Рабчевский Евгений Андреевич
Никитин Дмитрий Алексеевич

Правовые аспекты регулирования оборота Больших данных с учетом тенденции распространения экстремистских и иных деструктивных материалов в сети Интернет

Рассмотрены правовые аспекты регулирования оборота Больших данных с учетом тенденции распространения экстремистских и иных деструктивных материалов в сети Интернет. Проанализированы законодательные инициативы Российской Федерации последних лет, направленные на решение задач в данной сфере. Отражен опыт Евросоюза и Соединенных Штатов в части юридического регулирования работы с персональными данными в контексте Больших данных.

Ключевые слова: Большие данные, персональные данные, экстремизм, социальные сети, пропаганда, Интернет, законодательство.

Legal aspects of regulating the circulation of big data, taking into account the trend of the spread of extremist and other destructive materials on the Internet

This paper is devoted to the legal aspects of regulating the treatment of big data, taking into account the trend of the spread of extremist and other destructive materials on the Internet. The legislative initiatives of the Russian Federation in recent years, aimed at solving problems in this area, are considered. The experience of the European Union and the United States in terms of legal regulation of personal data treatment in the context of big data is researched.

Key words: big data, personal data, extremism, social networks, propaganda, Internet, legislation.

В настоящее время происходит активная цифровизация всех сфер жизни и деятельности человека. Многие процессы уже перенесены в цифровую среду, и такая тенденция будет лишь усиливаться с течением времени, учитывая повсеместное развитие технологий Четвертой промышленной революции (Большие данные, искусственный интеллект, Интернет вещей, квантовые вычисления, блокчейн-технологии и т.д.).

Однако вместе с возможностями, открывающимися благодаря новым технологиям цифровой эпохи, возникают также новые вызовы и угрозы, сопряженные с ними. Массовое использование социальных сетей для распространения материалов экстремистского и иного деструктивного характера в сети Интернет – одна из угроз новой эпохи.

В связи с все возрастающей ролью Больших данных, а также методов и средств их мониторинга в жизни общества интерес к ним появляется не только среди преступных элементов и специалистов по информационному противоборству, но и в федеральных органах законодательной власти, поскольку в профессиональной среде возникает понимание необходимости законодательного регулирования оборота и использования Больших данных. Роль Больших данных обусловлена в этом случае как вопросами национальной безопасности, так и их коммерческой ценностью. Немаловажное значение имеет и отношение общества к данному вопросу, поскольку юридическое регулирование оборота Больших данных неизбежно затрагивает и оборот персональных данных. Возникает необходимость поиска баланса между обеспечением решения задач национальной безопасности, соблюдением коммерческих интересов компаний, задействованных в сфере Больших данных, и обеспечением гражданам гарантий неприкосновенности их частной жизни, которая в наше время в значительной мере перетекла в информационно-телекоммуникационную плоскость.

Ниже рассматривается ряд законодательных инициатив последних лет, связанных с повышением цифрового суверенитета и обеспечением информационно-идеологической безопасности Российской Федерации. В контексте рассматриваемых в настоящей работе

вопросов обращают на себя внимание следующие инициативы, приведенные в хронологическом порядке:

1. Федеральный закон от 28 декабря 2013 г. № 398-ФЗ «О внесении изменений в Федеральный закон “Об информации, информационных технологиях и о защите информации”» [1]. Этот закон предусматривает возможность блокировки информационных интернет-ресурсов за распространение призывов к массовым беспорядкам, осуществлению экстремистской деятельности и участию в массовых беспорядках. Процедура блокировки не требует решения суда и может быть начата Генеральным прокурором РФ и его заместителями на основании результатов мониторинга информационного пространства, а также обращений органов власти, организаций и граждан. Решение о блокировке направляется в Роскомнадзор, адресующий операторам связи требование заблокировать доступ к сайту с деструктивной информацией. Оператор связи при этом должен немедленно ограничить доступ к сайту. Далее Роскомнадзор определяет провайдера хостинга ресурса, содержащего противозаконную информацию, и уведомляет его о необходимости ее удаления. Сайт может быть разблокирован после получения Роскомнадзором сообщения об удалении деструктивной информации.

