Statut Publishers
ИЗДАТЕЛЬСТВО СТАТУТ

А.И. САВЕЛЬЕВ

ЭЛЕКТРОННАЯ КОММЕРЦИЯ В РОССИИ И ЗА РУБЕЖОМ:

правовое регулирование

СТАТУТ
МОСКВА 2014

УДК 341
ББК 67.412.2
С 12

Савельев А.И.
С 12 **Электронная коммерция в России и за рубежом: правовое регулирование**. – М.: Статут, 2014. – 543 с.

ISBN 978-5-8354-1018-7 (в пер.)

Монография посвящена анализу вопросов, возникающих при осуществлении деятельности в сфере электронной коммерции: юрисдикционных аспектов электронной коммерции; перспектив исполнения решения, вынесенного на территории иностранного государства; общих проблем заключения договоров в сети Интернет; использования электронных подписей, персональных данных и др.

Для предпринимателей, ведущих деятельность в сфере электронной коммерции, практикующих юристов, представителей научного сообщества, а также всех, интересующихся данной темой.

УДК 341
ББК 67.412.2

ISBN 978-5-8354-1018-7

посвящается моему Учителю –
профессору Марине Николаевне Малеиной,
без усилий и таланта которой эта работа
вряд ли бы появилась

Оглавление

Введение

Интернет является ядром современной мировой экономики и основной движущей силой инновационного развития. Значение сети Интернет для современного бизнеса весьма емко охарактеризовано в приписываемом бывшему главе *Microsoft* Биллу Гейтсу (*Bill Gates*) высказывании: «В будущем на рынке останутся два вида компаний: те, кто в Интернете, и те, кто вышел из бизнеса». Можно по-разному относиться к данному утверждению, но последнее десятилетие весьма убедительно продемонстрировало особую роль информационно-телекоммуникационных технологий в развитии бизнеса. В наибольшей степени это нашло свое проявление в появлении и развитии особой сферы экономической деятельности – электронной коммерции.

Электронная коммерция стала неотъемлемой частью современной экономики. Все больше потребителей приобретают товары посредством сети Интернет, а коммерческие организации так или иначе используют возможности данной сети при осуществлении предпринимательской деятельности. Общий мировой объем продаж в одном только потребительском сегменте электронной коммерции превысил в 2012 г. отметку в 1 трлн долл. и характеризуется устойчивым ростом[1]. Рынок электронной коммерции в Европе достиг 312 млрд евро в 2012 г. Россия заняла пятое место по объему рынка электронной коммерции после Великобритании, Германии, Франции и Испании, при этом доля России составила порядка 10,3 млрд евро в 2012 г. с приростом 35% по сравнению с 2011 г.[2] Эти сухие цифры показывают, что феномен электронной коммерции имеет весьма радужные перспективы с экономической точки зрения, а следовательно, вопросы ее правового регулирования приобретают особую актуальность.

Однако на фоне бурного развития электронной коммерции освещение данного явления в отечественной юридической литературе выглядит достаточно бледно. Многие работы по данной тематике, несмотря

---

[1] Ecommerce Sales Topped $ 1 Trillion for First Time in 2012. 05.02.2012 // http://www.emarketer.com/Article/Ecommerce-Sales-Topped-1-Trillion-First-Time-2012/1009649#t8zvCcCjOogMAZ-31.99

[2] Europe B2C Ecommerce Report 2013. Brussels // https://www.ecommerce-europe.eu/website/facts-figures/light-version/download%20

на несомненную научную ценность некоторых из них, являются либо устаревшими, либо фрагментарными, либо описательными. Любое из указанных качеств является важным для понимания электронной коммерции.

Как известно, законодательство в этой сфере развивается достаточно динамично, и то, что имеет место сейчас, существенным образом отличается от того, что было 5 и уж тем более 10 лет назад. Если учитывать трансграничный характер сети Интернет, а вместе с ним и характер электронной коммерции, становится очевидным, что в отрыве от положений зарубежного законодательства в указанной сфере, а также анализа сопутствующих юрисдикционных проблем невозможно нарисовать более-менее четкую картину правового регулирования в указанной сфере.

К тому же многие вопросы, традиционно рассматриваемые в отечественной литературе раздельно, требуют комплексного анализа. Например, вопросы получения согласия пользователя сети Интернет на обработку персональных данных нередко неразрывно связаны с вопросами действительности условий так называемых *click-wrap-* и *browse-wrap*-соглашений, которая должна оцениваться через призму положений международного частного права и международного гражданского процесса. Именно поэтому данная книга объединяет в себе темы хотя и разнородные с точки зрения их отраслевой принадлежности, но имеющие непосредственное отношение к проблематике электронной коммерции. В результате содержание книги может показаться несколько эклектичным, однако оно отражает достаточно простой факт: право электронной коммерции, так же как и интернет-право, киберправо и иные популярные ныне обозначения, не представляет собой самостоятельной отрасли права с единой концепцией. Они представляют собой комплекс разнородных по своей отраслевой природе вопросов, объединенных общностью предмета, к которому они относятся[1].

Глава 1 книги рассматривает понятие электронной коммерции. В отличие от многих иных дефиниций данного явления, существующих в литературе, в данной книге оно связано исключительно с экономическими отношениями, возникающими в сети Интернет, поскольку именно благодаря ей оно оформилось, приобрело те масштабы,

[1] Безусловно, существуют и иные точки зрения на этот счет, в том числе обосновывающие самостоятельность интернет-права как отрасли. Но поскольку данная работа все же не об интернет-праве, я могу себе позволить роскошь не вдаваться в данную дискуссию, тем более что в российских реалиях она носит не столько научный, сколько коньюнктурно-научный характер.

которые имеет сейчас и получило «в нагрузку» многие проблемы, о которых будет говориться в других главах книги. Поскольку многие правовые проблемы, возникающие в сфере электронной коммерции, предопределены техническими особенностями архитектуры сети Интернет, которые в свою очередь обусловлены особенностями появления и развития данной сети, мне показалось целесообразным посвятить данным вопросам отдельные параграфы.

Глава 2 посвящена рассмотрению на примере США, Европейского союза и России юрисдикционных аспектов электронной коммерции: компетентности суда по рассмотрению того или иного спора, возникающего в сфере электронной коммерции; определения права, применимого к такому спору; а также перспектив последующего исполнения вынесенного решения на территории иностранного государства. Подробное рассмотрение законодательства США и стран Европейского союза по данным вопросам обусловлено тем фактом, что рынки данных стран играют важную роль в сфере электронной коммерции и в силу этого факта их законодательство должно учитываться при ведении деятельности с клиентами из данных правопорядков или, наоборот, при желании ограничить риски, связанные с подпаданием под их юрисдикцию. К тому же доктрина и законодательство данных правопорядков по вопросам юрисдикции отличаются высоким уровнем развития и нередко заимствуются российским законодателем, в связи с чем всегда полезно знать «истоки».

Глава 3 рассматривает общие вопросы заключения договоров в сети Интернет путем обмена документами или акцепта оферты конклюдентными действиями, проблемы использования электронных подписей и электронных агентов при заключении договора, а также особенностей одностороннего изменения и расторжения договоров, заключенных в онлайн-режиме. Особое внимание уделяется рассмотрению особого рода договоров, которые нередко именуются как *click-wrap*- и *browse-wrap*-соглашения и представляют собой новый уровень эволюции договорной практики, развивающий идеи договоров присоединения в электронной среде.

Глава 4 представляет собой развитие положений предыдущей главы и рассматривает вопросы использования информации, содержащейся в сети Интернет (переписки по электронной почте и данных, размещенных на веб-сайтах) в качестве доказательств в гражданском и арбитражном процессе. Учитывая легкость, с которой можно изменить или удалить информацию в сети Интернет, затрудняя тем самым защиту нарушенных прав других лиц, особый интерес представляют

собой интернет-архивы, позволяющие в ряде случаев находить некогда размещенную на веб-сайте информацию. В данной главе приводится судебная практика использования информации из таких интернет-архивов на примере *Wayback Machine*.

Глава 5 посвящена веб-сайту как одному из основных инструментов электронной коммерции. Достаточно подробно рассматриваются вопросы его правовой природы, а также правовые аспекты его введения в действие: договор на разработку веб-сайта, регистрация доменного имени и размещение веб-сайта на хостинговой площадке. Поскольку многие веб-сайты, задействованные в сфере электронной коммерции, носят высокоинтерактивный характер и позволяют размещать пользовательский контент, возникает ряд вопросов, связанных с разграничением ответственности между владельцами ресурса, провайдерами хостинга и пользователями за такой контент.

В главе 6 рассматриваются вопросы, связанные с цифровым контентом. В частности, анализ правовой природы существующих бизнес-моделей его распространения. Особое внимание уделяется распространению программного обеспечения в цифровой форме: в виде предоставления ссылок для загрузки и в виде предоставления удаленного доступа к нему (программное обеспечение как услуга). Поскольку все больше и больше пользователей сети Интернет становятся участниками различного рода многопользовательских игр и иных подобных проектов, все более актуальным становится вопрос о правовом статусе внутриигровых объектов, приобретаемых за реальные деньги. Несмотря на то что правовое регулирование подобной виртуальной «собственности» находится в зачаточном состоянии, уже сейчас есть судебная практика, позволяющая задуматься о дальнейших путях развития данного явления. В связи с этим мне показалось целесообразным выделить данный вопрос в отдельный параграф, хотя, конечно, он заслуживает гораздо большего внимания.

Электронная коммерция немыслима без новых форм платежей, в значительной степени облегчающих реализацию товаров и услуг в электронной среде. Феномен электронных денег достаточно долго будоражил умы экономистов и юристов как в России, так и за рубежом. В значительной степени вопросы, связанные с правовым статусом электронных денег, были разрешены с принятием Федерального закона от «О национальной платежной системе». Однако появляются все новые и новые средства платежей в сети Интернет, отдельные из которых носят настолько инновационный характер, что возможности их правового регулирования существенно ограниченны. Речь идет

о различного рода децентрализованных виртуальных валютах вроде *Bitcoin*, которые не получали еще подробного освещения в отечественной юридической литературе. Рассмотрению вопросов, связанных с электронными деньгами посвящена глава 7 книги.

В главе 8 рассматриваются вопросы использования сети Интернет в рекламных целях. В частности, при каких условиях информация, размещенная на веб-сайте, может рассматриваться в качестве рекламы с распространением на нее специальных требований законодательства о рекламе; особенности размещения рекламы в баннерообменных сетях и поисковых сервисах, а также проблемы борьбы со спамом.

Завершает книгу глава, посвященная вопросам регулирования персональных данных, поскольку большинство предпринимателей, ведущих деятельность в сфере электронной коммерции, вынуждены так или иначе обрабатывать массив персональных данных своих действительных или потенциальных клиентов. В связи с этим возникает множество вопросов, связанных с получением согласия на обработку таких данных, принятием необходимых организационно-технических мер по их защите, передачей персональных данных на обработку третьим лицам, трансграничной передачей и т.д. Особый интерес в контексте ведения трансграничной коммерческой деятельности представляют собой планируемые изменения в законодательстве о персональных данных Европейского союза, поскольку именно оно является «источником вдохновения» для многих других стран, включая Россию.

К сожалению, некоторые вопросы, главным образом публично-правового характера (вопросы налогообложения, уголовно-правовой ответственности за нарушения в указанной сфере, лицензирования и сертификации и пр.), остались за рамками данной книги в силу ряда причин, в том числе и ради соблюдения разумного объема. Я надеюсь, что в последующих работах по данной тематике мне удастся восполнить хотя бы отчасти указанные пробелы. Так или иначе, не претендуя на бесспорность высказанных суждений, я буду признателен за отзывы и комментарии к данной книге, которые можно отправлять по адресу: *alexandersavelyev@outlook.com*.

Тексты нормативных правовых актов приведены по состоянию на 1 октября 2013 г. Высказанные в настоящей книге суждения являются личным мнением автора и могут не совпадать с официальной позицией компании *IBM*.

Глава 1. Понятие электронной коммерции

§ 1. Вопросы терминологии

Электронная коммерция – достаточно неблагодарный термин с точки зрения поиска его дефиниции. В отсутствие сформулированного в российском законодательстве определения данного явления[1] приходится довольствоваться теми дефинициями, которые содержатся либо в зарубежном законодательстве и международных актах, либо в отечественной и зарубежной доктрине.

Данная книга не преследует цели консолидации всего многообразия имеющихся определений данного явления, тем более что при наличии особого интереса к данному вопросу можно обратиться к ряду существующих работ[2]. Что хотелось бы сделать здесь, так это, во-первых, разграничить термины «электронный бизнес» (*e-business*) и «электронная коммерция» (*e-commerce*) по причине того, что в индустрии информационных технологий в них вкладывается различный смысл. Во-вторых, сформулировать рабочее определение электронной коммерции, пригодное для рассмотрения вопросов, охватываемых данной книгой. В-третьих, сказать несколько слов о популярном в отечественной литературе термине «электронная торговля» и его возможном соотношении с понятием «электронная коммерция».

Считается, что термин «электронный бизнес» был впервые сформулирован президентом корпорации *IBM* Луи Герстнером (*Louis Gerstner*)

---

[1] Данный термин, хотя и без дефиниции, все же употребляется в российских правовых актах. См., например: постановление Правительства РФ от 19 марта 2002 г. № 169 «О Федеральной целевой программе «Экономическое и социальное развитие Дальнего Востока и Забайкалья на 1996–2005 и до 2010 года»» // СЗ РФ. 2002. № 13. Ст. 1208; п. 118 ч. 7 Положения о Министерстве экономического развития и торговли Российской Федерации, утвержденного постановлением Правительства РФ от 21 декабря 2000 г. № 990 «Об утверждении Положения о Министерстве экономического развития и торговли Российской Федерации» // СЗ РФ. 2001. № 1 (ч. II). Ст. 125.

[2] *Васильева Н.М.* Электронная коммерция как правовая категория // Юрист. 2006. № 3; *Карев Я.А.* Электронные документы и сообщения в коммерческом обороте: правовое регулирование. М., 2006. С. 42–48; *Тедеев А.А.* Электронная коммерция (электронная экономическая деятельность). Правовое регулирование и налогообложение. М., 2002. С. 14 и др.

в 1996 г.[1] В самом общем виде под ним понимается любое использование интернет-технологий для трансформации и оптимизации бизнес-процессов[2]. Можно выразить данную мысль и несколько иначе: электронный бизнес – это любой процесс, осуществляемый коммерческой организацией с использованием компьютерных сетей[3].

Такое использование интернет-технологий может иметь как внутренние аспекты, так и внешние. К внутренним можно отнести применение в масштабах компании систем управления взаимоотношениями с клиентами (*CRM*); систем планирования ресурсов предприятия (*ERP*); систем управления персоналом (*HRM*) и др. Данные системы имеют в своей основе специализированное программное обеспечение, которое унифицирует и сводит соответствующие бизнес-процессы воедино. Для обмена данными, поступающими из различных подразделений территориально распределенной организации, используются интернет-технологии. К внешним аспектам электронного бизнеса можно отнести процессы, связанные со взаимодействием с третьими лицами посредством использования интернет-технологий, главным образом для целей заключения и исполнения договоров. Обычно именно этот внешний аспект и именуется электронной коммерцией. Таким образом, понятие электронного бизнеса шире понятия электронной коммерции за счет включения в него различных информационных технологий, направленных на оптимизацию *внутренних* бизнес-процессов компании[4]. Электронная коммерция является, таким образом, разновидностью электронного бизнеса, представляя собой отношения, связанные с заключением, исполнением сделок посредством сети Интернет.

В подобном ключе электронная коммерция понимается, например, в законодательстве США, где под данным термином для налоговых целей понимаются «любые сделки, совершаемые через Интернет или с использованием доступа к Интернету, включая куплю-продажу, предоставление имущества в пользование, лицензирование, оферту на совершение вышеуказанных действий или предоставление прав на имущество, товары, услуги или информацию за плату или без; дан-

---

[1] *Maney K., Hamm S., O'Brien J.* Making the World Work Better: The Ideas that Shaped a Century and a Company. IBM Press. P. 158–159.

[2] A Brief Intoduction to E-Business. IBM. October 2001. P. 3 // http://www.redbooks.ibm.com/-redbooks/pdfs/sg246711.pdf

[3] *Thomas L. Mesenbourg.* Measuring Electronic Business: Definitions, Underlying Concepts, and Measurement Plans. US Department of Commerce // http://www.census.gov/epcd/www/ebusines.htm

[4] *Sampson G.* Electronic business. The British Computer Society: Chippenham, 2008. P. XIX; *Winn J.*, *Wright B.* The Law of Electronic Commerce. § 1.02 (4th ed. 2002).

ный термин также включает предоставление доступа к Интернету»[1]. В Европе под электронной коммерцией принято понимать продажу товаров (услуг) в онлайн-режиме[2]. Министерство международной торговли и промышленности Японии под электронной коммерцией понимает «проведение коммерческих сделок (обмен товарами, услугами, информацией и (или) денежными средствами между поставщиками и потребителями в целях осуществления передачи товаров на коммерческой основе субъектами экономической деятельности) с помощью электронных средств с использованием интернет-технологий»[3].

Как следует из вышеуказанных определений, «ядром» электронной коммерции является транзакция (сделка), совершенная посредством сети Интернет. При этом не обязательно, чтобы такая транзакция носила возмездный характер. Предоставление доступа к электронному ресурсу, скачивание бесплатной программы в сети Интернет также могут охватываться понятием электронной коммерции, поскольку вокруг данных действий вполне могут быть построены эффективные бизнес-модели.

Учитывая, что заключению сделки обычно предшествуют определенные предварительные действия со стороны предпринимателя, направленные на продвижение товара, услуги или иного объекта прав на рынке в целом и в сети Интернет в частности, и данные действия оказывают непосредственное влияние на решение контрагента по совершению транзакции, подобные «подготовительные» действия, совершенные в сети Интернет, также должны включаться в понятие электронной коммерции. В таких случаях налицо тесная взаимосвязь между преддоговорным и договорным аспектами, которая обусловливает не только наличие специального регулирования преддоговорного аспекта[4], но и целесообразность совместного и целостного рассмотрения данных вопросов в рамках работы, посвященной электронной коммерции.

Вряд ли целесообразно включать в определение электронной коммерции упоминание иных сетей помимо Интернета[5], поскольку в на-

---

[1] Section 1104 (3) The Internet Tax Freedom Act, 1998.

[2] http://www.ecommerce-europe.eu/about

[3] Towards the Age of the digital Economy – For Rapid Progress in the Japanese Economy and World Economic Growth in the 21st Century. Ministry of International Trade and Industry, Government of Japan. 1997. Цит. по: *Васильева Н.М.* Указ. соч.

