ПРАВОВЫЕ ПРОБЛЕМЫ ПРЕСЕЧЕНИЯ ИСПОЛЬЗОВАНИЯ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ И СВЯЗИ В ПРОТИВОПРАВНЫХ ЦЕЛЯХ

Сегодня очевидно не только прогрессивное применение информационных технологий и связи, но и реальная опасность их деструктивного использования. В этой связи особенно важно развитие правового регулирования общественных отношений, связанных с предотвращением распространения информации посредством использования информационно-телекоммуникационных сетей, и особенно недопущением распространения информации террористического и экстремистского характера.

Этот аспект приобретает еще большую актуальность еще и потому, что террористы и экстремисты используют информационные технологии для распространения своих аудиовизуальных записей, электронных сообщений и размещают информацию на интернет-сайтах.

Основные принципы распространения информации с использованием ИТ определены в Декларации Комитета министров Совета Европы о свободе выражения мнений и информации СМИ в контексте борьбы с терроризмом от 02.03.2005 года; Декларации о свободе общения в Интернете (2003 год); Рекомендациях Парламентской Ассамблеи Совета Европы №1706 (2005 год) «Средства массовой информации и терроризм»; Рекомендациях №R (2001 год) Комитета министров Совета Европы «О вопросах регулирования виртуального содержания (саморегулирование и охрана пользователей от противоправного или причиняющего вред содержания новых информационных и коммуникационных услуг)» от 05.09.2001 года; Дополнительном протоколе к Конвенции о киберпреступности относительно введения уголовной ответственности за правонарушения, связанные с проявлением расизма и ксенофобии, совершенные посредством компьютерных систем, от 28.01.2003 года и других.

В настоящее время в ряде государств – участников Содружества Независимых Государств приняты законы о противодействии экстремизму и терроризму, содержащие нормы о запрете распространения противоправной информации. Особого внимания заслуживают нормы законов Республики Молдова и Республики Беларусь, связанные с отнесением к экстремистской деятельности предоставления информационных услуг.

К информационным услугам в указанных государствах в соответствии с законами «Об информатике» и «Об информатизации» соответственно отнесены предлагаемые на рынке услуги по использованию программных продуктов, оборудования и информационных систем, а также информационная деятельность по доведению до пользователя информационной продукции, проводимая в определенной форме. Аналогичная схема развития правового регулирования применяется и в Российской Федерации.

Государственной Думой РФ принят Федеральный закон «О внесении изменений в отдельные законодательные акты Российской Федерации в связи с совершенствованием государственного управления в области противодействия экстремизму». Статьей 8 указанного закона устанавливаются новые дефиниции, определяющие критерии экстремистской деятельности, к которым отнесено и оказание информационных услуг.

В этой связи представляется, что для дальнейшего развития федерального законодательства в сфере информационной безопасности необходимо внесение изменений в принятый в 2006 году базовый Закон «Об информации, информационных технологиях и о защите информации». При этом особенно острым становится вопрос о совершенствовании дефиниций, определяющих понятийный аппарат в информационной сфере, в частности, в указанном законе не определено содержание понятия информационной услуги. В дальнейшем соответственно встает вопрос об ответственности за противоправные деяния, совершаемые с использованием предоставления информационных услуг в противоправных целях, что актуально и в рамках международной информационной безопасности.

В пункте 6 статьи 10 Федерального закона «Об информации, информационных технологиях и о защите информации» установлен запрет распространения информации, направленной на пропаганду войны, разжигание национальной, расовой или религиозной

ненависти и вражды, а также иной информации, за распространение которой предусмотрена уголовная или административная ответственность. Кроме того, федеральными законами может быть предусмотрена обязательная идентификация личности, организаций, использующих информационно-телекоммуникационную сеть при осуществлении предпринимательской деятельности. При этом получатель электронного сообщения, находящийся на территории Российской Федерации, вправе провести проверку, позволяющую установить отправителя электронного сообщения, а в установленных федеральными законами или соглашением сторон случаях обязан провести такую проверку (пункт 4 статьи 15).

Правовые нормы, направленные на противодействие распространению экстремистской и террористической информации и устанавливающие ответственность за осуществление такой деятельности, содержатся в федеральных законах от 25.07.2002 №114-ФЗ «О противодействии экстремистской деятельности» (статьи 1, 8, 11, 12, 13, 15, 17); от 07.07.2003 №126-ФЗ «О связи» (статьи 13, 29–40); от 06.03.2006 №35-ФЗ «О противодействии терроризму» (статья 3); Кодексе РФ об административных правонарушениях (статья 20.3,часть 1 статьи 20.27, статья 20.28); Уголовном кодексе РФ (статьи 205, 205.1, 205.2, 280, 282, 282.2) и других.

