovaniya Instagram // Oficial'nyj sajt Instagram // URL: https://help.instagram.com/581066165581870 (data obrashcheniya 27 dekabrya 2018 g.)
3. Soglashenie ob akkreditacii registratorov // Oficial'nyj sajt ICANN URL: https://www.icann.org/resources/unthemed-pages/approved-with-specs-2013-10-31-ru(data obrashcheniya 28 avgusta 2018 g.)
4. Ruje N. Spory o domennyh imenah: vybor mezhdu chastnymi procedurami (udrp i prochimi) i razbiratel'stvom v gosudarstvennom sude // Pravo v sfere Interneta. Sbornik statej / Ruk. avt. kol. i otv. red. d.yu.n. M.A. Rozhkova. – M.: Statut, 2018. – 528 s.

5. Minbaleev, A. V. Principy informacionnogo prava / A. V. Minbaleev // Vestnik YUUrGU. Seriya «Pravo». – 2015. – T. 15. № 1. – S. 79-84.
6. Polyakova T.A. Bazovye principy kak osnovnye nachala pravovogo obespecheniya informacionnoj bezopasnosti // Trudy Instituta gosudarstva i prava RAN. – 2016. – № 3 (55). –S. 17-40.

САВЕНКОВА Дарья Дмитриевна, преподаватель кафедры информационного права и цифровых технологий Московского государственного юридического университета им О.Е. Кутафина (МГЮА). 125167, г. Москва, Ленинградский проспект, 47. E-mail: 5hdd@mail.ru

SAVENKOVA Daria, Lecturer, Department of Information Law and Digital Technologies, Moscow State Law University named after O.E. Kutafina (MSLA). 125167, Moscow, Leningradsky Avenue, 47. E-mail: 5hdd@mail.ru