[4] См., например: Федеральный закон от 13 марта 2006 г. № 38-ФЗ «О рекламе» (далее – Закон о рекламе), ст. 9, 10 Закона РФ от 7 февраля 1992 г. № 2300-I «О защите прав потребителей» (далее – Закон о защите прав потребителей) (право потребителя на достоверную информацию о товаре (услуге) и контрагенте (изготовителе (продавце)).

[5] Как это предлагает делать, например, Т.Ю. Кулик, приводя при этом примеры таких сетей, которые остались в прошлом веке (ARPANET). См.: *Кулик Т.Ю.* Правовая природа электронной коммерции // Правовые вопросы связи. 2006. № 2.

стоящее время сеть Интернет либо поглотила существовавшие ранее коммерческие сети, которые могли использоваться для осуществления коммерческой деятельности, либо так или иначе является фундаментом для построения иных сетей, более закрытых.

Факсы, телексы, телефаксы и другие подобные средства связи, несмотря на наличие в них электронной составляющей, также не заслуживают быть охваченными понятием электронной коммерции в современных реалиях: многие из них безнадежно устарели и фактически уже не используются в деловом обороте. Они требуют наличия у каждого из участников коммуникаций громоздких и недешевых устройств и, что немаловажно, совместимых между собой. При этом такие устройства несут существенные ограничения по характеру возможной к передаче информации (например, звук или видео с их помощью не передашь), не позволяют осуществлять одновременное общение и содержат ряд иных недостатков.

Технологические условия участия в коммуникациях посредством факсов, телексов, телефаксов и прочих подобных средств связи, а также существенные ограничения, налагаемые на формат передаваемой информации, обусловливают тот факт, что многие актуальные вопросы электронной коммерции просто не возникают при использовании подобных технических средств из прошлого века: конфликт юрисдикций, обусловленный общедоступным характером веб-сайта, проблемы с новыми формами заключения договора (*click-wrap-* и *browse-wrap-*соглашения), правовая природа цифрового контента, спама и многие другие вопросы. Спрашивается, каков тогда практический смысл включения факсов, телексов, телефаксов, телеграмм и иных некогда актуальных средств связи в состав понятия электронной коммерции, если в большинстве случаев их использование не создает актуальных для современной электронной коммерции проблем? И если Типовому закону ЮНСИТРАЛ «Об электронной торговле» можно простить широкий и либеральный подход к дефиниции электронной коммерции по причине его разработки и принятия в середине 90-х гг. прошлого века, а также узкого спектра вопросов, затронутых в нем, то при современном уровне развития технологий такой подход можно объяснить лишь излишним консерватизмом, педантичностью и некоторой оторванностью от реальности. В конечном счете сфера электронной коммерции получила свое масштабное развитие только с приходом Интернета[1]. Как отмечается, именно сочетание развития рынка в сфере

[1] Online Contract Formation. Ed. by Stephan Kinsella and Andrew Simpson. Oceana Publications. N.Y., 2004. P. 483.

интернет-услуг, технологий в области дизайна веб-сайтов и новых вычислительных технологий в итоге и привело к появлению нового поколения коммерции – электронной коммерции[1]. Именно Интернет обеспечил существенное сокращение издержек, связанных с ведением предпринимательской деятельности (на рекламу, на аренду помещений, персонал и пр.), сократив тем самым время выхода на рынок (*go to market*). Наконец, именно трансграничная природа сети Интернет позволяет вести деятельность в мировом масштабе и получать выход на зарубежные рынки, а потребителям – получать выбор глобального масштаба[2]. Таким образом, не отрицая исторической значимости иных электронных видов связи, приходится сделать вывод о том, что их роль в современной электронной коммерции носит маржинальный характер, которым можно пренебречь при конструировании понятия «электронная коммерция».

В результате получается следующее определение электронной коммерции: «*электронная коммерция представляет совокупность отношений, возникающих в связи с ведением предпринимательской деятельности в сети Интернет, в частности при совершении сделок, а также при продвижении товаров, работ, услуг и иных объектов в сети Интернет*»[3].

Наконец, необходимо сказать несколько слов о термине «электронная торговля». Его появление в отечественной доктрине, с одной стороны, связано с тем, что английское слово «*commerce*» может быть переведено на русский и как «коммерция», и как «торговля»[4]. Отмечается, что немалую роль в популяризации термина «электронная торговля» играет и консерватизм отдельных представителей российской доктрины и чиновничества, предпочитающих «родные» русские эквиваленты заморских терминов[5]. Одним из критиков понятия

[1] См.: *Faye Fangrei Wang.* Internet Jurisdiction and Choice of Law: Legal Practices in the EU, US and China. Cambridge, 2010. P. 3.

[2] *Юрасов А.В.* Основы электронной коммерции. М., 2008. С. 27–28.

[3] Данное определение не отвечает признакам технологической нейтральности, так как прямо упоминает определенную технологию (Интернет) в качестве конститутивного признака. Признавая справедливость данного аргумента, полагаю, что можно было бы усовершенствовать данную дефиницию, использовав более нейтральный термин «информационно-телекоммуникационная сеть»: *электронная коммерция представляет собой совокупность возникающих в связи с совершением сделок, а также рекламированием товаров, услуг и иных объектов в сети Интернет и иных информационно-телекоммуникационных сетях.* Другое дело, что на данном этапе о наличии каких-либо иных информационно-телекоммуникационных сетей не приходится говорить.

[4] См., например: *Мюллер В.К.* Англо-русский словарь. М., 1956. С. 125.

[5] Достаточно подробно данный аспект рассматривает Н.М. Васильева. См.: *Васильева Н.М.* Указ. соч. Хотя, на мой взгляд, все гораздо проще. Основным источников вдохновения при рассмотрении проблематики электронной коммерции для данных кате-

«электронная коммерция» является А.А. Тедеев, заявляющий, что «эффективное государственное регулирование в Российской Федерации всех экономических видов деятельности, осуществляемых с использованием глобальной компьютерной сети Интернет, невозможно на основе правовых конструкций, в качестве несущих элементов которых выступят понятия «коммерция», «электронная коммерция», поскольку указанные термины «не имеют общепризнанного определения, наполненного юридическим содержанием, и различно трактуются в экономической теории и на практике»[1]. Данный автор предлагает взамен использовать понятие «экономическая деятельность, осуществляемая в электронной форме с использованием глобальной компьютерной сети Интернет» или для краткости просто «электронная экономическая деятельность»[2]. В связи с этим хотелось бы отметить следующее. Во-первых, предлагаемое автором понятие «экономическая деятельность» тоже не имеет общепризнанного определения, наполненного юридическим содержанием, о чем свидетельствуют споры специалистов в области арбитражно-процессуального права, в котором это понятие является одним из ключевых при определении подведомственности дела арбитражным судам. К тому же вряд ли столь апокалиптичные прогнозы о невозможности эффективного правового регулирования с вышеуказанными «несущими элементами» имеют под собой основание: как только будет дана законодательная дефиниция определенному явлению, его иным пониманием на практике и уж тем более в экономической теории можно будет в значительной степени пренебречь. Да и сама идея замены широко используемого в законодательствах зарубежных стран и мировой бизнес-практике термина на многословные конструкции, слабо отражающие существо отношений, вызывает мало сочувствия.

Существует ряд законопроектов с наименованием «Об электронной торговле», в которых предполагается урегулировать гражданско-правовые отношения, возникающие в сети Интернет. Для того чтобы оценить их качество, можно привести предложенные в них дефиниции понятия электронной торговли. В одном из них под электронной торговлей понималось «заключение путем обмена электронными документами

горий граждан был Типовой закон ЮНСИТРАЛ «On Electronic Commerce», официально переведенный на русский язык как закон «Об электронной торговле». Естественно, что пример столь уважаемой организации, как комиссии ЮНСИТРАЛ при ООН, весьма заразителен.

[1] *Тедеев А.А.* Электронная экономическая деятельность в сети Интернет // Законодательство и экономика. 2003. № 11.

[2] Там же.

следующих сделок, предусмотренных ГК РФ (но не ограничиваясь ими): купля-продажа, поставка, возмездное оказание услуг, перевозка, заем и кредит, финансирование под уступку денежного требования, банковский вклад, банковский счет, расчеты, хранение, страхование, поручение, комиссия, агентирование, доверительное управление имуществом, коммерческая концессия, простое товарищество, публичное обещание награды, публичный конкурс, а также приобретение и осуществление с использованием электронных средств иных прав и обязанностей в сфере предпринимательской деятельности»[1]. В другом законопроекте данный термин определялся как «система заключения с использованием электронных средств массовых коммуникаций предусмотренных действующим законодательством Российской Федерации сделок, направленных на приобретение и осуществление прав и обязанностей (покупка и продажа товаров, предоставление и получение услуг), в том числе в сфере предпринимательской деятельности, а также переговоры в связи с заключением таких сделок, оформляемые путем обмена электронными документами»[2]. Были и иные законопроекты с аналогичными наименованиями, которые постигла та же участь: они были либо отозваны, либо отклонены[3]. Однако настойчивость в использовании термина «электронная торговля» достаточно показательна. Представляется, что веских оснований для выделения самостоятельного термина «электронная торговля», кроме терминологически-патриотичных и конъюнктурных, все же нет. Бóльшая часть мира все равно будет использовать термин «электронная коммерция» как в правовых актах, так и в бизнес-лексике и коммерческой деятельности. Это неизбежно

[1] Статья 3 проекта федерального закона № 11081-3 «Об электронной торговле», внесенного 3 октября 2000 г. депутатами Государственной Думы РФ В.И. Волховским, Л.С. Маевским, О.А. Финько, А.В. Шубиным. При рассмотрении во втором чтении Постановлением ГД № 440-IV ГД от 24 апреля 2004 г. проект был снят с дальнейшего рассмотрения.

[2] Статья 2 проекта федерального закона № 47432-3 «Об электронной торговле», внесенного 12 января 2001 г. депутатом Государственной Думы РФ В.Я. Комиссаровым. 6 июня 2001 г. был отозван депутатом обратно.

[3] См., например: проект федерального закона № 310163-4 «Об электронной торговле», внесенного 16 июня 2006 г. депутатами В.Я. Комиссаровым, С.В. Ивановым, А.Н. Хайруллиным, К.В. Ветровым, А.А. Кармеевым, С.А. Насташевским, Б.Л. Резником, А.В. Островским, И.В. Лебедевым. Постановлением ГД № 5470-5 ГД от 15 июня 2011 г. законопроект был отклонен; проект федерального закона № 136018-4 «Об электронной торговле», внесенного 31 января 2005 г. В.Я. Комиссаровым, К.В. Ветровым, А.Н. Хайруллиным, снятый с рассмотрения в связи с отзывом его субъектом права законодательной инициативы; проект федерального закона № 132754-4 «Об электронной торговле», внесенного 24 января 2005 г. депутатами В.Л. Горбачевым, В.А. Язевым, снятый с рассмотрения в связи с отзывом субъектом права законодательной инициативы.

будет приводить к тому, что данный термин будет «просачиваться» и в российскую доктрину, и в правовые акты, что уже имеет место быть, как было показано в начале главы. И вместо решения вопроса с его дефиницией будет возникать проблема с отграничением его от отечественного аналога – термина «электронная торговля». К тому же в современных условиях термин «торговля» более ассоциируется с деятельностью по приобретению и продаже товаров в офлайн-режиме[1], в то время как электронная коммерция гораздо шире по сфере своего охвата (см. далее).

В завершение небольшого терминологического экскурса необходимо сказать несколько слов еще и о таком понятии, как «электронный документооборот», поскольку оно достаточно часто упоминается при рассмотрении тематики электронной коммерции. Исторически данный термин связан с понятием «электронный обмен данными» (*electronic data interchange*, *EDI*), представлявший собой автоматизированный обмен электронными данными между заранее известным кругом лиц с использованием заранее согласованных протоколов и форматов данных. Согласно ст. 2 (*b*) Типового закона ЮНСИТРАЛ «Об электронной торговле» 1996 г. «электронный обмен данными (ЭДИ) означает электронную передачу с одного компьютера на другой информации с использованием согласованного стандарта структуризации информации». Таким образом, *EDI* характерен использованием в закрытых (корпоративных) информационных системах с ограниченным кругом пользователей, например, между банками[2] или между банками и клиентами. Безусловно, *EDI* может использоваться и для заключения сделок, однако в таких случаях отсутствует основное преимущество электронной коммерции в сети Интернет: возможность привлечения новых клиентов и завоевания новых рынков. В случае с *EDI* речь может идти только о деловых взаимоотношениях между контрагентами, которые ранее уже установили контакт между собой в реальном мире. Так что *EDI* и электронная коммерция находятся с некоторых пор в несколько антагонистических взаимоотношениях, что не мешает им в лучших традициях диалектики обладать определенным единством. В конце концов, протокол *TCP/IP* тоже направлен на унификацию «языка общения» между различными сетями и ком-

[1] См.: Федеральный закон от 28 декабря 2009 г. № 381-ФЗ «Об основах государственного регулирования торговой деятельности в Российской Федерации».

[2] См., например: Положение о правилах обмена электронными документами между Банком России, кредитными организациями (филиалами) и другими клиентами Банка России при осуществлении расчетов через расчетную сеть Банка России (утв. Банком России 12 марта 1998 г. № 20-П).

пьютерами в их составе. Так или иначе, с появлением сети Интернет большинство компаний, желающих заниматься электронным бизнесом, перешли на использование сети Интернет в качестве средства коммуникаций с бизнес-партнерами[1].

Что же касается электронного документооборота, то он, безусловно, имеет отношение к электронной коммерции, поскольку заключаемые в ходе осуществления последней договоры представляют собой не что иное, как электронные документы[2]. Однако в последнее время термин «электронный документооборот» все чаще используется не столько в связи с электронной коммерцией, сколько в связи с проблематикой электронного правительства в части необходимости обеспечения эффективного межведомственного информационного обмена[3]. Поэтому представляется целесообразным там его и оставить, не упоминая без особой надобности при рассмотрении правовых аспектов электронной коммерции.

§ 2. Классификация отношений, возникающих в сфере электронной коммерции

Субъекты предпринимательской деятельности могут по-разному использовать возможности сети Интернет для достижения своих целей, в связи с чем можно выделить следующие модели отношений.

Информационно-рекламная поддержка существующего неэлектронного бизнеса в целях облегчения коммуникаций с действующими и потенциальными контрагентами, формирования положительного имиджа компании и повышения спроса на товары (услуги). Данная цель реализуется путем создания корпоративного сайта, содержащего информацию о товарах, работах, услугах, адресах точек продаж, а иногда – ответы на вопросы клиентов, тематические форумы

[1] *Prins C.* et al. Trust in Electronic Commerce. Kluwer Law International, 2002. P. 12.

[2] В соответствии с п. 11.1 ст. 2 Федерального закона от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и защите информации» (далее – Закон об информации) под электронным документом понимается документированная информация, представленная в электронной форме, т.е. в виде, пригодном для восприятия человеком с использованием электронных вычислительных машин, а также для передачи по информационно-телекоммуникационным сетям или обработки в информационных системах.

[3] См., например: распоряжение Правительства РФ от 6 мая 2008 г. № 632-р «О Концепции формирования в Российской Федерации электронного правительства до 2010 года»; постановление Правительства РФ от 6 сентября 2012 г. № 890 «О мерах по совершенствованию электронного документооборота в органах государственной власти» и ряд других документов.

и прочие инструменты получения обратной связи от потребителей. Обычно такая информационная поддержка сопровождается размещением рекламы в сети Интернет (баннерной, контекстной и пр.). Данная модель, несмотря на всю ее простоту и явно вспомогательный характер по отношению к основному офлайновому виду деятельности, тем не менее подпадает в значительной степени под ряд тех же законодательных положений, которые характерны и для других форм электронной коммерции (защита прав потребителей в части предоставления необходимой информации, законодательство о рекламе, определение пределов ответственности владельца веб-сайта за высказывания пользователей форума, защита персональных данных зарегистрированных пользователей и пр.).

Организация продаж через Интернет товаров или услуг существующего неэлектронного бизнеса. В данном случае веб-сайт организации помимо функций, перечисленных применительно к информационной модели, содержит возможность размещения онлайн-заказа и нередко возможность приема платежей. В данной модели сеть Интернет используется преимущественно в качестве средства коммуникации при заключении договора, предметом которого являются традиционные товары, работы или услуги, которые предоставляются «за пределами» Интернета. С правовой точки зрения ко всем правовым аспектам, описанным в предыдущей модели, добавляются еще и вопросы надлежащего оформления договорных отношений, действительности электронных договоров, соблюдения законодательных требований к электронным платежам и т.п.

Создание полноценного интернет-предприятия, охватывающего весь цикл отношений по продвижению продукта до потребителя: как информационный (преддоговорный), так собственно его реализацию (договорный). Важно подчеркнуть, что в данной модели договоры не только заключаются, но и *исполняются* в сети Интернет. Это характерно для договоров, связанных с предоставлением цифрового контента, а также оказанием различного рода внутрисетевых услуг (рекламных услуг, хостинга, услуг «облачных» вычислений и т.д.). В данной модели максимально используются все преимущества электронной коммерции: сокращение транзакционных издержек на содержание складов и обслуживающий персонал, возможность ведения деятельности в глобальном масштабе с выходом на зарубежные рынки. Однако в качестве дополнительной нагрузки появляются еще и риски подпадания под юрисдикцию иностранных государств, необходимость соблюдения иностранного права и т.д.

С точки зрения субъектного состава участников электронной коммерции принято выделять следующие ее категории (таблица): 1) *Business-to-Consumer* (*B2C*); 2) *Business-to-Business* (*B2B*); 3) *Consumer-to-Consumer* (*C2C*); 4) *Business-to-Government* (*B2G*)[1].

Категория	Описание	Примеры
Business-to-Consumer (*B2C*)	Договоры заключаются между предпринимателем и потребителем	Подавляющее большинство интернет-магазинов (*Ozon.ru*; *Amazon.com* и др.)
Business-to-Business (*B2B*)	Договоры заключаются между предпринимателями	Предоставление «облачных» сервисов, услуг хостинга, рекламные услуги в сети Интернет и прочие внутрисетевые услуги, а также осуществление продаж традиционных «офлайновых» товаров и услуг коммерческого назначения с использованием веб-сайтов в сети Интернет, в том числе специализированных торговых площадок
Consumer-to-Consumer (*C2C*)	Договоры заключаются между двумя потребителями (физическими лицами)	Различного рода виртуальные площадки вроде *ebay*, *avito.ru* и др.
Business-to-Government (*B2G*)	Договоры заключаются между предпринимателем и публичными образованиями в ходе осуществления процедур государственных (муниципальных) закупок	Размещение заказов путем проведения открытого аукциона в электронной форме[2]

Как известно, субъектный состав договора непосредственно влияет на квалификацию отношений и применимые нормы. Так, например, осуществление продаж товара посредством размещения заказа на вебсайте в сети Интернет будет квалифицироваться как договор рознич-

[1] *Schneider G.* Electronic Commerce. Course Technology. Mass. 9th ed. 2011. P. 7.