Как средство или способ совершения преступления, а также средство связи глобальные компьютерные сети могут использоваться при подготовке и совершении преступлений, предусмотренных статьями 206, 208, 211, 272–274, 277 УК РФ и рядом других.

Федеральным законом «О противодействии экстремистской деятельности» установлен запрет на распространение информации экстремистского толка, в частности на распространение через средства массовой информации экстремистских материалов и использование сетей связи общего пользования для осуществления экстремистской деятельности.

В соответствии со статьей 13 Федерального закона на территории Российской Федерации запрещено издание и распространение печатных, аудио-, аудиовизуальных и иных материалов, содержащих хотя бы один из признаков экстремистской деятельности.

В соответствии со статьей 3 Федерального закона «О противодействии терроризму» террористическая деятельность включает в себя информационное пособничество в планировании, подготовке или реализации террористического акта; пропаганду идей терроризма, распространение материалов или информации, призывающих к осуществлению террористической деятельности либо обосновывающих или оправдывающих необходимость осуществления такой деятельности.

Указанный Федеральный закон допускает ведение контроля за информацией, передаваемой по каналам телекоммуникационных систем, а также осуществление поиска на каналах электрической связи в целях выявления информации об обстоятельствах совершения террористического акта, о лицах, его подготовивших и совершивших, и в целях предупреждения совершения других террористических актов.

Кроме того, данный Федеральный закон вводит такие меры, как приостановление оказания услуг связи юридическим и физическим лицам или ограничение использования сетей связи и средств связи.

В настоящее время существует тенденция к расширению сферы правового регулирования противодействия терроризму и экстремизму в федеральном законодательстве.

Федеральным законом «О внесении изменений в отдельные законодательные акты Российской Федерации в связи с совершенствованием государственного управления в области противодействия экстремизму» вносятся изменения в Закон Российской Федерации «О средствах массовой информации» и устанавливается запрет на распространение информации об общественном объединении или иной организации, в отношении которых судом принято вступившее в законную силу решение суда о ликвидации или запрете деятельности по основаниям, предусмотренным Федеральным законом «О противодействии экстремистской деятельности», без указания на данное решение суда.

Заслуживает внимания опыт правового регулирования Республики Казахстан. Законом «О противодействии экстремизму» установлено, что уполномоченный орган по делам СМИ проводит мониторинг продукции СМИ на предмет недопущения в них пропаганды и оправдания экстремизма.

В соответствии с Федеральным законом «Об оперативно-розыскной деятельности» прослушивание телефонных и иных переговоров допускается только в отношении лиц, подозреваемых или обвиняемых в совершении тяжких или особо тяжких преступлений, а также лиц, которые могут располагать сведениями об указанных преступлениях. Фонограммы, полученные в результате прослушивания телефонных и иных переговоров, хранятся в опечатанном виде в условиях, исключающих возможность их прослушивания и тиражирования посторонними лицами.

Статьей 64 Федерального закона «О связи» установлены правовые основания предоставления уполномоченным государственным органам, осуществляющим оперативно-розыскную деятельность или обеспечение безопасности Российской Федерации, информации о пользователях услугами связи и об оказанных им услугах связи, а также иной информации, необходимой для выполнения возложенных на эти органы задач, в случаях, установленных федеральными законами, операторами связи.

Постановлением Правительства РФ от 27 августа 2005 года №538 утверждены Правила взаимодействия операторов связи с уполномоченными государственными органами, осуществляющими оперативно-розыскную деятельность. Указанные Правила определяют порядок взаимодействия операторов связи с уполномоченными государственными органами, осуществляющими оперативно-розыскную деятельность с использованием технических средств, обеспечивающих эту деятельность в сети связи оператора связи, при предоставлении оператором связи уполномоченным органам информации об абонентах и оказанных им услугах связи, а также иной информации, необходимой для выполнения возложенных

на уполномоченные органы задач в порядке и случаях, установленных федеральными законами.

Оператор связи обязан своевременно обновлять информацию, содержащуюся в базах данных об абонентах оператора связи и оказанных им услугах связи. Указанная информация должна храниться оператором связи в течение 3 лет и предоставляться органам ФСБ и органам МВД путем осуществления круглосуточного удаленного доступа к базам данных.

Статьей 3 вышеназванного Федерального закона внесены изменения в статью 8 Федерального закона «Об оперативно-розыскной деятельности» и установлен новый порядок оперативно-розыскной деятельности с использованием технических средств.