2. Федеральный закон от 7 июня 2017 г. № 109-ФЗ «О внесении изменений в Федеральный закон “Об основах системы профилактики безнадзорности и правонарушений несовершеннолетних” и статью 15.1 Федерального закона “Об информации, информационных технологиях и о защите информации” в части установления дополнительных механизмов противодействия деятельности, направленной на побуждение детей к суицидальному поведению» [2]. Этот закон публично поддержал, в том числе, и Президент РФ В.В. Путин, назвав «как минимум преступниками» пропагандирующих в сети Интернет самоубийство: «В этой связи поддерживаю инициативу депутатов Госдумы о дополнении законодательства нормой, расширяющей перечень действий, при которых наступает уголовная ответственность за доведение до самоубийства. Это позволит привлекать к ответственности хозяев, создателей и администраторов подобных сайтов, пресекать их деструктивную, преступную деятельность» [3].

3. Федеральный закон от 18 декабря 2018 г. № 472-ФЗ «О внесении изменений в статью 15.1 Федерального закона “Об информации, информационных технологиях и о защите информации” и статью 5 Федерального закона “О защите детей от информации, причиняющей вред их здоровью и развитию”» [4]. Одним из авторов этого нормативного правового акта является вице-спикер Государственной Думы РФ (далее – ГД РФ) И.А. Яровая. Он был вызван к жизни рядом инцидентов с использованием как холодного, так и огнестрельного оружия в школах России. В соответствии с рассматриваемым законом блокировке подлежит любая информация в сети Интернет, склоняющая к действиям, опасным для жизни или здоровья самих детей либо других людей.

4. Федеральный закон от 18 марта 2019 г. № 30-ФЗ «О внесении изменения в Федеральный закон “Об информации, информационных технологиях и о защите информации”» [5]. Авторы этого закона – члены Совета Федерации А.А. Клишас, Л.Н. Бокова и депутат ГД РФ Д.Ф. Вяткин. Цель данной инициативы – противодействие распространению информации, оскорбляющей человеческое достоинство, общественную нравственность, государство или государственные символы. В случае выявления контента подобного рода Генеральный прокурор РФ или его заместители должны обратиться в Роскомнадзор, который ограничит доступ к противоправной информации и осуществит комплекс мероприятий по ее удалению.

5. Федеральный закон от 18 марта 2019 г. № 31-ФЗ «О внесении изменений в статью 15.3 Федерального закона “Об информации, информационных технологиях и о защите информации”» [6]. Данный нормативный правовой акт, инициированный теми же законодателями, что и рассмотренный выше, и неофициально именуемый «законом о фейк-ньюз», запрещает публикацию ложной общественно значимой информации, выдаваемой в качестве подлинной, при условии, если эта информация несет угрозу жизни и здоровью, влияет на общественный порядок и безопасность, препятствует работе объектов жизнеобеспечения, инфраструктуры, финансов и т.д. Согласно этому закону Генеральный прокурор РФ или его заместители имеют возможность без решения суда потребовать ограничения доступа к ресурсам, размещающим фальшивые новости. Далее в соответствии со стандартной процедурой Роскомнадзор известит об этом редакцию, разместившую недостоверные сведения, и потребует безотлагательно удалить неправдоподобные данные, иначе будет осуществлено ограничение доступа к ресурсу. В случае последующего удаления фейковых новостей его работа может быть возобновлена.

6. Постановление Правительства РФ от 21 марта 2019 г. № 295 «О внесении изменений в постановление Правительства Российской Федерации от 26 октября 2012 г. № 1101» [7]. Настоящее постановление наделяет Федеральное агентство по делам молодежи (Росмолодежь) полномочиями по досудебной блокировке интернет-ресурсов, склоняющих несовершеннолетних к противоправным действиям. Таким образом, в настоящее время Росмолодежь способна включать доменные имена в единый реестр запрещенных сайтов на основании наличия информации, вовлекающей несовершеннолетних в совершение противоправных действий, представляющих угрозу для их жизни и здоровья либо для жизни и здоровья иных лиц.