[2] Глава 3.1 Федерального закона от 21 июля 2005 г. № 94-ФЗ «О размещении заказов на поставки товаров, выполнение работ, оказание услуг для государственных и муниципальных нужд».

ной купли-продажи с применением законодательства о защите прав потребителей в случае *B2C*; как договор купли-продажи с применением общих положений § 1 гл. 30 ГК РФ – в случае *C2C*; как договор поставки (или розничной купли-продажи[1]) – в случае *B2B*; как поставка товаров для государственных или муниципальных нужд (§ 4 гл. 30 ГК РФ и специальное законодательство о государственных закупках[2]).

В рамках данной работы будут рассмотрены вопросы, характерные для отношений, возникающих в сфере электронной коммерции в *B2B*- и *B2C*-секторах. *C2C*- и *B2G*-сегменты, по моему мнению, не обладают на данный момент существенной спецификой, которая бы оправдывала выделение их в отдельные категории *для целей правового анализа*. Основные проблемы, которые возникают в данных случаях, касаются стадии заключения договора с учетом того, что большинство договоров в данных сегментах предполагают исполнение в офлайн-режиме. В связи с этим те проблемы и решения, которые характерны для *B2B* и *B2C*, будут вполне применимы и здесь. Не исключено, что по мере развития взаимодействия государства и бизнеса в сети Интернет потребуется детальный анализ правовых аспектов возникающих в связи с этим отношений.

В любом случае к какому сегменту не относилась бы отдельно взятая сделка с сфере электронной коммерции, она всегда будет обладать определенной спецификой, отличающей ее от традиционных договоров, заключаемых в офлайн-режиме. Указанная специфика предопределяется особенностями архитектуры сети Интернет, на которой имеет смысл остановиться подробнее для того, чтобы представлять себе причину появления тех специфических проблем, которые характерны для сферы электронной коммерции, а также историю ее развития.

§ 3. История создания сети Интернет

Правовые проблемы, возникающие в сфере электронной коммерции, в большинстве своем являются следствием архитектуры сети Интернет. Именно технические особенности ее функционирования

[1] См.: п. 5 постановления Пленума ВАС РФ от 22 октября 1997 г. № 18 «О некоторых вопросах, связанных с применением положений Гражданского кодекса Российской Федерации о договоре поставки».

[2] Федеральный закон от 21 июля 2005 г. № 94-ФЗ «О размещении заказов на поставки товаров, выполнение работ, оказание услуг для государственных и муниципальных нужд» (с 1 января 2014 г. Федеральный закон от 5 апреля 2013 г. № 44-ФЗ «О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд»).

во многом и предопределили те специфические проблемы, с которыми приходится сталкиваться государствам и участникам оборота при использовании Интернета в своей деятельности. То, что изначально представлялось неоспоримым преимуществом данной сети с технической точки зрения, на определенном этапе ее развития создало проблемы, с которыми право оказалось не в силах самостоятельно справиться. В свою очередь особенности технической архитектуры предопределены историческими особенностями разработки и создания данной сети.

Возможно, это прозвучит несколько провокационно, но Интернет во многом появился благодаря усилиям СССР. К сожалению, не столько в связи с наличием в СССР зачатков сильной *IT*-индустрии, сколько благодаря достигнутым им успехам на ниве гонки вооружений. В 1953 г. Советский Союз проводит успешные испытания водородной бомбы, в 1957 г. запускает в космос первый спутник. Очевидные преимущества в космической сфере в совокупности с наличием мощного ядерного оружия вызывали серьезную озабоченность Соединенных Штатов Америки. На столы президентов США попадали доклады о состоянии ядерной угрозы и возможных сценариях ядерной войны. Все эти сценарии так или иначе предполагали определенные ответные действия со стороны США, реализация которых зависела от принятого президентом решения. Для того чтобы такое решение могло быть доведено до сведения исполнителей, необходимо было наличие сети связи, устойчивой к возможным ядерным ударам[1]. Существовавшие в то время линии телефонной связи носили централизованный характер, т.е. предполагали наличие центрального коммутатора и управляющего органа. При повреждении такого центрального коммутатора отдельные фрагменты сети становились изолированными и не могли устанавливать соединение между собой.

В таких условиях возникла потребность в создании сети нового типа, построенной на иных принципах. Она должна была быть способной к функционированию при утрате любого ее фрагмента, иметь возможность использования для передачи данных любых доступных каналов связи в различной комбинации с оперативным изменением маршрута в зависимости от работоспособности ее отдельных фрагментов.

В основу сети нового поколения была положена идея распределенной коммуникационной сети, разработанная американцем Полом Бэраном[2], и теория пакетной передачи данных, разработанная тем

[1] *Ryan J.* A History of Internet and the Digital Future. London, 2010.

[2] *Baran P.* On Distributed Communications. Twelve volumes // RAND Corporation papers. 1964.

же Бэраном и англичанином Дональдом Дэвисом[1] независимо друг от друга. Если П. Бэран, разрабатывая теорию пакетной передачи данных, думал при этом о применении данной технологии в военных целях, то Д. Дэвис рассматривал ее в качестве средства для более эффективного распределения скудных вычислительных ресурсов, доступных для проведения научных исследований. Так или иначе, суть пакетной передачи данных заключается в разделении исходного сообщения на множество составляющих («пакетов»), направляемых в соответствии с определенным алгоритмом по самостоятельному маршруту, с последующим их воссоединением у адресата. Инновационный потенциал данного подхода заключался в том, что он а) снижал нагрузку на вовлеченные в процесс передачи сообщения компьютеры, позволяя использовать для этих целей более дешевые и компактные устройства, б) затруднял подслушивание, в) позволял одновременно взаимодействовать множеству пользователей, сети которых имеют разную пропускную способность. Однако, несмотря на очевидные преимущества, создание сети, построенной на пакетной передаче данных, виделось многим ученым и специалистам того времени бесперспективной задачей, а иногда и вовсе воспринималось враждебно. Добавление специальных алгоритмов разделения сообщения на «пакеты» с их последующей маршрутизацией неизбежно усложняло процесс передачи данных. Несовместимость используемых в различных университетах и организациях компьютеров еще более усложняло задачу. Не последнюю роль сыграл и консерватизм ученых и представителей бизнеса, чья деятельность была связана с традиционными сетями связи.

Финансирование разработки сети нового поколения осуществлялось Министерством обороны США через Агентство передовых научных проектов (*Advanced Research Projects Agency*, *APRA*), которое весьма благожелательно относилось к высокорисковым проектам. К тому же реализация данного проекта позволяла Агентству не только приобщиться к решению вопросов общенационального масштаба, но и решить собственные проблемы: все компьютеры, используемые аме-

[1] *Davies D.* Proposal for the Development of a National Communication Service for On-Line Data Processing. Memorandum, National Physical Laboratory. 15 December 1965. Принимая во внимание, что перед Англией в то время не стояло амбициозных целей противостояния СССР, и то, что данное исследование носило исключительно научный характер, оно не смогло получить того внимания и финансирования, которое получили идеи П. Бэрана в США, что отнюдь не умаляет значимости работы Д. Дэвиса в контексте истории разработки сети Интернет. Многие его идеи при его активном участии были использованы при разработке сети *ARPANET*. См.: *Abbate J.* Inventing the Internet. The MIT Press. 1999. P. 30.

риканскими университетами и подрядчиками, приобретались за счет Агентства, и оно было постоянно завалено запросами на приобретение новых компьютеров, поскольку вычислительной мощи разрозненных компьютеров все время не хватало. Соединение существующих компьютеров в единую сеть с образованием общего «пула» вычислительных мощностей позволило бы гораздо более эффективно использовать имеющиеся мощности[1]. К тому же это позволило бы объединить географически разрозненных ученых вместе, создав сообщество талантов, работающих над решением определенной проблемы[2].

В 1969 г. была создана сеть, соединившая четыре компьютера, расположенные в Калифорнийском университете в Лос-Анджелесе, Калифорнийском университете в Санта-Барбаре, Университете штата Юта и Стэнфордском научно-исследовательском институте. Так появилась сеть *ARPANET*, которую обычно считают прародительницей современного Интернета[3].

Поскольку реализация механизма пакетной передачи данных в отношении множества несовместимых между собой компьютеров являлась чрезмерно сложной, приветствовались любые средства, позволяющие ее упростить. Одним из таких средств стал многоуровневый подход (*layering*) к строению сети *ARPANET*, а впоследствии – и сети Интернет. Вся совокупность задач, стоявших перед сетью, разделялась на определенные независимые друг от друга уровни, взаимодействующие между собой по определенным правилам (начиная с физического уровня, обрабатывающего электрические сигналы, и заканчивая абстрактным уровнем, обрабатывающим команды и запросы пользователей, сделанные на высокоуровневом языке программирования). Преимущество многоуровневой организации сети заключается в том, что администратор определенного уровня не должен иметь представление о внутреннем устройстве всех остальных уровней: каждый уровень сети может создаваться и модифицироваться независимо от других при условии использования общих интерфейсов между ними. Все это существенно

[1] Внимательный к современным технологиям читатель увидит здесь прообраз популярной нынче концепции «облачных» вычислений (*Cloud Computing*).

[2] *Roberts L.* Multiple Computer Networks and Intercomputer Communication // Symposium on Operating System Principles. Gatlinburg. Tennessee, 1967. P. 2. Как видно, идеи, которые положены в основу столь популярного ныне движения *open source*, высказывались еще в середине 60-х гг. XX в. и были положены в основу создания сети Интернет.

[3] См.: American Civil Liberties Union, et al. v. Janet Reno, Attorney General of the United States. 929 F. Supp. 824, E.D. Penn (1996). Данное судебное решение примечательно тем, что содержит в себе достаточно детальное описание истории возникновения сети Интернет и ее технических особенностей.

упрощало проектирование сетей, их тестирование и отладку. В более глобальном контексте данная архитектурная особенность сети Интернет обеспечивала ее гибкость и децентрализованный характер.

При таком подходе к устройству сети принципиальное значение приобретают протоколы. Ведь если проблему несовместимости компьютеров, подключенных к одной сети, нельзя преодолеть насильственной их стандартизацией, необходимо, чтобы они все придерживались одного протокола как необходимого условия «членства» в такой сети[1]. Первым таким протоколом стал *NCP* (*Network Control Protocol*), на смену которому впоследствии придет протокол *TCP/IP*.

Таким образом, архитектура сети Интернет воплотила в себе как черты, имеющие явное военное назначение (отказоустойчивость и гибкость), так и черты, свойственные научному сообществу (открытый обмен информацией и децентрализованное управление).

В 1972 г. состоялась презентация возможностей сети *ARPANET* на Международной конференции по компьютерным коммуникациям (*International Computer Communication Conference*, *ICCC*), где заинтересованные лица могли вживую оценить возможности новой сети. Это событие сыграло ключевую роль в развитии сети *ARPANET*, а вместе с ней и сети Интернет в целом, так как возможность построения сети, основанной на пакетной передаче данных и многоуровневой архитектуре, была доказана не только на бумаге, но и в жизни и стала отправной точкой для дальнейших исследований и коммерческих проектов в данной сфере.

Однако несмотря на упомянутый успех, сеть *ARPANET* никогда бы не смогла перерасти в нечто глобальное, если бы не попытки отдельных пользователей придать ей «человеческое лицо». По замечанию одного из ранних пользователей *ARPANET*, «в данной сети не было ничего такого, что могло бы привлечь пользователей, не являющихся компьютерными гиками»[2]. В значительной степени это было связано с существенными сложностями подключения новых компьютеров к данной сети. Такой компьютер должен был принадлежать организации, аффилированной с *ARPA*, в противном случае стоимость подключения могла достигать 100 000 долл.[3] При этом все существующее программное обеспечение должно было быть адаптировано к требованиям сети и протоколу *NCP*, что было сопоставимо с годовым объемом работы программиста.

[1] *Marill T., Roberts L.* Toward a Cooperative Network of Time-Shared Computers. AFIPS Press. 1966. P. 428.

[2] *Abbate J.* Op. cit. P. 84.

[3] Ibid.

Таким образом, существенные временны́е и материальные затраты делали перспективы присоединения к данной сети малопривлекательными. Но еще менее привлекательными были те возможности, которые она предоставляла на тот момент. Данная сеть изначально задумывалась как сеть, обеспечивающая доступ к компьютерам (вычислительным мощностям), а не к людям. Это было хоть как-то оправдано во времена дорогих мейнфреймов, которые далеко не каждая организация могла себе позволить, а те, которые и могли, не часто использовали их в полную силу. Но с появлением персональных компьютеров, которые могли себе позволить даже небольшие компании и учебные заведения, экономическая целесообразность наличия такой сети становилась все менее очевидной.

Ситуацию спас Рэй Томлинсон (*Ray Tomlinson*), благодаря которому в 1972 г. появилось одно из самых популярных сетевых приложений — электронная почта, открывшая новое измерение для межличностных коммуникаций. Данное приложение фактически переставило сеть *ARPANET* на новые рельсы, сделав ее привлекательной в том числе и для неэкспертов в области компьютерных технологий. *ARPANET* стал превращаться из компьютерной технологии в *коммуникационную* технологию.

Но *ARPANET* еще не был Интернетом в его современном понимании. Подобно своему предшественнику, Интернет появился опять же в значительной степени благодаря усилиям военных ведомств США. Теперь они нуждались не только в отказоустойчивой и надежной системе наземной связи, необходимо было обеспечить такой связью и мобильные подразделения армии. А это означало необходимость включения в сеть не только сигналов, передаваемых по классическим телефонным сетям, но и сигналов, передаваемых по радио- и спутниковой связи. К середине 70-х гг. XX в. в ведении *ARPA* оказалось три сети: *ARPANET*, *PRNET* (радиосвязь) и *SATNET* (спутниковая связь). В силу их существенных различий между собой необходимо было выработать новые подходы к организации взаимодействия между ними. Так появилась программа «Интернет». Ключевую роль в реализации данной программы сыграли Винтон Серф (*Vinton Cerf*), работавший некоторое время в *IBM*, и Роберт Кан (*Robert Kahn*), ранее работавший в *AT & T Bell Labs*. Также в ней приняли участие представители Великобритании и Франции, которые познакомились с сетью *ARPANET* в ходе ее презентации на конференции 1972 г. В данных странах также были созданы собственные сети, построенные на основе пакетной передачи данных, и на повестке дня также стоял вопрос об их соединении между

собой и присоединении к *ARPANET*. Таким образом, архитектура новой сети формировалась в неформальном порядке группой ученых-экспертов без участия коммерческих структур. В результате этого взаимодействия в 1974 г. был создан протокол *TCP/IP*, который по праву считают «сердцем» Интернета. Компьютерные сети и иные телекоммуникационные сети общего пользования существовали и до Интернета, более того, и сейчас продолжают сосуществовать вместе с ним[1]. Однако Интернет появился лишь тогда, когда был разработан и введен в действие универсальный язык для взаимодействия компьютерных сетей, который как раз и выражен в протоколе *TCP/IP*[2].

На тот момент это был весьма революционный протокол, переход на который требовал значительных усилий и времени. Возможно, подобная миграция затянулась бы на долгое время, если бы опять этим не занялись военные. Дело в том, что *ARPA*, будучи небольшим исследовательским агентством, не имело мощностей для того, чтобы выступать оператором изрядно выросшей к тому времени сети. Начались поиски государственного учреждения или коммерческой организации, которая была бы готова взять на себя такую роль. Крупнейшая американская телекоммуникационная компания *AT & T* отказалась от данной роли, поскольку технология пакетной передачи данных представляла собой существенное ответвление от основного бизнеса компании, а ее коммерческое применение не было очевидно. Так, сеть *ARPANET* попала за неимением лучших кандидатур в ведение Управления связи Министерства обороны США (*Defense Communication Agency*), что повлекло существенную «милитаризацию» сети. К 1976 г. воздушные, морские и наземные военные силы США использовали *ARPANET*. Потребность в соединении сети *ARPANET* с существовавшей ранее военной сетью *AUTODIN* обусловила необходимость в скорейшей повсеместной имплементации протоколов *TCP/IP*. В свойственном для военного руководства стиле была поставлена задача провести такую миграцию к январю 1983 г. Те, кто не успел осуществить переход на *TCP/IP* к указанному сроку, были отключены от сети[3].

---

[1] В качестве примера можно привести сеть *GLORIAD*, запущенную 12 января 2004 г. и объединяющую научно-исследовательские центры России, США и Китая и ряда иных стран. Основным направлением деятельности сети является предсказание природных катастроф, ядерные и космические исследования. Скорость передачи данных составляет до 10 Гб/с. Узлов передачи трафика Интернета в данной сети нет. См.: *Robert Britt.* High-Speed «Other» Internet Goes Global // LiveScience. 15 October 2009.

[2] *Crawford S.* The digital broadband migration: Internet think // Journal on Telecommunications & High Technology Law. No 5. 2007. P. 469.

[3] *Abbate J.* Op. cit. P. 141.

Новый стиль руководства сетью нашел свое отражение и в ее режиме пользования, который ознаменовался «закручиванием гаек»: жесткие процедуры авторизации пользователей, запрет на любое использование сети не по назначению, необходимость получения предварительного согласия владельца файла на его последующее копирование – все это противоречило принципам, укоренившимся в научном сообществе, стоявшем у истоков создания сети. После того как появились персональные компьютеры и возросла угроза несанкционированного использования сети, существенно возрос и контроль за соблюдением процедур. Разумеется, научное сообщество не приветствовало такие нововведения. В результате 4 апреля 1983 г. под предлогом необходимости обеспечения повышенной безопасности военных коммуникаций из сети *ARPANET* выделилась сеть *MILNET*. С этого момента сеть *ARPANET* приобрела гражданский характер, снова став инструментом для научно-исследовательской деятельности университетов.

Повсеместная имплементация протокола *TCP/IP* в военных ведомствах не означала, впрочем, что в гражданской сфере все были готовы следовать их примеру. Одним из последних рубежей на пути распространения сети Интернет были телекоммуникационные компании, которые опасались возрастания влияния производителей компьютерного оборудования, фактически использовавших собственные стандарты. Особую озабоченность вызывал проприетарный стандарт *Systems Network Architecture*, продвигаемый *IBM*, поскольку его использование телекоммуникационными компаниями означало их «привязывание» к оборудованию одной компании. Так, в 1976 г. появился стандарт X.25, принятый Международным союзом электросвязи[1]. Данный стандарт представлял собой альтернативный подход к построению сетей, отражавший видение телекоммуникационных компаний. В отличие от протокола *TCP/IP*, предоставляющего пользователям бóльший контроль над функциональностью сети, X.25 исходит из того, что такой контроль должен быть у оператора сети для более качественного сервиса. Предполагалось, что монопольное положение телекоммуникационных компаний, существовавшее в большинстве стран, позволит создать единую сеть в масштабах страны с последующим объединением их в международном масштабе на основе единого стандарта. В результате существовавшее многообразие несовместимых между собой сетей уйдет в небытие. *TCP/IP*, напротив, с самого начала рассчитан на соединение самых разнообразных по своей архитектуре сетей,

[1] В то время он именовался Международным консультативным комитетом по телефонии и телеграфии.