В соответствии с Федеральным законом от 04.04.2007 №32-ФЗ «Об Общественной палате Российской Федерации» Общественная палата призвана обеспечить согласование общественно значимых интересов граждан Российской Федерации, общественных объединений, органов государственной власти и органов местного самоуправления путем привлечения граждан, общественных объединений и представителей СМИ к обсуждению вопросов, касающихся соблюдения свободы слова в СМИ, реализации права граждан на распространение информации законным способом, обеспечения гарантий свободы слова и свободы массовой информации и выработки по данным вопросам рекомендаций.

Представляется, что вопросы противодействия использованию информационно-телекоммуникационных сетей в целях распространения противоправной информации должны стать широким достоянием общественности именно с учетом соответствующих полномочий Общественной палаты Российской Федерации.

Интернет наряду с объективными благами впитал в себя, к сожалению, и многие пороки общества и создает принципиально новые угрозы, не совместимые с задачами поддержания мировой стабильности и безопасности.

К ним можно отнести и распространение информации об изготовлении наркотиков, отравляющих и взрывчатых веществ, незаконную торговлю оружием, осуществление связи посредством этой информационно-телекоммуникационной системы между преступными формированиями. Интернет также является мощным средством идеологической поддержки и информационных воздействий деструктивных экстремистских организаций. Интернет используется для создания баз разведывательных данных, перехвата информации правоохранительных органов, пропаганды террористических и экстремистских взглядов, вербовки сообщников, сбора пожертвований, размещения руководств по организации терактов, психологического терроризма, сбора информации о предполагаемых целях и объектах шантажа, подготовки террористов, пропаганды расовой, религиозной и других форм нетерпимости.

Сложность урегулирования вопросов ответственности и осуществления противодействия распространению противоправной информации в информационно-телекоммуникационных системах, в том числе Интернете, определяется такими их свойствами, как анонимность, экстерриториальность и саморегулирование, что позволяет радикальным организациям регистрировать доменные имена сайта в одной стране, размещая при этом информацию в другой. В то же время в настоящее время существует и проблема определения признаков сайтов, пропагандирующих терроризм и экстремизм.

В ряде европейских государств, например во Франции, приняты законы, в которых предусмотрена обязательная регистрация всех владельцев веб-сайтов и обязанность провайдеров сообщать сведения об авторах сайтов любому заинтересованному третьему лицу, при этом запрещается предоставление хостинга неидентифицированным пользователям. За нарушение этих норм установлена уголовная ответственность провайдеров. Также предусматривается уголовная ответственность и авторов сайтов за предоставление неполных или недостоверных личных данных. Введена проверка на уровне провайдера, а все сайты, авторство которых не установлено, переходят под ответственность провайдера. В рамках законов по борьбе с организованной преступностью и с особо опасными преступлениями предусматривается наказание в виде трех лет лишения свободы за распространение любыми техническими средствами информации, позволяющей изготовлять технические устройства.

В Великобритании фильтрация контента (содержания) интернет-ресурсов осуществляется Национальным отделением по борьбе с преступлениями в сфере высоких технологий. Существует также «горячая линия» по разбору жалоб по этим вопросам – «Фонд Интернет Наблюдения». Провайдер обязан после получения информации о противоправности содержания немедленно удалить материал с сервера, в этом случае провайдер не подвергается преследованию.

Ряд проблем может быть решен в рамках оказания правовой помощи по уголовным делам, что вытекает, например, из Европейской конвенции о взаимной правовой помощи по уголовным делам от 20.04.1959 года, Европейской конвенции о передаче судопроизводства по уголовным делам от 15.05.1972 года. В рамках СНГ действуют Конвенции о правовой помощи и правовых отношениях по гражданским, семейным и уголовным делам от 22.01.1993 года и от 07.10.2002 года. Российской Федерацией заключено также более 20 двусторонних соглашений в этой области с различными государствами. Порядок оказания правовой помощи и взаимодействия с судебными и правоохранительными органами компетентных государств регулируется статьями 453–459 Уголовно-процессуального кодекса Российской Федерации. Однако при применении положений данных нормативных актов необходимо учитывать, что распространение вредоносной информации в глобальных информационно-телекоммуникационных системах, а также другие правонарушения в этой сфере, признаваемые таковыми в одном или группе государств, в других государствах могут не рассматриваться как противоправные. В связи с этим очевидна роль международных процессов, направленных на достижение международных договоренностей в этой области.