7. Федеральный закон от 1 мая 2019 г. № 90-ФЗ «О внесении изменений в Федеральный закон “О связи” и Федеральный закон “Об информации, информационных технологиях и о защите информации”» [8]. Данный закон предусматривает создание национальной системы маршрутизации интернет-трафика. Основная задача, решаемая с помощью этой инициативы, – обеспечение надежной работы российского сегмента глобальной сети в случаях сбоев в инфраструктуре Интернета за пределами России или целенаправленного масштабного внешнего влияния деструктивного характера. Требования настоящего закона затрагивают операторов связи и владельцев технологических сетей, которым необходимо будет изменить маршруты передачи данных. Среди пользователей закон в первую очередь повлияет на операторов государственных и муниципальных информационных систем, а также бизнес в сфере госзакупок: сейчас необходимо использовать базы данных и технические средства, размещенные на территории Российской Федерации.

Обратимся теперь к зарубежному опыту в части регулирования оборота Больших данных, начав рассмотрение со стран Европы. Так, 25 мая 2018 г. Европейский союз (ЕС) перешел к новой процедуре обработки персональных данных, установленных Общим регламентом по защите данных (Регламент ЕС 2016/679 от 27 апреля 2016 г. GDPR – General Data Protection Regulation [9]). Настоящий регламент, имеющий прямое действие во всех 28 странах Евросоюза, пришел на смену рамочной Директиве о защите персональных данных 95/46/ЕС от 24 октября 1995 г. [10]. Важная особенность GDPR – экстерриториальный принцип действия новых правил обработки персональных данных, применяемый ко всем организациям, обрабатывающим персональные данные резидентов и граждан ЕС, вне зависимости от места нахождения этих структур. С учетом указанного обстоятельства российским компаниям следует внимательно относиться к данному аспекту, если их услуги ориентированы на международные рынки.

Помимо обработки персональных данных, в GDPR вводится понятие мониторинга поведения субъектов данных, которое включает в сферу действия GDPR еще одну категорию субъектов. GDPR применяется к организациям, созданным за пределами ЕС, если они контролируют поведение жителей ЕС (в той степени, в которой такое поведение имеет место в ЕС). Мониторинг подразумевает под собой отслеживание резидента ЕС в Интернете, а также использование методов обработки данных для профилирования отдельных лиц, их поведения или отношения к чему-либо (например, для анализа или прогнозирования личных предпочтений).

Персональные данные в логике GDPR – это любая информация, относящаяся к идентифицированному или идентифицируемому физическому лицу (субъект данных), по которой прямо или косвенно можно его определить. К такой информации относятся, в том числе, имя, данные о местоположении, онлайн-идентификатор, а также один или несколько факторов, характерных для физической, физиологической, генетической, умственной, экономической, культурной или социальной идентичности указанного физического лица. Таким образом, даже IP-адреса могут рассматриваться в качестве персональных данных. Необходимо отметить, что существуют определенные типы персональных данных, относящиеся к категории особых или конфиденциальных персональных данных. Это информация, раскрывающая расовое или этническое происхождение, политические взгляды, религиозные или философские убеждения и членство в профсоюзах. Кроме того, к этой группе относятся: генетические и биометрические данные, используемые для идентификации физического лица; данные о состоянии здоровья; сведения, касающиеся сексуальной жизни или сексуальной ориентации.

Таким образом, GDPR – важнейший законодательный документ, существенно повышающий уровень защиты персональных данных в ЕС и за его пределами, требующий внимательного ознакомления и соблюдения. Данная реформа в части оборота персональных данных позволяет сформировать последовательный

подход, который должен применяться в сфере защиты данных. Она также восстанавливает доверие со стороны интернет-пользователей, что позволяет бизнесу максимально эффективно реализовывать возможности информационно-телекоммуникационных технологий на едином европейском цифровом рынке с учетом того, что сбор, анализ и перемещение персональных данных по всему миру приобрели критически важное экономическое значение.