и такое разнообразие рассматривалось не как неудобство, а как благо, позволяющее лучше адаптировать сети к специфическим потребностям пользователей (преимущественно военных, учитывая историю разработки данного протокола). Ущербность X.25 проявлялась еще и в том, что данный стандарт дискриминировал частные сети, поскольку, по мнению разработчиков протокола, они не должны были стать широко распространенными. Например, за частными сетями закреплялось незначительное количество адресов (по 10 на страну, лишь за США было закреплено 200)[1]. Хотя нельзя говорить о том, что X.25 был однозначно плох: он выполнил основную функцию, перераспределив контроль над сетевыми стандартами между производителями компьютеров и телекоммуникационными компаниями в пользу последних (*IBM* и другие компании стали предлагать свои продукты с использованием протокола X.25, который был имплементирован во многих публичных и коммерческих сетях).

Следующим усилием по установлению сетевых стандартов была разработка в 1978 г. Концепции взаимодействия открытых систем (*Open Systems Interconnection*, *OSI*), которая по замыслу разработчиков (Международной организации по стандартизации) должна была продолжить идеи X.25 в части обеспечения открытости спецификаций сетевого оборудования различных производителей и их совместимости между собой. Но поскольку данный рынок был только в стадии формирования, явных кандидатов на роль стандартов не находилось, в силу чего было принято решение остановиться на систематизации существующих функций сетей и сведению их к семи уровням протоколов, к каждому их которых впоследствии должен был быть принят определенный стандарт. Нижние уровни включали в себя функции, связанные с передачей сигналов, в то время как целями высших уровней были более абстрактные задачи, связанные с обработкой информации. Не вдаваясь в дальнейшие технические детали, без которых юристы вполне могут прожить, следует сказать, что основным значением *OSI* стало «цементирование» принципа многоуровнего построения сети (*layering*), который на тот момент был отражен в сети *ARPANET/INTERNET*. Принятие открытых стандартов особенно приветствовалось в странах Западной Европы в качестве инструмента, позволяющего укрепить положение местных производителей компьютеров, которые не могли тягаться с американскими гигантами и проталкивать свои стандарты. Как отмечалось в одном из отчетов французского

[1] *Cerf V., Kirstein P.* Issues in Packet-Network Interconnection // Proceedings of the IEEE. No 66. 1978. P. 1400.

правительства, «если бы *IBM* стала хозяином рынка сетевых технологий, желая того или нет, она бы приобрела долю в мировых властных структурах»[1]. Протоколы Интернета (*TCP/IP*) первоначально не могли быть приняты в качестве открытых стандартов, поскольку они не были установлены каким-либо органом, были разработаны в США и вовсю применялись американскими компаниями, что давало им преимущество по отношению ко всем остальным[2]. Тем не менее, несмотря на все благие намерения разработчиков *OSI*, эта модель так и не смогла стать универсальным стандартом. Интернет продолжал использовать *TCP/IP*, а *OSI* оставался лишь «одним из многих». Но в любом случае *OSI* оказала огромное влияние на *представления* людей о сетях.

В условиях, когда ни X.25, ни *OSI* не смогли получить единодушного признания, но в то же время находили свою имплементацию в отдельных сетях, роль *TCP/IP* как наиболее гибкого и универсального из всех протоколов, позволяющего объединить любые сети, еще более возросла и превратила его в стандарт *de facto*. Война стандартов, а по сути – война за контроль над технологией, лишь привела в итоге к укреплению положения *TCP/IP* и его международному признанию. Данная история имеет не только историческую ценность, повествуя о том, как центральный компонент Интернета – *TCP/IP* – незаметно завоевал международное признание. Это также и хорошая иллюстрация того факта, что чисто технические на первый взгляд решения могут иметь далеко идущие социально-экономические последствия, изменяя баланс сил между участниками рынка и даже целыми странами нередко ценой свободы пользователей.

Возвращаясь к истории развития сети *ARPANET*, из которой выделилась военная составляющая в лице *MILNET*, можно отметить, что эра *ARPANET* приходила к концу. Сеть, возраст которой уже перевалил за 15 лет, не обладала достаточной пропускной способностью. Финансирование дальнейшего развития сети перешло от Министерства обороны к Национальному научному фонду США (*NSF*), подконтрольному Министерству торговли США. *NSF* в рамках новой программы развития суперкомпьютеров создал еще одну сеть – *NSFNET*, обладавшую гораздо большей пропускной способностью по сравнению с *ARPANET*, что позволило объединить большее количество университетов на гораздо более либеральных условиях. В таких условиях было принято решение свернуть программу *ARPANET* и перевести всех пользователей на платформу *NSFNET*. 28 февраля 1990 г. сеть

[1] Protocol-Linkup Paln Would Stymie IBM // Electronics. 8 June 1978. P. 70.
[2] *Lynch D., Rose M.* Internet system handbook. Addison-Wesley, 1993. P. 11.

ARPANET официально прекратила свое существование, а вместе с ней пришла к концу и военная эпоха в развитии сети Интернет.

Дальнейшее развитие сети Интернет было связано с ее постепенной приватизацией. Дело в том, что использование сети *NSFNET* в коммерческих целях не допускалось, поскольку она финансировалась за счет бюджетных средств в целях развития науки и образования[1]. Нетрудно догадаться, что столь жесткий подход не приветствовался пользователями, число которых с каждым годом все возрастало, в том числе среди коммерческих организаций[2]. Многие организации предоставляли сетевую инфраструктуру на платной основе. Запрет коммерческого трафика в *NSFNET* приводил к созданию провайдерами собственных коммерческих сетей. К середине 90-х гг. прошлого века параллельно с *NSFNET* существовали коммерческие сети (*MCI*, *AT & T*, *Sprint*), построенные на протоколе *TCP/IP*. В июле 1991 г. некоторые коммерческие провайдеры договорились о взаимном пропуске трафика, создав некоммерческую организацию, основанную на членстве *Commercial Internet Exchange* (*CIX*). Это позволило пользователям одной коммерческой сети взаимодействовать с пользователями других сетей, существенно повысив ценность этих сетей[3]. *CIX* стала своего рода коммерческой версией Интернета. Руководству *NSF* стало очевидно, что сохранение существующих ограничений негативно скажется на развитии Интернета в целом, и было принято решение расформировать сеть *NSFNET*, предоставив возможность оказания услуг по предоставлению доступа в сеть коммерческим провайдерам, обладающим собственной сетью, заключающим между собой соглашения о пропуске трафика. Для целей научных исследований создавалась особая сеть (*vBNS*). 30 апреля 1995 г. *NSFNET* была окончательно расформирована, коммерческий сегмент Интернета в результате стал основным. Это сняло ограничения на подключение к сети Интернет иностранных сетей, так как это более не могло рассматриваться как предоставление иностранцам ресурса, субсидируемого на средства американских налогоплательщиков. Последние препятствия к международной экспансии Интернета были устранены. К 1995 г. Интернет

[1] NSFNET Acceptable Use Policy, 1992.

[2] Около трети миллиона компьютеров было подсоединено к *NSFNET* в 1990 г. с удвоением их количества каждый последующий год. См.: *Ryan J.* A History of Internet and the Digital Future.

[3] В Европе подобные функции выполняло созданное в 1989 г. объединение европейских провайдеров *RIPE* (*Réseaux IP Européens* – Европейские *IP*-сети), в рамках которого осуществлялся обмен трафиком. Можно говорить о том, что данная орагнизация представляла собой своего рода общеевропейский Интернет.

включал в себя 22 000 иностранных сетей[1]. Одной из таких сетей стала сеть Европейской организации по ядерным исследованиям (*CERN*), с которой связано появление Всемирной паутины (*World Wide Web*, *WWW*), преобразившей Интернет до неузнаваемости.

До появления *WWW* основным способом использования сети была электронная почта и передача файлов. Все это сопровождалось малодружелюбным текстовым интерфейсом, что резко контрастировало с завоевавшим на тот момент популярность на рынке операционных систем графическим пользовательским интерфейсом. Другая проблема заключалась в сложности нахождения нужной информации: для того чтобы скачать нужный файл, нужно было заранее знать его точный адрес. Поисковых систем в современном их понимании тогда не было. Связь между различными файлами также отсутствовала.

На фоне данной ситуации разработанная Тимом Бернерсом-Ли (*Tim Berners-Lee*) в 1993 г. технология Всемирной паутины была поистине прорывной. В ее основе лежит идея систематизации содержащейся в сети Интернет информации посредством перекрестных ссылок, которые образуют своего рода «паутину». Всемирная паутина представляет собой совокупность электронных документов, пребывающих в памяти различных компьютеров, подключенных к Интернету и унифицированных посредством использования специального языка гипертекстового документа (*HTML*). Каждый из таких документов имеет свой уникальный электронный адрес (*URL*). Использование стандартизированных форматов отображения (*HTML*) и передачи данных (*HTTP*) обеспечивает возможность восприятия электронного документа каждым пользователем, использующим специальную программу – браузер[2]. Благодаря *WWW* Интернет стал мультимедийным: графическое и звуковое сопровождение стало неотъемлемой частью многих ресурсов сети.

Данная технология стала настолько популярной, что *WWW* нередко отождествляют с Интернетом в целом, хотя это и некорректно, так как Всемирная паутина является лишь одним из приложений (*application*) Интернета наряду с электронной почтой (*e-mail*), системой интерактивного общения, позволяющим мгновенный обмен сообщениями (*IRC*), приложением удаленного доступа (*Telnet*) и многими другими «надстройками» сети Интернет.

WWW позволила использовать Интернет не только преимущественно как средство общения, но и как источник информации. Неда-

[1] *Abbate J.* Op. cit. P. 210.

[2] *Yee Fen Lim*. Cyberspace Law: Commentaries and materials. Oxford, 2002. P. 11–13.

ром Верховный суд США сравнил Всемирную паутину одновременно с огромной библиотекой, содержащей миллионы проиндексированных систематизированных материалов, и с огромным супермаркетом[1]. Таким образом, *создание Всемирной паутины окончательно завершило трансформацию Интернета из прикладного средства для научных исследований в популярную среду общения*. Каждый пользователь мог стать не только потребителем информации, но и ее создателем. Дальнейшее совершенствование поисковых механизмов, браузеров и компьютерных технологий в целом создавало все больше условий для самореализации пользователей в сети Интернет и ведения коммерческой деятельности. Появление технологии Всемирной паутины позволило раскрыть коммерческий потенциал сети Интернет как площадки для ведения бизнеса. С этого момента (приблизительно 1995 г.) можно говорить о начале новой эпохи сети Интернет – эпохе электронной коммерции. Многие коммерческие компании (*Dell*, *Cisco* и др.) открывают свои веб-сайты в сети Интернет и начинают их активно использовать в коммерческой деятельности. В 1995 г. был запущен сайт *Amazon.com*, являющийся одним из крупнейших в мире по продаже товаров и услуг через Интернет (сегмент *B2C*). В том же году появляется одна из наиболее известных платформ для интернет-аукционов – *eBay* (сегменты *B2C* и *C2C*).

Все это никоим образом не входило в первоначальные планы создателей Интернета, но его децентрализованная многоуровневая архитектура создала благодатную почву для постоянных «сюрпризов»: появления все более новых средств использования и восприятия сети Интернет.

Как видно из истории развития сети Интернет, она прошла ряд этапов становления. На ранних этапах данная сеть воспринималась в качестве составной части военной программы. Однако эта программа реализовывалась не военными, а учеными, которые привнесли в нее свое видение того, как должна быть организована сеть. Реализованная в итоге децентрализованная структура сети Интернет предполагала отсутствие иерархии, подчинения одних ее фрагментов другим. Передаваемые «пакеты» данных содержали минимум необходимой информации. Идентификация личности отправителя данных, географического расположения отправителя, содержимого сообщения – все это было излишним в контексте стоявших задач: об использовании Интернета для электронной коммерции тогда даже и не думали, а для обмена научными идеями хватало и того, что было. К тому же утяжеление пакетов данных дополнительной информацией могло потенциально

[1] Reno v. ACLU, 521 U.S. 844, 853 (1997).

перегрузить и без того ненадежные сети с низкой пропускной способностью. Подобная децентрализованная архитектура сети Интернет вполне отражала и мировоззрение ее создателей – компьютерных хакеров, которые не очень любят подчиняться формальным правилам и признавать иерархию.

Существенные преобразования архитектуры сети Интернет начались тогда, когда начал меняться характер ее пользователей: монополия профессиональных программистов и технических специалистов в определенный момент начала разбавляться обычными пользователями, чему способствовало два фактора: 1) революция в сфере компьютерной индустрии, в результате которой появился персональный компьютер, доступный для обычного пользователя, и 2) изобретение Всемирной паутины.

Сделав Интернет более дружелюбным для среднестатистического пользователя, а также обеспечив возможность отображения графических изображений, *WWW* создала благоприятные условия для электронной коммерции, что предопределило постепенный процесс трансформации Интернета в нечто все более и более регулируемое[1].

Выделим теперь те ключевые особенности сети Интернет, которые оказывают непосредственное влияние на ее правовое регулирование и эффективность такового.

§ 4. Архитектурные особенности сети Интернет и их влияние на правовое регулирование электронной коммерции

Сказанное ранее о сети Интернет позволяет прийти к выводу, что он представляет собой гигантскую компьютерную сеть, которая объединяет между собой бесчисленное множество более мелких компьютерных сетей. Как указал один из судов США, Интернет – это сеть сетей[2]. Данные в Интернете циркулируют благодаря «сотням тысяч коммутируемых компьютеров и телефонных сетей»[3].

Отсюда следует первое важное следствие: *в сети Интернет отсутствуют географические границы* (1). Они абсолютно иррелевантны для интернет-протоколов, объединяющих такие сети. События в сети Интернет происходят «везде» и «нигде конкретно», в связи с чем бывает невозможно привязать их к конкретному географическому месту.

---

[1] *Lessig L.* Code. Ver. 2.0. Basic Books. N.Y., 2006. P. 61.

[2] American Civil Liberties Union v. Janet Reno, Attorney General of the United States (ACLU v. Reno) {1996}: *Yee Fen Lim*. Op. cit. P. 4.

[3] *Post D.* Anarchy, State and the Internet: an essay on law-making in Cyberspace. 1995. P. 2.

Стоимость и скорость передачи сообщения в сети Интернет являются почти полностью независимыми от физического местоположения[1]. Пользователь может легко оказаться на сайте, расположенном в другом городе, государстве или на другом континенте. Более того, как правило, пользователи даже и не имеют представления о том, где расположен тот или иной сайт. Такая способность пользователя перемещаться «сквозь» границы порождает множество правовых проблем: защиты личной информации о пользователе, защиты прав потребителей в сети Интернет, защиты интеллектуальной собственности, регулирования содержания предоставляемой интернет-провайдером пользователю информации. Более подробно соответствующие вопросы будут рассмотрены далее. Сейчас же следует отметить, что архитектура сети Интернет, а именно ее децентрализованный характер, выражающийся в отсутствии единого центра, контролирующего все информационные процессы, происходящие в Интернете, является одной из основных причин невозможности их эффективного унифицированного правового регулирования.

При этом не стоит, конечно, впадать в крайность и утверждать об отсутствии возможности какого-либо правового регулирования в принципе. Все участники информационных процессов, происходящих в сети Интернет, так или иначе имеют физическое присутствие в какой-либо точке планеты и, следовательно, подчиняются как минимум юрисдикции того государства, на территории которого находятся. Поскольку доступ к сети Интернет может произойти из любой точки планеты, потенциально соответствующие отношения могут быть подчинены юрисдикции любого государства. Поэтому Интернет является не анархичным пространством, находящимся вне правового воздействия, а скорее самым «зарегулированным» местом во всем мире[2]. Тем не менее данная особенность сети Интернет чрезмерно обостряет решение и без того непростых вопросов определения юрисдикции компетентных органов того или иного государства по рассмотрению спора, осложненного иностранным элементом; определения применимого права, а также последующего исполнения вынесенного решения в иностранном государстве.

Следующей особенностью архитектуры сети Интернет, которая может иметь значение при решении тех или иных правовых вопросов, является *разделение каждого цифрового сообщения на отдельные пакеты данных, каждый из которых направляется автономным способом адресату* (2). При этом пакеты могут «огибать» участки сети, которые повреж-

[1] *Johnson D., Post D.* Law and Borders – The Rise of Law in Cyberspace // Stanford Law Review. No 48. 1996. P. 1370.

[2] *Reed C.* Internet Law: Cases and Materials. Cambridge University Press. 2004. P. 2.

дены либо в силу иных причин непригодны для использования. Так, например, отдельные пакеты сообщения, отправленного из Москвы в Санкт-Петербург, могут пройти через Германию, США и иные страны, прежде чем дойдут до назначения и реконструируются у адресата. Иными словами, информационный обмен, осуществляемый посредством сети Интернет, потенциально осложнен иностранным элементом в виде возможного прохождения информации через территорию иностранных государств. Как отмечалось ранее, данная особенность сети Интернет обусловлена военно-исследовательскими корнями.

В качестве иллюстрации того, как эта особенность может иметь значение с правовой точки зрения, можно привести одно дело, рассмотренное в суде США. Ответчик, проживающий в штате Юта, отправил сообщение своей подруге о якобы заложенной бомбе у нее на работе, которая расположена всего в нескольких милях от него. При этом он использовал специальную программу для обмена сообщениями фирмы *America Online* (*Instant Messenger*), сервер которой находился на территории штата Виргиния. Суд указал, что поскольку данное сообщение дошло до адресата через сервер, расположенный в Виргинии, т.е. через территорию другого штата, то ответчик виновен в совершении квалифицированного вида угрозы – с использованием территории различных штатов[1]. Таким образом, данная особенность может иметь значение при решении вопросов, придающих правовое значение трансграничной передаче данных, например при регулировании обработки персональных данных.

Учитывая большое число лиц, так или иначе принимающих участие в передаче отдельных пакетов, а также огромное число пакетов, постоянно передаваемых через каждый ее участок, в ряде случаев достаточно сложно установить этап, на котором пакет был утрачен или в него были внесены изменения. Таким образом, используемая технология передачи данных в рамках Интернета, как правило, не позволяет возлагать на кого-либо ответственность за их сохранность[2].