Важно отметить, что статьей 12 УК РФ допускается привлечение к уголовной ответственности в соответствии с законодательством Российской Федерации также иност-

ранных граждан и лиц без гражданства, не проживающих постоянно на ее территории, за преступления, совершенные за границей против интересов Российской Федерации. Необходима гармонизация международных правовых норм и унификация национальных законодательств государств, определяющих составы правонарушений в сфере Интернета, выработка единого подхода к установлению юрисдикции и развитие соответствующих положений Конвенции о киберпреступности, а также заключение соответствующих межгосударственных соглашений.

Представляется важным также решение проблемы наделения правоохранительных органов полномочиями по осуществлению общего мониторинга сетей передачи данных, включая Интернет.

Требуют решения вопросы формирования «пространства доверия», идентификации пользователей Интернета, регистрации доменных имен и интернет-сайтов. Общеизвестно, что порядок регистрации доменных имен регулируется Правилами регистрации доменных имен в домене RU, утвержденными решением Координационного центра национального домена в сети Интернет от 24.04.2006 №П2-2.1,4.1/06, в которых предусмотрено предоставление для регистрации сведений, необходимых для идентификации администратора домена (имя, место жительства физического лица, документ, удостоверяющий личность; наименование, место нахождения и сведения о государственной регистрации юридического лица). Однако среди оснований для отказа в регистрации и для аннулирования регистрации (пункт 4.4., разделы 5 и 8 Правил) отсутствует такое основание, как использование домена для ведения противоправной деятельности. В качестве основания прекращения права администрирования не указано также решение суда, устанавливающего факт использования доменного имени для осуществления противоправной деятельности. Информация третьим лицам о доменном имени и сведения об администраторе предоставляются посредством сервиса «whois», а также по запросу суда и в иных установленных законом случаях в объеме, ограниченном целями запроса (пункты 3.2, 3.4). Сведения о точном полном наименовании (имени) и месте нахождения администратора могут быть сообщены третьим лицам исключительно для целей предъявления судебного иска. При этом регистратор обязан по запросу администратора предоставить ему информацию о лицах, которым были сообщены указанные сведения. Все это не исключает возможность регистрации домена от имени подставного лица или организации.

В законодательстве Российской Федерации для пресечения распространения противоправной информации не предусмотрена возможность аннулирования лицензии провайдера, размещающего сайты террористического или экстремистского характера, после вынесения соответствующего предупреждения и внесения сведений об аннулировании лицензии в реестр. Отсутствует ответственность провайдеров за размещение в компьютерных сетях материалов, признанных экстремистскими по решению суда, или возобновление деятельности сайта, закрытого по мотивам размещения террористических или экстремистских материалов, а также возможность административного приостановления деятельности интернет-провайдера, допускающего размещение материалов противоправного характера.

В Правилах регистрации доменных имен целесообразно предусмотреть: возможность прекращения права администрирования, если по решению суда сайт признан террористическим (экстремистским), либо к организации предъявлен иск о ликвидации по мотивам экстремистской деятельности, блокировку доменного имени при наличии возбужденного уголовного дела по факту террористической или экстремистской деятельности по мотивированному постановлению правоохранительных органов; запрет на совершение сделок с доменным именем по этим основаниям; обязанность регистратора сообщать информацию о доменном имени и администраторе по запросу правоохранительных органов и обеспечивать конфиденциальность сведений о факте запроса и о передаче сведений.

Представляется целесообразным также создание системы интернет-контента, позволяющей предотвращать распространение на интернет-сайтах противоправной информации.

Правовое урегулирование проблем противодействия использованию Интернета в террористических и экстремистских, а также в иных противоправных целях необходимо для обеспечения информационной безопасности личности, общества и государства, а также является важной составляющей обеспечения международной информационной безопасности.

Вопросы правового регулирования пресечения распространения противоправной информации посредством использования информационных технологий и предоставления информационных услуг нуждаются также в дополнительном обсуждении с привлечением представителей международного сообщества и общественности.

ЗАМЕСТИТЕЛЬ ДИРЕКТОРА ДЕПАРТАМЕНТА
КОНСТИТУЦИОННОГО ЗАКОНОДАТЕЛЬСТВА
И ЗАКОНОДАТЕЛЬСТВА О БЕЗОПАСНОСТИ МИНЮСТА РОССИИ
Т.А. Полякова,
СОВЕТНИК ОТДЕЛА УГОЛОВНОГО ЗАКОНОДАТЕЛЬСТВА
И ЗАКОНОДАТЕЛЬСТВА О БЕЗОПАСНОСТИ ДЕПАРТАМЕНТА
КОНСТИТУЦИОННОГО ЗАКОНОДАТЕЛЬСТВА
И ЗАКОНОДАТЕЛЬСТВА
О БЕЗОПАСНОСТИ МИНЮСТА РОССИИ
Е.В. Семизорова