Важно также обратиться и к опыту Соединенных Штатов Америки (США) в рассматриваемом вопросе, поскольку эта страна является ключевым потребителем информационно-телекоммуникационных услуг, а также средоточием всевозможных стартап-проектов в сфере цифровой экономики. Наиболее известным нормативным правовым актом, регламентирующим оборот больших пользовательских данных в этой стране, является «Акт о сплочении и укреплении Америки путем обеспечения надлежащими средствами, требуемыми для пресечения и воспрепятствования терроризму» [11] (более известен под названием «Патриотический акт») – федеральный закон, принятый в США в октябре 2001 г. Этот документ значительно расширил полномочия правительства и силовых структур в части надзора за гражданами. «Патриотический акт» был принят как ответная реакция на печально известные атаки террористов 11 сентября 2001 г. и расширил, в частности, права Федерального бюро расследований (ФБР) и Агентства национальной безопасности (АНБ) по контролю телефонных переговоров граждан и их активности в сети Интернет, что многими экспертами и общественностью было воспринято как нарушение четвертой поправки к Конституции США.

В рамках реализации норм «Патриотического акта» спецслужбы США выполняли слежку за пользователями Интернета и телефонных сетей, осуществляя контроль при поддержке крупнейших информационно-телекоммуникационных компаний. Реагируя на ставшую общеизвестной в результате откровений Эдварда Сноудена в 2013 г. информацию о секретной программе PRISM (комплекс мероприятий АНБ, проводимых с 2007 г. в целях массового негласного сбора информации, передаваемой по сетям электросвязи), Президент США Барак Обама назвал критику в ее адрес «спекуляцией», отказавшись приносить извинения за прослушку и сбор данных и заявив, что она «того стоит». Он призвал общественность прийти к пониманию того обстоятельства, что «безопасность и личная информация не могут быть отделены друг от друга на 100%, каждый должен это понимать».

В рамках реализации программы PRISM системы сбора информации АНБ в ежедневном режиме перехватывали и записывали около 1,7 млрд телефонных разговоров и электронных сообщений и около 5 млрд записей о геолокации пользователей мобильных девайсов по всему миру. При этом основными поставщиками данных являлись американские телеком-гиганты Microsoft, Google, Yahoo, Facebook, America Online и Apple, открывшие АНБ прямой доступ к своим серверам. В ядро программы PRISM заложены те же компоненты, что и в «гражданских», традиционных решениях Больших данных (например, программное обеспечение с открытым исходным кодом Hadoop). То обстоятельство, что АНБ осуществляет деятельность в масштабах Больших данных с использованием новейших технологий, подтверждают и сами представители АНБ [12, с. 43–66].

Разоблачения Эдвардом Сноуденом государственной системы тотального слежения вызвали широкий резонанс в американском обществе, и руководство США было вынуждено отреагировать на это обстоятельство. Результатом этой реакции явился «Акт о свободе США» 2015 г., пришедший на смену «Патриотическому акту». Данный документ запрещает АНБ и другим спецслужбам вести прослушивание телефонных переговоров и электронную слежку, а также собирать информацию о гражданах США в негласном порядке. Сейчас проведение подобных мероприятий возможно только по решению специального секретного суда, имеющего, тем не менее, особый порядок судопроизводства.