К тому же с точки зрения процесса организации электронного документооборота данная особенность имеет то значение, что в сети Интернет полностью утрачивается какой-либо смысл в разграничении понятий «оригинал» и «копия» документа, так как до пользователя доходит лишь *n*-ная «копия» документа[3]. Поэтому традиционное

[1] United States v. Kammersell (1999): *Kerr O.S.* The problem of perspective in Internet law. (доступна на сайте www.heinonline.org, последнее посещение – 15 декабря 2006 г.).

[2] См.: *Калятин В.О.* Право в сфере Интернета. М., 2004. С. 22.

[3] *Reed C.* Internet Law: Cases and Materials. P. 15.

придание отечественными правоприменительными органами некой особой силы оригиналам договоров утрачивает какой-либо смысл применительно к договорам, заключенным в электронной среде.

Следующей характеристикой сети Интернет, которая имеет фундаментальное значение для ее правового регулирования, является *сложность идентификации пользователей сети Интернет* (3)[1]. Пользователь может осуществлять свою информационную деятельность из любой точки мира, отправляя и получая любую информацию. Источник происхождения сообщения может быть скрытым или закодированным. Пользователь сети может иметь псевдоним или электронную идентификацию личности, отличную от его реальной идентификации[2]. Более того, обмен информацией может производиться не человеком, а компьютерной программой. Сам по себе *IP*-адрес, которым обладает каждое из устройств, подсоединенных к сети Интернет, позволяет лишь идентифицировать в сети Интернет такое устройство, но не позволяет произвести идентификацию лица, которое его использует. Максимум, что можно установить, это факт передачи информации определенным интернет-провайдером либо получение информации при помощи услуг определенного провайдера. Именно интернет-провайдер присваивает пользователю определенный *IP*-адрес, подключая его компьютер к своему каналу связи[3]. Часть *IP*-адреса идентифицирует компьютер пользователя, другая часть – идентифицирует провайдера (точнее, ту сеть, которую он контролирует).

Все это создает значительные трудности при идентификации контрагентов по договорам, заключенным в сети Интернет, а равно при идентификации лиц, ответственных за совершение правонарушений, совершенных с использованием сети Интернет. В ответ на возрастающие потребности в обеспечении определенности в отношениях с использованием сети Интернет был разработан ряд технологий, которые в совокупности с правовыми презумпциями способны обеспечить приемлемый для правового регулирования уровень определенности субъектного состава. К ним относятся как достаточно простые технологии, связанные с присвоением пользователю уникального логина и пароля, которые презюмируются известными лишь данному лицу, так и более сложные технологии, связанные с использованием электронных цифровых подписей.

---

[1] *Volker Haug*. Grundwissen Internetrecht. Stuttgart, 2005. S. 8.

[2] *Якушев М.А.* Интернет и право // Законодательство. 1997. № 1. С. 65.

[3] Как отмечается в американской литературе, «быть в Сети – означает иметь доступ к компьютеру, которому был присвоен *IP*-адрес». См.: *David Post* et al. Cyberlaw Problems of Policy and Jurisprudence in the Information Age. 2003. P. 201.

Особая роль интернет-провайдеров в осуществлении процессов информационного обмена в сети Интернет, а также зависимость пользователей от их деятельности не могут не влиять на правовые аспекты регулирования отношений в сети Интернет. Интернет-провайдеры предоставляют доступ к сети Интернет (*Access-providers*), обеспечивают возможность размещения информации в сети Интернет и обмена ею (*Hosting-providers*). Как следствие, они располагают данными, позволяющими идентифицировать пользователей сети Интернет, а также техническими возможностями по влиянию на происходящие информационные процессы[1]. *Зависимость отношений между участниками сети Интернет от интернет-провайдеров* (4) является, таким образом, еще одной фундаментальной чертой архитектуры сети Интернет. Недаром интернет-провайдеров нередко обозначают как «хранителей врат» Интернета (*Internet* «*gatekeepers*»), в связи с чем они становятся основным проводником политики государства в отношении Интернета.

Наконец, еще одной важной чертой архитектуры сети Интернет, непосредственно влияющей на возможность ее контроля, является *централизованная иерархическая структура системы адресации в сети Интернет* (5). Правильная адресация запроса в пределах одной системы возможна, только если адреса хостов не будут совпадать, иначе говоря, каждый используемый адрес должен являться *уникальным*[2]. Ведь каждое устройство, подключенное к сети Интернет, должно идентифицироваться и отграничиваться от бесчисленного множества других устройств, что может быть достигнуто лишь при наличии упорядоченной системы реестров адресов.

Система распределения *IP*-адресов построена по иерархическому принципу. *ICANN* (*Internet Corporation for Assigned Names and Numbers*), некоммерческая организация, созданная по законодательству штата Калифорния, США, осуществляет координацию распределения *IP*-адресов и корреспондирующих им доменных имен. Подробнее вопросы, связанные с регистрацией доменных имен, будут рассмотрены далее. Необходимо подчеркнуть, что в основе деятельности *ICANN* лежит Меморандум о взаимопонимании, заключенный с Министерством торговли США, которое обладает определенными контрольными функциями в отношении деятельности *ICANN*[3]. Несмотря на международный

[1] *Savin A.* EU Internet Law. Edward Elgar: Cheltenham. 2013. P. 104.

[2] *Калятин В.О.* Доменные имена. М., 2005. С. 9.

[3] www.icann.org/en/about/agreements/mou-jpa/icann-mou-25nov98-en.htm. Впоследствии данный Меморандум был заменен на Соглашение о совместной проектной деятельности (*Joint Project Agreement*), заключенное в 2006 г.

характер деятельности *ICANN* и активное участие в ней интернет-сообщества, государственных органов различных стран, данная компания, находясь под юрисдикцией США, обладает фактическим контролем над реестрами, содержащимися в корневых серверах. Удаление записи о каком-либо доменном имени из соответствующего реестра означает «смерть» ресурса в сети Интернет, так как его просто не будут «видеть» все остальные компьютеры, подключенные к Интернету[1]. Некоторые авторы видят в наличии у определенных субъектов такой фактической власти возможность установления экстерриториальной юрисдикции над интернет-отношениями, потенциально даже более эффективной, нежели обычная территориальная юрисдикция, с которой сопряжены проблемы последующего принудительного исполнения вынесенного решения в другой стране[2]. В качестве примера реализации *ICANN* своих полномочий можно привести Типовую политику разрешения споров о доменных именах (*Uniform Domain Name Dispute Resolution Policy*), регламентирующую процедуры рассмотрения споров между владельцами доменных имен и товарных знаков, которой должны придерживаться все регистраторы доменных имен верхнего уровня.

На данный момент пока отсутствуют серьезные основания для того, чтобы сгущать краски и опасаться диктатуры *ICANN* в вопросах регулирования отношений в сети Интернет. Однако потенциальные возможности данной организации в этой сфере, предопределенные архитектурой сети Интернет, не следует недооценивать и не исключено, что объем нормотворчества *ICANN* будет со временем возрастать.

Итак, архитектура сети Интернет отличается следующими особенностями: *отсутствие географических границ; особая децентрализованная процедура доставки сообщений; сложность идентификации пользователей; зависимость происходящих в сети Интернет процессов и отношений от интернет-провайдеров; иерархическая структура адресации в сети Интернет, создающая потенциальные условия для централизованного регулирования отдельных видов отношений в сети Интернет*.

---

[1] В условиях все большей зависимости жизни общества от сетей исключение из сети рано или поздно может стать таким же решающим для социального статуса, каким когда-то было исключение человека из античного полиса или отлучение от церкви. См. подробнее: *Войниканис Е.* Право интеллектуальной собственности в цифровую эпоху. Парадигма баланса и гибкости. М., 2013. С. 35.

[2] См.: *Бабкин С.А.* Интеллектуальная собственность в сети Интернет. М., 2006. С. 247.

Глава 2. Юрисдикционные аспекты электронной коммерции

§ 1. Общие положения о юрисдикции в сети Интернет

Вопросы, связанные с юрисдикцией, являются, пожалуй, одними из наиболее часто и широко обсуждаемых со времен начала дискурса по вопросам регулирования отношений в сети Интернет.

Сложности начинаются уже при попытке определения термина «юрисдикция». Дело в том, что его значение может существенно варьироваться в зависимости от контекста и правопорядка. Неудивительно, что единого понимания данного термина в науке и практике до сих пор не было выработано, что отмечают как зарубежные и отечественные ученые[1], так и суды[2].

Так, понятие «юрисдикция» может использоваться в весьма широком смысле, в частности как синоним определенной системы права (*civil law jurisdiction*, *common law jurisdiction*) или правопорядка определенного государства[3]. Иногда под юрисдикцией понимают право, применимое к определенному отношению (*governing law*)[4]. Весьма часто юрисдикция определяется как компетенция судов конкретного государства по рассмотрению и вынесению решений по данному спору[5].

В международно-правовых актах юрисдикция обычно рассматривается с позиции возможности распространения суверенной власти государства на какие-либо объекты или участки территории, т.е. как

---

[1] См., например: *Akehurst M.* Jurisdiction in International Law // Jurisdiction in International Law // Ed. by W.M. Reisman. Dartmouth, 1999. P. 145; *Каюмова А.Р.* Понятие и содержание юрисдикции в доктрине международного и внутригосударственного права // Известия вузов. Правоведение. 2011. № 4; Международное право. Общая часть: учебник / отв. ред. Р.М. Валеев, Г.И. Курдюков. М., 2011.

[2] United Phosphorus Ltd v. Angus Chemical Co., 322 F.3d 942, 948 (7th Cir. 2003): «Юрисдикция – это слово, имеющее много и даже слишком много значений».

[3] См., например: *Scassa T., Currie R.* New First Principles? Assessing the Internet's Challenges to Jurisdiction // Georgetown Journal of International Law. No 42. 2011. P. 1023. http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2116364

[4] *Yee Fen Lim*. Op. cit. P. 18.

[5] *Collier J.G.* Conflict of Laws. 3rd ed. Cambridge University Press, 2001. P. 71.

проявление территориального верховенства[1]. В доктрине подобное публично-правовое понимание юрисдикции находит свое отражение в формулировках вроде следующих: «возможность государства реализовывать власть в отношении всех объектов и субъектов, расположенных на его территории», «сфера суверенной власти государства по законодательству, суду, управлению»[2]; «право государства устанавливать общеобязательные правила поведения и применять в случае их нарушения предусмотренные законом меры ответственности»[3].

Многоаспектный характер понятия «юрисдикция» нередко представляется в виде трех его составляющих: предписывающей юрисдикции (*jurisdiction to prescribe*), судебной юрисдикции (*jurisdiction to adjudicate*) и принудительной юрисдикции (*jurisdiction to enforce*). Предписывающая юрисдикция представляет собой полномочие государства устанавливать общеобязательные правила поведения (принимать нормативные правовые акты); судебная – полномочие государства подчинять физических и юридических лиц выносимым его судами решениям; принудительная – полномочие государства осуществлять принудительное исполнение вынесенных его органами решений, в том числе судебных[4].

Как можно судить из приведенных подходов к дефиниции понятия «юрисдикция», данное явление так или иначе всегда связано с государством и реализацией им своих властных полномочий, а вместе с ним и с понятием суверенитета государства, предполагающим, что государственная территория находится под исключительной и полной властью лишь одного государства и недоступна для действия властей другого государства[5].

По общему правилу под действие властных велений государства подпадают: 1) граждане такого государства и юридические лица, созданные (зарегистрированные) на его территории[6], а также 2) объекты,

---

[1] Международное право. Общая часть: учебник / отв. ред. Р.М. Валеев, Г.И. Курдюков.

[2] *Лунц Л.А.*, *Марышева Н.И.* Международный гражданский процесс. М., 1976. С. 58.

[3] *Кемрадж А.С.* К вопросу о юрисдикции государства в отношении отдельных сегментов сети Интернет // Правовые аспекты использования интернет-технологий. М., 2002. С. 10.

[4] Данная классификация нашла свое отражение в некоторых правительственных документах. См., например: Recommendation No R (97) 11 of the Committee of Ministers of member States of the amended Model plan for the classification of documents concerning State Practice in the Field of Public International Law.

[5] См.: *Молодцов С.В.* Некоторые вопросы территории в международном праве // Советское государство и право. 1954. № 8. С. 63.

[6] Black's Law Dictionary 9th ed. 2011. Thomson West. P. 927.

расположенные на его территории, в том числе и информация, размещенная на территории такого государства (в виде материальных носителей с такой информацией, коими могут выступать серверы и иные компьютерные устройства).

Если деятельность граждан и юридических лиц никоим образом не выходит за пределы территории определенного государства, то вопросов, связанных с юрисдикцией органов такого государства, определения применимого права, а также юридических возможностей по исполнению вынесенных решений, не возникает в принципе. Однако применительно к деятельности, осуществляемой в сети Интернет, такая ситуация далеко не всегда имеет место быть. Как отмечалось ранее, одной из фундаментальных архитектурных особенностей сети Интернет является ее безразличие к географическим границам. Контент в сети Интернет может быть без особых затруднений перемещен с одного сервера на другой, а также быть одновременно размещенным на различных серверах, расположенных в разных странах. Будучи размещенным в сети Интернет, такой контент становится доступным любому лицу, подключенному к сети, тем самым беспрепятственно «проникая» на территорию разных государств. Любое распространение информации в сети Интернет тем самым способно породить отношения, носящие *потенциально трансграничный характер*[1]. В то же время решение вопросов юрисдикции всегда предполагает привязку отношений к определенной территории (локализацию), в связи с чем классические подходы к определению юрисдикции нередко весьма сложно «транслируются» на отношения, возникающие в сети Интернет.

Как следствие, правовые нормы одновременно сразу нескольких стран могут допускать установление компетенции государственных органов разных стран в отношении одного и того же правоотношения и его субъектов. Принимая во внимание тот факт, что суды, как, впрочем, и любой государственный орган, действуя от имени государства, реализуют одну из важных составных частей суверенитета этого государства, при решении вопросов юрисдикции они руководствуются положениями своего внутреннего законодательства и не принимают во внимание возможности установления юрисдикции по данному вопросу иным государством.

Особые сложности возникают в тех случаях, когда те или иные нормы, действующие в одном государстве, нарушаются иностранными гражданами или юридическими лицами. Так, законодательство одного государства может содержать запрет на осуществление опре-

[1] См.: *Бабкин С.А.* Интеллектуальная собственность в сети Интернет. С. 222.

деленной деятельности в сети Интернет (организация азартных игр, продажа алкогольных напитков, лекарств, товаров с нацистской символикой и т.п.), в то время как законодательство другого государства, национальность которого имеет юридическое лицо, организовавшее такую деятельность, не содержит. В условиях, когда граждане первого государства имеют доступ к такому интернет-сайту, деятельность такого интернет-сайта нарушает законодательство этого государства, в связи с чем вполне понятны попытки его государственных органов установить свою юрисдикцию в отношении иностранного лица – владельца сайта, чтобы пресечь указанное нарушение. В результате может возникнуть ситуация, когда юрисдикция одного государства будет носить *экстерриториальный характер*, т.е. представлять собой попытку распространить сферу действия своих законов за пределы своей территории[1]. С другой стороны, судебные решения, вынесенные иностранным государством, являются необязательными для судов другого государства. Для того чтобы стать таковыми, они должны пройти специальную процедуру признания и приведения в исполнение, в рамках которой суд, руководствуясь уже нормами своего законодательства, будет определять, насколько обоснованным было рассмотрение данного спора иностранным судом. Учитывая, что законы и представления о справедливости в разных странах различаются, а также тот факт, что вопросы действия иностранных властных актов на территории другого государства являются весьма «чувствительными» для его суверенитета и нередко приобретают политический окрас, добиться реального исполнения судебного решения против иностранного лица, которое своей деятельностью в сети Интернет нарушило законы страны, где было вынесено такое решение, весьма проблематично.

Если посмотреть на ситуацию с другой стороны, то нередко можно увидеть, что ответчик нередко никакого намерения нарушать законы другой страны не имел и даже не ожидал вероятности привлечения его к суду в таком иностранном государстве. Глупо ожидать от любого лица знания и соблюдения законодательства всех стран, где имеется доступ к сети Интернет. Поиск справедливого баланса между национальными интересами государства и интересами иностранных лиц, осуществляющих деятельность в сети Интернет, является одной из наиболее сложных проблем при решении вопросов юрисдикции в сети Интернет.

Можно привести несколько резонансных дел, которые наглядно иллюстрируют обозначенные проблемы.

[1] См., например: *Dodge W.S.* Extraterritoriality and Conflict-of-Laws Theory: an Argument for Judicial Unilateralism // Harvard International Law Journal. 1998. No 39. 101.

1. *Dow Jones & Co. Inc. v. Gutnik*[1]. Данное дело дошло до Верховного суда Австралии и представляет собой ставшим образцовым пример рассмотрения спора о защите чести, достоинства и деловой репутации вследствие распространения порочащих сведений в сети Интернет иностранным лицом. В качестве ответчика выступала известная американская компания *Dow Jones*, являющаяся одним из ведущих мировых агентств финансовой информации и учредителем журнала *Barron's*. Данный журнал опубликовал в печатной и онлайн-версии статью под названием «Порочные доходы» («*Unholy Gains*»), из которой можно было сделать вывод о причастности истца, Джозефа Гутника, к налоговым махинациям. Особенностью данного спора являлся тот факт, что истец предъявил иск в австралийский суд по месту своего жительства, притом что на территории Австралии было распространено только пять бумажных экземпляров издания. Интернет-версия насчитывала порядка 550 000 подписчиков, из которых всего 1700 были из Австралии. Суд, несмотря на это, все же принял иск к рассмотрению и удовлетворил требования истца, указав, что «если кто-либо собирается делать бизнес в определенной стране или жить в ней, просто попутешествовать по ней, никто не ожидает, что такое лицо будет освобождено от обязанности соблюдения ее законов. Тот факт, что событие в сети Интернет происходит одновременно «везде», не означает, что оно происходит «нигде». Отвергая аргумент ответчика о том, что подобный подход приводит ко всемирной юрисдикции и бремени проверки материала на предмет соответствия диффамационным законам, существующим по всему миру, возлагаемом на каждое лицо, размещающее его в сети Интернет, суд указал, что данные опасения беспочвенны: идентифицируя лицо, которому посвящен такой материал, всегда можно определить суд, в который оно может обратиться, и право, регулирующее такие отношения. В итоге дело завершилось мировым соглашением, по которому *Dow Jones* согласилась выплатить компенсацию и опубликовала опровержение.

2. Дело *Yahoo!, Inc. v. LICRA*[2] получило еще больший резонанс, поскольку затронуло публичный интерес разных государств. Суть дела сводилась к следующему. На американском сайте компании *Yahoo!* осуществлялась продажа предметов нацистской атрибутики. Доступ к данному сайту имели французские граждане. Согласно французскому законодательству продажа подобных товаров запрещена. Французская

[1] Dow Jones & Co. Inc. v. Gutnik, [2002] HCA 56, 210 CLR 575.

[2] Yahoo!, Inc. v. La Ligue Contre Le Racisme et L'Antisemitisme 145 F. Supp. 2d 1168 (N.D. Cal. 2001).

общественная организация по борьбе с расизмом и антисемитизмом (*LICRA*) обратилась с жалобой на компанию *Yahoo!*, *Inc.* в суд г. Парижа. Суд в решении от 22 мая 2000 г. признал жалобу обоснованной и обязал американскую компанию принять меры по блокировке доступа французских граждан к американскому сайту, а также разместить на французском сайте компании предупреждение о том, что использование поисковой системы *Yahoo!* может привести к обнаружению материалов, запрещенных в соответствии со ст. 645-1 УК Франции. Суд отверг довод ответчика об отсутствии юрисдикции французского суда над американской компанией, указав, что если соответствующий материал, содержащийся в сети Интернет, доступен во Франции, владелец веб-страницы должен соблюдать французское законодательство. В ответ компания *Yahoo!* заявила ходатайство в окружной суд Калифорнии о констатации решения французского суда недействительным и не имеющим силы на территории США, поскольку нарушает гарантируемое Конституцией США право на свободу слова. В ответ организация *LICRA* сделала заявление об отсутствии у американского суда юрисдикции в отношении нее. Суд отверг заявление ответчика и удовлетворил требования *Yahoo!*, указав, что «мирное выражение агрессивных точек зрения предпочтительнее установления государственного контроля над свободой слова», а также то, что «если исполнение иностранного судебного решения противоречит интересам США, американский суд не обязан его исполнять».

Данные споры достаточно убедительно иллюстрируют тот факт, что вопросы компетентности иностранного суда по рассмотрению спора, вопросы применимого права и перспективы принудительного исполнения решения иностранного суда должны рассматриваться комплексно. Только такой подход позволяет создать целостную картину и оценить риски быть привлеченным в качестве ответчика в иностранном суде в связи с деятельностью, осуществляемой в сети Интернет. Поэтому за основу при дальнейшем рассмотрении данной проблематики в данной работе будет взято описанное ранее комплексное понимание юрисдикции как предписывающей юрисдикции (*jurisdiction to prescribe*), судебной юрисдикции (*jurisdiction to adjudicate*) и принудительной юрисдикции (*jurisdiction to enforce*).

Прежде чем перейти к рассмотрению положений российского законодательства по данным вопросам, имеет смысл остановиться на существующих в США и Европейском союзе подходах к определению юрисдикции, применимого права и порядка исполнения иностранных судебных решений. С практической точки зрения это позволит оценить

и минимизировать риски возникновения нежелательных процессов в таких странах, а с научной точки зрения – ознакомиться с наиболее прогрессивными на данный момент подходами к регулированию вопросов юрисдикции в сети Интернет.

§ 2. Юрисдикция в сети Интернет по законодательству США

Законодательство США в области юрисдикции представляет собой особый интерес не только потому, что перспективы предъявления иска в американском суде способны вызвать неудобства для практически любой более-менее крупной *IT*-компании по причине неизбежной связи ее деятельности с территорией США. Основная причина заключается в том, что проблематика коллизии юрисдикций и законов является наиболее разработанной именно в США из-за особенностей их территориального устройства: каждый штат обладает широкой автономией и собственным законодательством (в том числе собственным гражданским и уголовным законодательством в отличие от России, где эти вопросы отнесены к исключительному ведению Российской Федерации), что неизбежно ставит вопрос о решении возможных коллизий не только между штатом и федеральным центром, но и между самими штатами. При этом принципы определения юрисдикции в отношении иностранных лиц аналогичны принципам ее установления в отношении резидентов иных штатов[1].

В США общий алгоритм рассмотрения вопросов, связанных с юрисдикцией суда по рассмотрению определенного спора, является следующим[2].

Во-первых, для начала суд решит вопрос о своей компетентности по рассмотрению данного спора, определив наличие предметной юрисдикции (*subject matter jurisdiction*), персональной юрисдикции (*personal jurisdiction*) и территориальной подсудности (*venue*).

Предметная юрисдикция (аналог российского понятия «подведомственность») определяет возможность суда рассматривать данную категорию спора. Принято различать суды общей юрисдикции, которые имеются в каждом штате США, а также суды ограниченной юрисдикции, которые уполномочены рассматривать лишь заранее определенные категории дел. К последним относятся, в частности, федеральные окружные суды, так как их компетенция ограничена

[1] *Graham Smith*. Internet Law and Regulation. London: Sweet & Maxwell, 2007. P. 665.

[2] *David Post*. Personal Jurisdiction on the Internet: An Outline for the Perplexed // Temple University Law School. June 1998. http://www.temple.edu/lawschool/dpost/outline.htm

определенными категориями споров (связанные с применением федеральных законов и соглашений, споры между штатами или штатом и гражданином другого штата и т.д.). Например, в соответствии с § 1332 *U.S. Code* федеральные окружные суды компетентны рассматривать гражданско-правовые споры с ценой иска более 75 000 долл. (не считая проценты и судебные издержки), если одна из сторон спора является иностранным лицом.

Персональная юрисдикция определяет компетентность суда рассматривать и выносить решения в отношении данного ответчика. Принято различать общую юрисдикцию (*general jurisdiction*), которая определяет право суда рассматривать все споры с участием такого ответчика, в том числе и не имеющие связи с территорией, где находится суд[1], и специальную юрисдикцию (*specific jurisdiction*), в основе которой лежит связь между предъявленным требованием и территорией, где расположен суд[2].

Территориальная подсудность (*venue*) представляет собой правовой механизм, обеспечивающий эффективное распределение судебных ресурсов и удобство сторон при рассмотрении спора. Нарушение правил о территориальной подсудности не влечет недействительности вынесенного решения в отличие от несоблюдения правил о предметной и персональной юрисдикции[3]. В спорах, связанных с иностранными лицами, не имеющими места жительства или местонахождения на территории США, *venue* не имеет особого значения, поскольку в соответствии с установившимся правилом иск к ним может быть предъявлен в суд любого округа, расположенного на территории соответствующего штата[4].

После того как суд положительно решит вопрос о наличии предметной и персональной юрисдикции, а также признает территориальную подсудность при отсутствии возражений сторон, суд может приступить к решению вопроса об определении применимого права к спорному требованию.

Наконец, рассмотрение спора компетентным судом по избранному им применимому праву заканчивается вынесением решения, которое в ряде случаев необходимо принудительно исполнить на другой тер-

---

[1] Black's Law Dictionary. 9th ed. 2011. Thomson Reuters. P. 929.

[2] Ibid. P. 931.

[3] *Jack H. Friedenthal* et al. Civil Procedure. 2nd ed. 1993. § 2.1; *Charles Wright*. The Law of Federal Courts. 5th ed. 1994. § 42.

[4] 28 U.S.C. § 1391(d). Brunette Mach. Works, Ltd v. Kockum Indus., Inc., 406 U.S. 706, 714 (1972).

ритории, не подведомственной данному суду, – в другом штате или государстве.

2.1. Основные источники регулирования вопросов юрисдикции в США

Весь массив правовых источников США, потенциально релевантных по отношению к вопросам юрисдикции в сети Интернет и представляющих наибольший интерес с учетом специфики настоящей работы, можно разделить на:

• источники права в классическом их понимании, т.е. носящие общеобязательный характер и обеспеченные санкцией за несоблюдение (*hard law*);

• источники «мягкого» права (*soft law*), под которым принято понимать правила, которые не являются формально обязательными, но в то же время не лишены какого-либо правового значения, выступая в качестве своего рода ориентира для участников оборота и правоприменителей[1]. «Мягкое» право, таким образом, содержит рекомендации, а не правила поведения, несоблюдение которых обеспечено какими-либо санкциями.

В числе классических источников права по рассматриваемой проблематике следует упомянуть следующие.

1. *Конституция США*. Данный акт содержит основополагающие положения по вопросам юрисдикции. К ним можно отнести: *a*) поправку XIV к Конституции о надлежащей правовой процедуре (*Due Process clause*), которая устанавливает пределы юрисдикции американских судов и составляет фундамент для решения вопросов о наличии персональной юрисдикции; *b*) положение о полном доверии и уважении (*The Full Faith and Credit Clause*: раздел 1 ст. IV), предусматривающее проявление всеми штатами США доверия и уважения к официальным актам и судебным документам любого другого штата; *c*) принцип верховенства Конституции (*The Supremacy Clause,* ст. VI); *d*) принцип недискриминации (*The Privileges and Immunities Clause,* раздел 2 ст. IV), согласно которому гражданам каждого штата предоставляются все привилегии и льготы граждан других штатов.

2. *Нормы федерального процессуального законодательства и процессуального законодательства соответствующего штата*. Данные нормы конкретизируют положения Конституции относительно компетентности суда рассматривать споры в отношении определенных лиц или предметов. Особо следует упомянуть так называемые длиннорукие законы (*long-arm statutes*) – положения процессуального законода-

[1] Black's Law Dictionary. 9th ed. 2011. Thomson West. P. 1519.

тельства, регламентирующие юрисдикцию федеральных судов либо судов штата в отношении ответчиков, не являющихся резидентами территории суда[1]. В качестве примера такого закона на федеральном уровне можно привести ст. 4 (*k*) (2) Федеральных правил гражданского процесса, содержащую положение, согласно которому федеральный суд США вправе установить юрисдикцию в отношении иностранного ответчика в тех случаях, когда он имеет достаточные контакты с территорией США, но не имеет достаточных контактов с отдельно взятым штатом, достаточным для установления юрисдикции в отношении него[2]. Каждый штат США имеет собственный «длиннорукий» закон, определяющий пределы установления его судами персональной юрисдикции над нерезидентами. На практике большинство штатов допускают установление юрисдикции в той степени, в какой это допускается с точки зрения *Due Process clause*, содержание которой истолковано в соответствующих прецедентах Верховного суда США[3]. Однако некоторые штаты содержат и более узкие по сфере своего действия *long-arm statutes*, нежели это возможно в соответствии с *Due Process clause*. В качестве примера можно привести законодательство штата Нью-Йорк[4].

3. *Единообразный торговый кодекс* (*ETK*). Первый его официальный текст был принят в 1952 г., второй (ныне действующий) – в 1990 г. ETK представляет собой собрание норм по отдельным, наиболее важным для хозяйственной деятельности институтам. Он не является федеральным законом США, поскольку гражданское законодательство находится в большинстве своем в ведении штатов. В каждом штате были приняты соответствующие редакции ETK, кроме штата Луизиана, находящегося в силу исторических причин под сильным влиянием континентально-правовых традиций (преимущественно французского права), где была принята усеченная редакция ETK, не включающая гл. 2 о купле-продаже.

4. *Единообразный закон об информационных сделках (Uniform Computer Information Transactions Ac. (UCITA))*. Данный Закон был призван обеспечить специальное правовое регулирование в отношении сделок, связанных с предоставлением объектов авторского права и иного контента

[1] Black's Law Dictionary. 9th ed. 2011. Thomson West. P. 1027.

[2] http://en.wikisource.org/wiki/United_States_Code/Title_28/Appendix/Federal_Rules_of_Civil_Procedure/Rule_4

[3] Детальный анализ законов процессуальных законов штатов в этой части см.: *David Thatch*. Personal Jurisdiction and the World-Wide Web: Bits (and Bytes) of Minimum Contacts // Rutgers Computer and Technology Law Journal No 23. 1997.

[4] См., например: New York Civil Practice Law. § 302.

в цифровой форме. Идея его разработки возникла по причине того, что в отсутствие специальных положений, посвященных данным отношениям, американские суды пытались применять нормы ЕТК о купле-продаже, которые, будучи предназначенными для оборота «классических» товаров, были мало приспособлены для регламентации нового вида отношений. Так, положения ЕТК о порядке заключения договора, отражающие подходы классического договорного права, не учитывают в полной мере сложившуюся практику заключения оберточных лицензий и *click-wrap*-соглашений (принцип «деньги сейчас, условия потом»). Регламентация гарантий, предоставляемых в отношении нового вида «товара», также требовала уточнений с учетом характера и существа отношений. Требовали своего решения и вопросы соотношения договорных условий с положениями федерального законодательства об интеллектуальной собственности США. Наконец, необходимо было адаптировать средства защиты, доступные сторонам по такого рода сделкам, и определить рамки применения способов самозащиты прав (вроде удаленной деактивации компьютерной программы). Несмотря на прогрессивный характер выработанных положений, законопроект вызвал немало дискуссий и критики как излишне защищающий права крупных компаний – производителей программного обеспечения, из-за которой он не получил широкого распространения и был имплементирован только в двух штатах – Вирджинии и Мэриленде. Некоторые штаты (Айова, Северная Каролина, Вермонт, Западная Виргиния) даже приняли специальные законы, направленные на воспрепятствование применению *UCITA* в случаях, когда право штата, имплементировавшего его, было указано в качестве применимого права договора[1].

Из положений «мягкого» права США, представляющих интерес в контексте проблематики юрисдикции в сети Интернет, следует особо упомянуть следующие.

1. *Свод норм коллизионного права* (*Restatement of Conflict of Laws*). Указанный документ представляет собой подготовленный Американским институтом права авторитетный источник, обобщающий существующее прецедентное право в сфере коллизионного регулирования и излагающий его в виде совокупности правил и принципов. Формально своды норм, подготовленные Американским институтом права, не являются обязывающими для судов, однако многие судебные решения и комментарии содержат ссылки на них. По меткому утверждению известного американского судьи Бенджамина Кардозо, «своды

[1] См.: *Ward Classen*. A Practical Guide to Software Licensing for Licensees and Licensors. ABA Publishing. 2008. P. 212.

норм проникнуты особым авторитетом, позволяющим не повелевать, но убеждать»[1]. Существует две редакции свода норм коллизионного права. *Restatement First on Conflict of Laws* (1934), который в значительной степени применяется в отдельных штатах США (Мэриленд, Вирджиния, Нью-Мексико, Южная Каролина, Джорджия, Алабама, Канзас, Вайоминг)[2]. Данный документ содержит достаточно жесткие коллизионные привязки (применительно к деликтам применяется право штата, где произошло последнее из действий, послуживших основанием для предъявления требования (§ 377); право, применимое к договорам, определяется преимущественно по праву штата, где был заключен договор (§ 311)). Произошедшие изменения в американской доктрине коллизионного права, заклеймившей такой механистический подход и выступившей за введение более гибких критериев выбора применимого права, обусловили разработку Второго свода законов в сфере коллизионного права (*Restatement Second on Conflict of Laws*, 1971), ядром которого является принцип тесной связи (*substantial relationship*). Подходы, заложенные в данной версии документа, нашли свое отражение в той или иной степени в штатах Нью-Йорк, Делавэр, Колорадо, Коннектикут, Аляска, Аризона, Калифорния, Айдахо, Иллинойс, Айова, Майне, Миссисипи, Миссури, Монтана, Небраска, Южная Дакота, Огайо, Техас, Юта, Вермонт, Вашингтон[3]. Данный Свод содержит в себе обширный перечень вопросов, связанных с юрисдикцией, определением применимого права, принудительным исполнением судебных решений. Несмотря на то что во время составления данного Свода в 1971 г. об Интернете еще не задумывались, подходы и принципы, заложенные в нем, являются отправной точкой для анализа всей проблематики юрисдикции в сети Интернет.

2. *Принципы определения юрисдикции, применимого права и принудительного исполнения судебных решений в сфере интеллектуальной собственности* (*Intellectual Property*: *Principles Governing Jurisdiction*, *Choice of Law*, *and Judgments in Transnational Disputes*. *ALI*, 2007). Данный документ, подготовленный Американским институтом права, содержит в себе положения, регламентирующие коллизионно-правовые аспекты трансграничных споров в сфере интеллектуальной собственности: принципы юрисдикции, определения применимого

[1] *Cardozo B.* The Growth of the Law. Yale University Press, 1924. P. 9.

[2] *Freiheit J.* Proskauer on International Litigation and Arbitration: Ch. 7 Choice of Law Issues. Selecting the Appropriate Law. www.proskauerguide.com/litigation/7/IV

[3] *Symeonides S.* Choice of Law in the American Courts in 2006: Twentieth Annual Survey // American Journal of Comparative Law. No 54. 2006. P. 697, 712.

права, исполнения судебных решений. Указанный документ в отличие от Свода правил коллизионного права разрабатывался с учетом проблематики, которую привносит Интернет в подобного рода споры. Примечательно, что он предназначен для использования в качестве ориентира не только для юристов англо-американской системы права, но и для континентальных юристов, что нашло отражение в используемой терминологии[1].

3. *Принципы договорного права в сфере программного обеспечения* (*ALI Principles of the Law of Software Contracts*, 2009). Указанные принципы, также подготовленные Американским институтом права, представляют собой более мягкий вариант *UCITA*, не претендуя на роль буквы закона[2]. В отличие от *UCITA* сфера их применения ограничена сделками с определенным видом цифрового контента – компьютерными программами. Принципы содержат в себе обобщение существующей практики в сфере оборота программного обеспечения и сформулированные на ее основе «лучшие практики». В контексте вопросов юрисдикции в сети Интернет наибольший интерес представляют положения § 1.13 (выбор применимого права) и § 1.14 (юрисдикционная оговорка).

Теперь имеет смысл подробнее остановиться на том, как в США решаются вопросы, связанные с установлением американским судом персональной юрисдикции в отношении иностранного лица, выбором применимого права, а также принудительным исполнением иностранных судебных решений.

2.2. Условия установления персональной юрисдикции в отношении иностранного лица (jurisdiction to adjudicate)

По общему правилу, для того чтобы американский суд имел персональную юрисдикцию в отношении ответчика, необходимо одно из следующих оснований: проживание или учреждение ответчика на территории штата, где расположен суд (1); согласие ответчика с юрисдикцией, выраженное в договоре (2); вручение повестки на территории штата, где расположен суд (3).

В отсутствие указанных оснований суд должен рассмотреть вопрос о том, насколько установление юрисдикции в отношении иностранного лица является допустимым с точки зрения положений *long-arm*

[1] Intellectual Property: Principles Governing Jurisdiction, Choice of Law, and Judgments in Transnational Disputes. American Institute of Law. Proposed final draft, 2007. Reporter's memorandum. P. XIX.