Продолжает тенденцию к усилению защиты прав граждан США и вступающий в силу с 2020 г. закон штата Калифорния о защите персональных данных интернет-пользователей. Эксперты называют данный нормативный правовой акт гораздо более жестким по сравнению с действующими в США на данный момент. Среди американской общественности уже раздаются призывы к тому, чтобы и другие штаты последовали примеру Калифорнии в части защиты прав пользователей. Согласно новому закону пользователи получают широкие права иметь представление о том, какую персональную информацию собирают интернет-компании, почему фиксируются именно эти данные, как и в связи с чем они используются информационно-телекоммуникационными фирмами в дальнейшем. Потребители также получают право требовать от компаний удаления инфор-

мации или запрещать ее продажу третьим лицам или рекламодателям. Кроме того, данный закон значительно ограничивает компании в вопросах передачи или продажи данных несовершеннолетних интернет-пользователей. Американские эксперты интернет-отрасли полагают, что принятие этого закона именно в Калифорнии, где расположены штаб-квартиры многих ведущих интернет- и технологических компаний (Google, Oracle, Yahoo!, Facebook, AT&T, HP, Intel, Apple и др.), может оказать намного более значительное влияние на вопрос обработки персональных данных в рамках всей страны, чем собственно на территории штата.

Резюмируя рассмотрение правовых аспектов регулирования оборота Больших данных с учетом тенденции распространения деструктивных материалов в сети Интернет, необходимо отметить, что интерес органов законодательной власти к данному вопросу имеет место не только в России, но и в других странах, поскольку Интернет давно уже приобрел критически значимый статус в жизни общества и государства как с точки зрения вопросов безопасности, так и в экономической сфере.

1. URL: https://rg.ru/2013/12/30/extrem-site-dok.html (date of access: 14.05.2019).

2. URL: https://rg.ru/2017/06/09/deti-dok.html (date of access: 15.05.2019).

3. URL: https://rg.ru/2017/03/09/putin-prizval-uzhestochit-otvetstvennost-za-sklonenie-detej-k-suicidu.html (date of access: 15.05.2019).

4. URL: https://rg.ru/2018/12/20/472-fz-dok.html (date of access: 15.05.2019).

5. URL: http://publication.pravo.gov.ru/Document/View/0001201903180022?index=0&rangeSize=1 (date of access: 15.05.2019).

6. URL: http://publication.pravo.gov.ru/Document/View/0001201903180031 (date of access: 15.05.2019).

7. URL: http://publication.pravo.gov.ru/Document/View/0001201903250016?index=0&rangeSize=1 (date of access: 15.05.2019).

8. URL: http://publication.pravo.gov.ru/Document/View/0001201905010025?index=0&rangeSize=1 (date of access: 15.05.2019).

9. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1532348683434&uri=CELEX:02016R0679-20160504 (date of access: 16.05.2019).

10. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:31995L0046&from=en (date of access: 16.05.2019).

11. URL: https://www.govinfo.gov/content/pkg/PLAW-107publ56/pdf/PLAW-107publ56.pdf (date of access: 16.05.2019).

12. Савельев А.И. Проблемы применения законодательства о персональных данных в эпоху «Больших данных» (Big Data) // Право. Журнал Высшей школы экономики. 2015. № 1; Savelyev A.I. The Issues of Implementing Legislation on Personal Data in the Era of Big Data // Law. Journal of The Higher School of Economics. 2015. № 1.

СВЕДЕНИЯ ОБ АВТОРАХ

Рабчевский Евгений Андреевич, генеральный директор ООО «СЕУСЛАБ», старший преподаватель кафедры компьютерных систем и телекоммуникаций Пермского государственного национального исследовательского университета; e-mail: e.rabchevskiy@seuslab.ru;

Никитин Дмитрий Алексеевич, кандидат физико-математических наук, директор по науке ООО «СЕУСЛАБ»; e-mail: d.nikitin@seuslab.ru

INFORMATION ABOUT AUTHORS

E.A. Rabchevskiy, Chief Executive Officer in SEUSLAB Ltd, Senior Lecturer of the Chair of Computer Systems and Telecommunications of the Perm State University; e-mail: e.rabchevskiy@seuslab.ru;

D.A. Nikitin, Candidate of Physics and Mathematics, Chief Research Officer in SEUSLAB Ltd; e-mail: d.nikitin@seuslab.ru