[2] ALI Principles of the Law of Software Contracts. Proposed final draft, 2009. P. 2.

statute соответствующего штата и Конституции США (*Due process clause*). Установив наличие основания для установления юрисдикции в *long-arm statute*, суд далее проводит анализ на предмет того, насколько ее осуществление соответствует требованиям Конституции США (*Due process clause*)[1], которая запрещает вынесение решения против лица, не имеющего контактов, связей или отношений с соответствующим штатом[2], и порядок применения которой истолкован в прецедентах Верховного суда США[3].

Одним из основных прецедентов, определяющих понимание *Due Process clause* для целей установления персональной юрисдикции, долгое время являлось дело *Pennoyer v. Neff*, в котором Верховный суд США указал, что физическое присутствие лица на территории штата является необходимым условием для осуществления в отношении него юрисдикции судом такого штата[4]. Данное правило достаточно быстро вошло в противоречие с реалиями коммерческой жизни, где основным игроком стали юридические лица. Учитывая, что юридическое лицо само по себе является фикцией, применение данного правила к коммерческой деятельности, осуществляемой такой «фикцией» на территории разных штатов, встретило существенные затруднения.

В 1945 г. Верховный суд США в знаменитом деле *International Shoe v. Washington* сформулировал новый подход, согласно которому персональная юрисдикция может быть установлена в том числе и если ответчик физически не присутствует на территории штата, «но имеет с ней определенные минимальные контакты, и рассмотрение спора не нарушает устоявшихся принципов правосудия и справедливости»[5]. Таким образом, в отсутствие традиционных оснований для установления персональной юрисдикции суд должен проанализировать характер деятельности («контактов») ответчика на территории штата, где расположен суд, и то, насколько распространение юрисдикции на такого ответчика является разумным и справедливым.

Анализ существующих контактов ответчика с территорией штата будет различным в зависимости от того, какой тип персональной юрис-

---

[1] In re Ski Train Fire in Kaprun, Austria on Nov. 11. 2000. 342 F. Supp. 2d 207 (S.D.N.Y. 2004).

[2] Соответствующее толкование было дано положениям V и XIV поправок к Конституции США, образующим Due Process Clause Верховным судом США в деле International Shoe v. Washington 326 U.S. 310 (1945).

[3] Детальный анализ процессуальных законов штатов в этой части см.: *David Thatch*. Op. cit.

[4] 95 U.S. 714 (1877).

[5] 326 U.S. 310 (1945).

дикции испрашивается: общий или специальный[1]. Для установления общей юрисдикции, позволяющей привлекать иностранное лицо в качестве ответчика по *любым* требованиям, необходимо, чтобы контакты со штатом были продолжительными, систематическими и существенными[2]. При этом могут приниматься во внимание такие обстоятельства, как наличие физического присутствия в виде движимого или недвижимого имущества, получение лицензии на определенный вид деятельности[3], общий объем прибыли, получаемой от коммерческой деятельности в данном штате[4].

В отсутствие оснований для установления общей юрисдикции специальная юрисдикция устанавливается при наличии минимальных контактов ответчика с территорией штата при условии, что ответчик должен разумно допускать возможность подпадания под юрисдикцию такого штата (*purposeful availment*). Такое допущение может быть сделано на основании действий ответчика, свидетельствующих о наличии намерения ответчика воспользоваться преимуществами и защитой, предоставляемой соответствующим штатом[5]. Указанное дополнительное требование направлено на защиту интересов ответчика, минимизируя неопределенность, которую могут вызвать его случайные, непроизвольные или поверхностные (*random, fortuitous and attenuated*) контакты с определенной территорией. В качестве примера такого случайного контакта можно привести известный прецедент *World-Wide Volkswagen Corp. v. Woodson*[6], в котором молодая пара, проживающая в Нью-Йорке, приобрела автомобиль в данном штате и попала в аварию, проезжая по территории штата Оклахома в направлении

---

[1] Разделение персональной юрисдикции на два типа – *general* и *specific* – было впервые сформулировано в знаменитой статье: *Arthur von Mehren, Donald Trautman*. Jurisdiction to Adjudicate: A Suggested Analysis // Harvard Law Review. No 79. 1966.

[2] Данный критерий неоднократно выделялся Верховным судом США: Perkins v. Benguet Consol. Mining Co. 342 U.S. 437 (1952); Helicopteros Nacionales de Colombia, S.A. v. Hall. 466 U.S. 408 (1984).

[3] См., например: Bird v. Parsons, 289 F. 3d 865, 873 (6th Cir. 2002); Butler v. Beer Across Am., 83 F. Supp. 2d 1261 (N.D. Ala. 2000).

[4] См., например: William Rosenstein & Sons Co v. BBI Produce, Inc., 123 F. Supp. 2d 268 (M.D. Pa. 2000). В данном деле суд указал, что продажи товара ответчиком в данном штате составляли всего 0,05% от всего объема продаж, чего явно недостаточно для установления общей юрисдикции. Gator.com Corp. v. L.L. Bean, Inc. 341 F.3d 1072 (9th Cir. 2003) (здесь доля продаж в штате в размере 6% от всего объема продаж была признана достаточной для установления общей юрисдикции, хотя суд и не указал, каков именно процент был сделан непосредственно через интернет-сайт).

[5] Данное правило впервые сформулировано Верховным судом США в деле Hanson v. Denckla, 357 U.S. 235, 252 (1958).

[6] 444 U.S. 286 (1980).

Аризоны. Причиной аварии являлась неисправность автомобиля, что повлекло предъявление иска к региональному дистрибьютору, через которого был приобретен автомобиль, в штате Оклахома, где он не осуществлял продаж своих автомобилей и не вел какого-либо иного бизнеса. Верховный суд США истолковал контакт ответчика со штатом Оклахома в качестве случайного и не дающего оснований для установления персональной юрисдикции.

Наконец, последним условием для осуществления персональной юрисдикции является ее разумность. Судом при этом могут приниматься во внимание различные факторы: обременительность рассмотрения спора на данной территории для ответчика; наличие интереса данного штата в рассмотрении такого спора; интерес истца в получении эффективной защиты своих прав; интерес судебной системы в целом в наиболее эффективном рассмотрении возникшего спора; общий интерес различных штатов в проведении определенной социальной политики[1]. В настоящее время пока не сложилось более или менее однозначной практики применения данных положений, в связи с чем соотношение данных требований с установленными минимальными контактами при решении вопроса об установлении персональной юрисдикции является неоднозначным[2].

Бремя доказывания наличия юрисдикции несет истец. Суд может оказать содействие в установлении определенных фактов, свидетельствующих о ее наличии (*jurisdictional discovery*), за исключением случаев очевидной необоснованности иска[3].

Необходимо отметить, что даже в случае наличия формальных оснований для установления персональной юрисдикции в отношении ответчика суд может отказать в этом со ссылкой на то, что место рассмотрения спора является существенно неудобным (*forum non conveniens*) и у истца имеется возможность предъявления иска в более удобном месте[4]. Как указал Верховный суд США, «каждый раз, когда встает вопрос о применении данной доктрины, предполагается наличие как минимум двух государств, где может быть рассмотрен спор, и указанная доктрина устанавливает критерии выбора между ними»[5]. Решая вопрос о возможности отказа в рассмотрении спора со ссылкой на *forum*

[1] Burger King Corp. v. Rudzewicz, 471 U.S. 462 (1985).

[2] *Nemeyer Q*. Don't Hate the Player, Hate the Game: Applying the Traditional Concepts of General Jurisdiction to Internet Contacts // Loyola Law Review. No 52. 2006. P. 155.

[3] Mass. Sch. of Law at Andover, Inc. v. Am. Bar. Ass'n, 107 F.3d, 1026, 1042 (3d Cir. 1997).

[4] § 84 Restatement Second on Conflict of Laws; Barett Edward. Doctrine of Forum Non Conveniens // California Law Review. No 35. 1947.

[5] Gulf Oil Corp. v. Gilbert, 330 U.S. 501, 506-07 (1947).

non conveniens, суды обычно последовательно используют следующие критерии (*three-part test*):

1) насколько выбор суда истцом является обоснованным и заслуживающим уважения. По общему правилу если в качестве истца выступает американское лицо, то он воспринимается судом с большим уважением, нежели выбор американского суда иностранным истцом[1]. Известно, что многие истцы, обладая формально возможностью выбора места предъявления иска, предпочитают юрисдикцию, наиболее благоприятную для них с точки зрения доступных средств защиты, возможной суммы взыскания, процессуальных правил и пр. Такое явление получило на практике наименование «*forum shopping*». Разумеется, нередко такие действия приводят к существенным обременениям для ответчика в виде временны́х и материальных расходов на участие в таком споре. Доктрина *forum non conveniens* дает суду *право* отказать в рассмотрении спора в случае явного *forum shopping*[2];

2) насколько доступным и адекватным является альтернативное место рассмотрения спора. Сам по себе факт наличия отличий в материальном праве не имеет значения для рассмотрения вопроса об адекватности альтернативного форума[3]. Однако политическая нестабильность может выступать в качестве фактора для признания альтернативного места рассмотрения спора неадекватным[4]. Необходимость определения и применения иностранного права, существенные обременения для ответчика, связанные с переводом документов на английский язык, значительные транспортные расходы также могут быть приняты во внимание в решении вопроса об отказе в установлении юрисдикции со ссылкой на доктрину *forum non conveniens*[5];

3) соотношение публичных и частных интересов. Так, например, судьи Южного округа штата Нью-Йорк традиционно считают себя одними из наиболее перегруженных в США, в связи с чем заинтересованы в отсеивании споров, не имеющих достаточной связи с их территорией[6]. Также исходя из соображений публичного порядка и международной вежливости американские суды уважают право иностранного суда рассмотреть спор в случаях, когда у него на то есть больше оснований.

---

[1] Piper Aircraft Co. v. Reyno, 454 U.S. 235, 256 (1981).

[2] Iragorri v. United Techs. Corp., 274 F.3d 65, 71, 73 (2d Cir. 2001).

[3] Piper Aircraft Co. v. Reyno, 454 U.S. 235, 256 (1981).

[4] Hatzlachh Supply, Inc. v. Tradewind Airways, Ltd, 659 F. Supp. 112 (S.D.N.Y. 1987); Canadian Overseas Ores Ltd. v. Compania de Acero del Pacifico S.A., 528 F. Supp. 1337 (S.D.N.Y. 1982).

[5] Blanco v. BancoIndus. de Venezuela, S.A., 997 F.2d 974 (2nd Cir. 1993).

[6] Doe v. Hyland Therapeutics Div., 807 F. Supp. 1117 (S.D.N.Y. 1992).

Приведенные выше принципы определения персональной юрисдикции нашли свою конкретизацию применительно к отношениям в сети Интернет. Вопреки распространенным в американской доктрине мнениям о необходимости выработки принципиально новых подходов к определению юрисдикции в сети Интернет[1] суды продолжали применять уже сложившееся законодательство. И, надо сказать, не без успеха.

Одним из наиболее острых стал вопрос о том, какое влияние имеет сайт в сети Интернет, доступный на территории соответствующего штата, на возможность установления персональной юрисдикции в отношении лица, разместившего соответствующую информацию на нем и не являющегося резидентом такого штата. Ведь информация, размещенная в сети Интернет, является потенциально доступной на территории всех штатов США. При этом каждый штат США по-своему регламентирует вопросы, связанные с распространением алкогольной продукции, допустимости азартных игр, защитой прав потребителей, защитой чести, достоинства и деловой репутации, и т.д. В связи с этим неудивительно, что деятельность участников сети Интернет, игнорирующая эти положения, не могла не вызвать попыток «подчинить» ее соответствующим локальным законодательным положениям.

Одним из первых подходов, достаточно быстро отвергнутых последующей практикой[2], был отражен в решении по делу *Inset Systems, Inc. v. Instruction Set, Inc.*[3] Компания, инкорпорированная в штате Коннектикут, предъявила иск о нарушении ответчиком прав на товарный знак регистрацией доменного имени с обозначением, эквивалентным товарному знаку истца (*inset.com*). Иск был предъявлен по местонахождению истца, в штате Коннектикут, на что ответчик заявил возражение об отсутствии у данного суда юрисдикции в отношении него. Суд не согласился с ответчиком, указав, что одного только факта размещения рекламы на веб-сайте достаточно для установления юрисдикции судом любого штата, на территории которого данный сайт доступен. В качестве обоснования указывалось, что реклама, размещенная на сайте, будучи потенциально доступной в масштабах всей страны, создает беспрецедентные условия для осуществления продаж в масштабах всей страны. Получение подобной выгоды возможно, по мнению суда, только при условии одновременного принятия на себя связанных

[1] См., например: *Johnson D., Post D.* Op. cit.

[2] В литературе его даже именуют аномалией в мире киберюрисдикции. См.: *Yvonne Beshany., Sean Shirley.* Cyber-Jurisdiction: When Does Use of the Internet Establish Personal Jurisdiction? // Alabama Law. No 63. 2002. P. 38.

[3] 937 F. Supp. 161 (D. Conn. 1996).

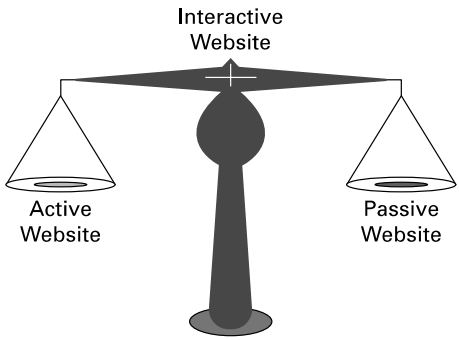
с этим рисков и обременений, к числу которых относится возможность предъявления иска к компании за пределами ее родного штата.

Данному подходу нельзя отказать в определенной логике. Однако несложно увидеть, что он создает возможность для предъявления иска к организации, ведущей деятельность в сети Интернет, практически в любой точке планеты, даже в тех странах, на которые эта деятельность не была направлена в принципе. Это создает чрезмерную неопределенность и означает необходимость принятия субъектом электронной коммерции на себя потенциально некалькулируемых рисков в силу одного только факта размещения информации в сети Интернет. Таким образом, такой подход по существу влечет установление *универсальной* юрисдикции в сети Интернет. Американцы, традиционно весьма трепетно относящиеся к вопросам распределения рисков, не могли долго придерживаться данного подхода. Да и сложившимся в доИнтернет эпоху принципам установления персональной юрисдикции подход *Inset* не очень соответствовал (речь идет о принципе *purposeful availment*). Требовался более тонкий подход, при котором для установления юрисдикции помимо факта доступности сайта на определенной территории необходимо было нечто большее.

Наиболее известным прецедентом, конкретизировавшим это «нечто большее», в течение долгого времени являлось дело *Zippo Manufacturing Co. v. Zippo Dot Com*, *Inc*.[1] Компания *Zippo*, всемирно известный производитель зажигалок, инкорпорированная в штате Пенсильвания, предъявила иск к компании *Dot Com*, инкорпорированной в штате Калифорния, основным видом деятельности которой являлось распространение платной подписки на новости. Иск был предъявлен в суд штата Пенсильвания в связи с нарушением ответчиком прав на товарный знак путем регистрации доменного имени, включающего обозначение «*Zippo*». Ответчик возражал против юрисдикции суда штата Пенсильвания, утверждая, что его контакты с данным штатом носят случайный характер, ссылаясь на вышеупомянутый прецедент *World-Wide Volkswagen Corp. v. Woodson*. Рассматривая вопрос о допустимости установления персональной юрисдикции над ответчиком, суд выработал тест скользящей шкалы (*sliding scale test*). Суть его заключалась в том, что все веб-сайты в сети Интернет делились на три категории (рисунок). С одной стороны шкалы находились так называемые пассивные сайты (*passive websites*), носящие исключительно информационный характер и не дающие оснований для установления юрисдикции на факте их доступности на территории определенного

[1] 952 F. Supp. 1119 (W.D. Pa. 1997).

штата[1]. На другом конце шкалы располагаются активные сайты, через которые лицо осуществляет предпринимательскую деятельность с резидентами иных штатов посредством систематической намеренной передачи компьютерных файлов в данные штаты (*active websites*), что влечет возможность установления юрисдикции судами таких штатов. Посередине располагаются сайты разной степени интерактивности, позволяющие пользователю осуществлять с ними обмен информацией. Возможность установления юрисдикции в таких случаях зависит от уровня интерактивности такого сайта и наличия коммерческой составляющей в информации, выступающей предметом обмена.



[2]

Применяя данный тест к обстоятельствам дела, суд признал сайт ответчика в достаточной степени интерактивным, так как он позволял разместить заказ на услуги ответчика не только по телефону, но и непосредственно на сайте. К тому же было установлено, что ответчик имел порядка 3000 подписчиков и 7 контрактов с интернет-провайдерами на территории штата Пенсильвания. Как следствие, суд отверг аргумент ответчика о случайном характере его контактов с территорией данного штата[3]. Если бы ответчик хотел избежать юрисдикции

[1] Во многом такой подход американских судов к пассивным сайтам обусловлен аналогией с размещением рекламы в общенациональных средствах массовой информации: доступность такой рекламы в определенном штате не является по общему правилу основанием для установления юрисдикции суда такого штата. См.: *Thomson G.* Personal Jurisdiction in Internet-Related Litigation / Online Contract Formation ed. by S. Kinsella and A. Simpson. 2004. P. 503 ff.

[2] Данная иллюстрация взята из работы: *Faye Fangrei Wang.* Internet Jurisdiction and Choice of Law: Legal Practices in the EU, US and China. Cambridge, 2010. P. 69.

[3] Суд не поленился при этом привести пример случайного контакта, транслированного на материю сети Интернет: ситуация, когда житель штата Калифорния взял

штата Пенсильвания, он должен был бы, по мнению суда, воздержаться от продажи своих сервисов жителям данного штата. В итоге характер контактов ответчика со штатом местонахождения суда был признан достаточным для установления персональной юрисдикции. В качестве аргумента в пользу разумности такого установления суд сослался на наличие серьезного интереса штата Пенсильвания в рассмотрении споров о нарушении товарных знаков, принадлежащих его резидентам.

Статус данного решения стал настолько высоким, что некоторые суды называли его «основным прецедентом в области решения вопроса об установлении персональной юрисдикции на основании функционирования веб-сайта»[1], «переломным моментом в развитии судебной практики»[2].

Подход, сформулированный в деле *Zippo*, является по существу адаптацией прецедента *International Shoe* к новым условиям. В связи с этим он, как и предшественник, отличается значительной гибкостью, которая одновременно является и его слабостью. Как отмечают отдельные комментаторы, данный тест не предлагает правоприменителям каких-либо определенных критериев относительно того, какой уровень интерактивности достаточен для установления юрисдикции, оставляя их один на один с уникальными обстоятельствами каждого конкретного дела[3]. К этому достаточно справедливому замечанию необходимо добавить, что дело *Zippo* было рассмотрено в 1997 г., когда многие сайты в силу неразвитости интернет-технологий были пассивными. В настоящее время подавляющее большинство коммерческих сайтов включают в себя те или иные интерактивные элементы, что лишний раз иллюстрирует факт того, что право часто не успевает за развитием технологий. Пассивных сайтов в том виде, как они описаны в деле *Zippo*, в современной сети Интернет практически не осталось.

с собой в путешествие компьютер и использовал его на территории штата Пенсильвания для получения доступа к сервисам ответчика.

[1] Toys «R» Us, Inc. v. Step Two, S.A., 318 F.3d 446, 452 (3rd Cir. 2003).

[2] Shamsuddin v. Vitamin Research Prods., 346 F. Supp. 2d 804, 809 (D. Md. 2004).

[3] См., например: *Kevin McMunigal*. Desert, Utility and Minimum Contracts: Toward a Mixed Theory of Personal Jurisdiction // Yale Law Journal. No 108. 1998. P. 189; *Daniel Steurer*. The Shoe Fits and the Lighter is Out of Gas: The Continuing Utility of International Shoe and the Misuse and Ineffectiveness of Zippo // Colorado Law Review. No 74. 2003. P. 319–325. Например, в деле Ty Inc. v. Clark (N.D. Ill. 2000) суд, рассматривая вопрос о возможности установления персональной юрисдикции в отношении ответчика из Великобритании, признал веб-сайт умеренно интерактивным (допускался обмен сообщениями по *e-mail*, но без возможности размещения заказа на самом сайте, пользователю могла быть отправлена форма заказа для распечатывания и последующего направления ответчику по обычной почте). Однако такая интерактивность, по мнению суда, являлась недостаточной для установления юрисдикции.

Также не следует забывать, что дело *Zippo* касалось лишь спора о нарушении прав на товарный знак. Но перспектива найти универсальное решение вопроса о юрисдикции в сети Интернет настолько заманчива, что данный тест начал рассматриваться многими американскими судами и учеными в качестве *универсального* решения вопросов юрисдикции в сети Интернет[1]. В то же время он, например, плохо подходит для рассмотрения споров о защите чести, достоинства и деловой репутации, ведь соответствующая информация может быть размещена и на чисто пассивном сайте, что по идее должно влечь отказ в установлении юрисдикции по местонахождению потерпевшего, несмотря на то, что можно говорить о том, что негативные последствия размещения информации наступили на территории его проживания[2]. Однако этот очевидной факт все равно не мешает судам придерживаться теста *Zippo* в таких случаях. Например, в ситуации, когда на веб-сайте компании, расположенной в Гонконге, были размещены сведения, порочащие деловую репутацию одного из ее бывших директоров, проживающего в штате Иллинойс, суд данного штата пришел к выводу о недостаточности оснований для своей юрисдикции в отношении гонконгской компании. Одним из аргументов как раз был пассивный характер такого сайта (тест *Zippo*)[3].

Также необходимо отметить, что *Zippo*-тест относится исключительно к вопросам установления специальной юрисдикции. Сама по себе степень интерактивности сайта не имеет значения для решения вопроса об установления общей юрисдикции[4]. Как отмечалось ранее, для этого необходимо, чтобы контакты носили продолжительный, систематический и существенный характер, что отнюдь не эквива-

---

[1] *Yokoyama D.* You Can't Always Use the Zippo Code: The Fallacy of a Uniform Theory of Internet Personal Jurisdiction // DePaul Law Review. No 54. 2004–2005. P. 1167–1168.

[2] Как отмечается в литературе, в таких случаях в соответствии с установившейся Верховным судом США практикой (Calder v. Jones, 465 U.S. 783, 1984; Keeton v. Hustler, 465 U.S. 770, 1984) должен применяться *effects test*, в соответствии с которым юрисдикция может быть установлена в отношении нерезидента в случае совершения им умышленного деяния, причинившего вред истцу на территории, где находится суд. Применение теста *Zippo* для данной категории дел не только не адекватно, но и противоречит упомянутым решениям Верховного суда США. Тем не менее многие суды при рассмотрении споров о диффамации в сети Интернет используют в качестве основания для установления персональной юрисдикции *Zippo* тест, модифицированный требованиями наличия направленности сайта на территорию штата истца (см.: *Borchers P.* Internet Libel: The Consequences of a Non-Rule Approach to Personal Jurisdiction // Northwestern University Law Review).

[3] Edelson v. Ch'ien 352 F. Supp. 2d 861 (N.D. Ill. 2005).

[4] Bell v. Imperial Palace Hotel/Casino, Inc., 200 F. Supp. 2d 1082, 1091 (E.D. Mo. 2001); Molnlycke v. Dumex, 1999 (E.D. Pa. 1999).

лентно степени интерактивности интернет-сайта. Хотя для полноты картины необходимо отметить, что встречаются и решения, где предпринимались попытки использовать тест *Zippo* при решении вопроса об установлении общей юрисдикции[1]. Такие решения подвергаются критике в американской литературе во многом по причине того, что они влекут установление универсальной «всемирной» общей юрисдикции, что однажды уже было признано неприемлемым в деле *Inset*[2].

Неудивительно, что указанные недостатки критериев *Zippo* повлекли дальнейшее уточнение критериев допустимости установления персональной юрисдикции на основании доступности веб-сайта на определенной территории. В качестве такого дополнительного критерия американские суды нередко стали использовать факт направленности деятельности владельца сайта на определенный штат. Как указал один из судов, «персональная юрисдикция не может быть установлена, если только ответчик не совершает чего-то большего, что бы свидетель-ствовало о направленности его действий по отношению к клиентам в штате Западная Вирджиния»[3]. Аналогичные подходы встречаются во многих других решениях[4].

Лучше всего суть нового подхода демонстрирует дело *Toys «R» Us, Inc. v. Step Two, S.A.*[5] Предметом данного спора, как и в деле *Zippo*, было рассмотрение требования, связанного с нарушением товарного знака. В качестве ответчика выступала испанская компания, которая владела более 160 магазинами по продаже детских игрушек под брендом «*Imaginarium*» в 10 странах (кроме США). Указанное обозначение было зарегистрировано ответчиком в качестве товарного знака в данных странах. Истец осуществлял продажи детских игрушек в 175 магазинах в разных штатах США под товарным знаком с аналогичным наименованием, но зарегистрированным в США. Впоследствии истец зарегистрировал доменное имя «*imaginarium.com*», а ответчик –«*imaginarium.es*». Оба ответчика имели высокоинтерактивные сайты, позволяющие делать покупки в онлайн-режиме. По мнению истца, его права на товарный знак были нарушены действиями испанской компании, поскольку ее

[1] Mink v. AAAA Dev. LLC, 190 F.3d 333 (5th Cir. 1999); MJC-A World of Quality, Inc. v. Wishpets Cp., Ltd, No 00 C 6803 (N.D. Ill. Aug. 27, 2001).

[2] *Yokoyama D.* Op. cit. P. 1194.

[3] Williams v. Advertising Sex (N.D. W.Va. 2007).

[4] ALS Scan v. Digital Services Consultants, Inc., 293 F. 3d 707 (4th Cir. 2002); Revell v. Lidov, 317 F.3d 467 (5th Cir. 2002); Neogen Corp. v. Neo Gen Screening, Inc., 282 F.3d 883, 890 (6th Cir. 2002); Jennings v. AC Hydraulic A/S, 383 F.3d 546 (7th Cir. 2004); Fairbrother v. Am. Monument Found., LLC, 340 F. Supp. 2d 1147, 1156 (D. Colo. 2004).

[5] 318 F.3d 446, 451 (3d Cir. 2003).

веб-сайт был доступен на территории США и с помощью него можно делать покупки товаров, схожих с товарами, продаваемыми истцом. Суд обозначил суть спора следующим образом: «достаточно ли факта использования коммерческого интерактивного сайта, доступного на определенной территории, для установления персональной специальной юрисдикции либо необходимы дополнительные доказательства направленности данного сайта на данную территорию». Суд отказался применять *Zippo*-тест прямолинейно, указав, что помимо интерактивности сайта необходимо, чтобы было установлено намеренное взаимодействие с территорией суда. Как установил суд, ответчик не имел магазинов, представительств, агентов на территории США. Сайт ответчика, несмотря на его интерактивность, не поощрял покупку товара американцами, так как был исполнен на испанском языке, цены были выражены в испанских песетах или евро, доставка осуществлялась только по адресам в Испании. В итоге суд пришел к выводу о недостаточности доказательств в пользу наличия взаимодействия, так как дизайн сайта явно не был направлен на осуществление продаж на территории США. Не помогла и контрольная закупка товара с данного сайта, сделанная истцом из Нью-Джерси, в результате которой покупатель получил товар (через промежуточную компанию в Испании) и пароль для получения доступа к Клубу покупателей. Эти контакты были сочтены судом недостаточными для установления юрисдикции.

Таким образом, основным критерием оценки при решении вопросов юрисдикции в соответствии с судебной практикой американских судов последних лет является наличие доказательств направленности деятельности ответчика с использованием веб-сайта на соответствующую территорию. Например, суд установил свою юрисдикцию в отношении японских резидентов на том основании, что японский веб-сайт, распространяющий по подписке контент для взрослых, имел обширную базу пользователей из США[1]. В другом деле факт наличия 240 пользователей на территории штата был признан достаточным для установления юрисдикции в отношении испанской компании, веб-сайт которой позволял загружать музыку в отсутствие соглашений с правообладателями[2].

При определении направленности веб-сайта на территорию определенного штата суд может принимать во внимание следующие фак-

[1] Viz Commc'ns, Inc. v. Redsun No. C-01-04235 JF, 2003 WL 23901766 (N.D. Cal. Mar. 28. 2003).

[2] Arista Records, Inc. v. Sakfield Holding Co., 314 F.Supp.2d 27 (D.D.C. 2004).

торы: 1) размещение файлов *cookie* на компьютеры резидентов штата; 2) количество участников – резидентов штата на форумах такого веб-сайта или в качестве комментаторов к новостным лентам такого сайта; 3) данные о платежах, совершенных посредством банковских карт резидентами штата при оплате товаров и услуг интернет-магазина; 4) размещение гиперссылок на веб-сайтах, деятельность которых направлена на данный штат[1].

Подход *Zippo* был отвергнут и в Принципах определения юрисдикции, применимого права и принудительного исполнения судебных решений в сфере интеллектуальной собственности. Данный документ развивает классические принципы установления юрисдикции в отношении деликтных требований – по месту совершения противоправных действий, по месту наступления последствий, адаптируя их в то же время к современным цифровым реалиям[2]. В соответствии с § 204 (1) иск может быть предъявлен к лицу в суд штата, где была совершена значительная часть действий, повлекших нарушение исключительных прав, либо совершена значительная часть подготовительных действий, повлекших такое нарушение. Причем юрисдикция такого суда распространяется на все нарушения, являющиеся следствием таких действий, безотносительно от того, где они имели место. Таким образом, в соответствии с данными Принципами иск может быть предъявлен 1) по местонахождению веб-сайта, на котором был размещен материал, нарушающий чьи-либо исключительные права, либо 2) по месту нарушения исключительного права, если установлено, что деятельность, которая повлекла нарушение, была направлена на такой штат (§ 204 (2)). При определении вопросов направленности комментарии к Принципам призывают принимать во внимание меры, принятые ответчиком для того, чтобы избежать нежелательной юрисдикции: наличие соответствующих оговорок на сайте; использование технологий географической идентификации с блокированием доступа пользователей с нежелательных юрисдикций; отказ от осуществления доставки в нежелательные страны, использования их языка и валюты; отказ в обработке транзакций, оплаченных банковскими картами из нежелательных юрисдикций; наличие специально выделенных сайтов, зарегистрированных под локальным доменным именем специально для ведения деятельности на определенной территории, и т.д.[3]

---

[1] *Rustad M.* Internet Law in a Nutshell. St. Paul: MN, 2009. P. 72.

[2] Intellectual Property: Principles Governing Jurisdiction, Choice of Law, and Judgments in Transnational Disputes. ALI, 2007. P. 93.

[3] Ibid. P. 95–96.

Принципы также указывают обстоятельства, которые не могут служить единственным и достаточным основанием для установления юрисдикции по трансграничным спорам, связанным с интеллектуальной собственностью. Придание им качества единственного основания для установления персональной юрисдикции в отношении иностранного ответчика может повлечь отказ в принудительном исполнении вынесенного решения[1]. К таким обстоятельствам относится: *a*) факт нахождения имущества на территории государства суда или возникновения права на интеллектуальную собственность в соответствии с его законами, за исключением случаев, когда спор связан с таким имуществом или правами; *b*) национальность истца и ответчика; *c*) осуществление ответчиком определенной деятельности на территории государства суда, не связанной с предъявленным требованием; *d*) вручение повестки на такой территории; *e*) совершение на территории такого государства заключительных формальностей (например, подписание) при заключении договора, в связи с нарушением которого предъявляется требование (§ 207). Указанные положения являются по существу конкретизацией упоминавшегося выше положения *purposeful availment* как одного из условий установления персональной юрисдикции на основании минимальных контактов.

В качестве обобщения можно указать, что в соответствии с американским законодательством иностранное лицо – владелец веб-сайта – может быть все же привлечено в качестве ответчика в суде штата при условии, что такой веб-сайт позволял осуществлять взаимодействие с резидентами такого штата и имели место обстоятельства, позволяющие говорить о направленности деятельности на территорию такого штата. Сам по себе факт осуществления деятельности за пределами США не освобождает иностранное лицо от потенциальной юрисдикции судов США при наличии вышеуказанных обстоятельств. При этом наличия специальных оговорок на сайте (*disclaimers*) о том, что лицо не осуществляет коммерческую деятельность на территории определенного штата, недостаточно для того, чтобы исключить фактор направленности деятельности такого лица на этот штат[2]. Для этого необходимы еще и соответствующие технические решения (использование специальных технологий, позволяющих блокировать запросы от пользователей с определенных территорий; отсутствие возможности

[1] Intellectual Property: Principles Governing Jurisdiction, Choice of Law, and Judgments in Transnational Disputes. ALI. 2007. P. 124.

[2] Euromarket Designs Inc. v. Crate & Barrel Ltd., 96 F. Supp. 2d 824 (N.D. III. May 16. 2000).

совершения платежей резидентами таких штатов; отсутствие доставки товара в указанный штат)[1] либо инкорпорированная в онлайн-договор юрисдикционная оговорка[2].

В завершение необходимо указать на наличие в американском процессуальном праве так называемого правила агрегации (*rule of aggregation*). Согласно правилу 4*k* Федеральных правил гражданского процесса в отсутствие минимальных контактов с территорией определенного штата такие минимальные контакты могут иметь место по отношению к США в целом. В таком случае любой федеральный суд США может установить юрисдикцию в отношении иностранного ответчика. В деле *Quokka Sports Inc. v. Cup International*, *Ltd*[3] данное положение было использовано в отношении ответчика из Новой Зеландии, единственным контактом которого с территорией США был веб-сайт, который инкорпорировал товарный знак истца (*America's Cup*) в свое доменное имя, *americascup.com* и активно конкурировал с истцом посредством данного сайта. Суд признал, что в данном случае сайт был направлен на территорию США в целом, а не на территорию определенного штата и со ссылкой на вышеуказанное правило 4*k* установил свою юрисдикцию в отношении ответчика. Таким образом, данное правило открывает дополнительные возможности по установлению юрисдикции американских судов в отношении иностранных лиц, которые нарушают интеллектуальную собственность американских компаний, осуществляющих свою деятельность в масштабе всех США.

2.3. Определение применимого права к отношениям в сети Интернет (jurisdiction to prescribe)

Квалификация характера спора и определение применимой коллизионной привязки осуществляются в соответствии с коллизионными нормами штата, где рассматривается спор (*lex fori*)[4]. Разумеется, в данной работе не представляется возможным осветить подходы в выбору применимого права, существующие во всех штатах США. Однако определенное представление о данном вопросе можно получить из таких источников, как ЕТК и *Restatement 2nd on Conflict of Laws* (Второй свод норм коллизионного права)[5].

---

[1] Toys «R» Us, Inc. v. Step Two, S.A. 318 F.3d 446, 451 (3d Cir. 2003).

[2] *Graham Smith*. Op. cit. P. 682.

[3] (N.D. Cal. 1999).

[4] Klaxon Co. v. Stentor Elec. Mfg. Co., 313 U.S. 487, 496 (1941).

[5] *Smith Gregory*. Choice of Law in the United States // The Hastings Law Journal. No 38. 1987. P. 1043–1044.

Согласно § 1-105 ЕТК при отсутствии соглашения сторон о выборе применимого права подлежат применению нормы ЕТК в том виде, в каком они были имплементированы в штате, суд которого рассматривает спор, при условии, что договор имеет надлежащую связь с этим штатом. Иными словами, ЕТК закрепляет привязку *lex fori* (применение закона места рассмотрения спора). Несмотря на то что формально положения ЕТК имеют бóльшую силу по отношению к правилам *Restatement 2nd on Conflict of Laws*, по крайней мере применительно к договорам, прямо урегулированным в ЕТК, на практике суды обычно игнорируют данное положение, обычно обращаясь к коллизионным нормам, принятым в их штатах[1].

Гораздо бóльший интерес в плане коллизионного регулирования представляют собой положения *Restatement 2nd on Conflict of Laws*. Основной принцип выбора применимого права заключается в применении права, имеющего наиболее тесную связь (*substantial relationship*) по отношению к сторонам и обстоятельствам спора. При определении такой тесной связи суды должны учитывать ряд факторов политико-правового характера, в числе которых: *a*) потребности межгосударственных и межштатовых взаимоотношений; *b*) соображения правовой политики штата по месту рассмотрения спора; *c*) интересы других потенциально заинтересованных в рассмотрении спора штатов (государств); *d*) защита обоснованных ожиданий сторон; *e*) основные принципы отрасли права, с которой связан спор; *f*) определенность и предсказуемость результата; *g*) легкость определения и применения выбранного права (§ 6).

Поскольку принцип тесной связи и принципы, лежащие в основе его определения, являются весьма размытыми, имеет смысл детальнее рассмотреть то, как он конкретизируется применительно к отдельным категориям отношений, имеющих значение в контексте сети Интернет, – как договорных, так и деликтных.

Выбор права, применимого к договорным отношениям

В соответствии с § 187 *Restatement 2nd on Conflict of Laws* основным принципом определения применимого права в договорных отношениях является принцип автономии воли, согласно которому стороны вправе самостоятельно выбрать право при условии соблюдения определенных ограничений.

[1] *Асосков А.В.* Коллизионное регулирование договорных обязательств. М., 2012. С. 396.

Таких ограничений два. Во-первых, выбранное право должно быть связано или с какой-либо из сторон, либо с самим договором, либо должно быть иное разумное обоснование для его выбора. Например, контрагенты с местонахождением в США и России по договору, исполняемому в России, не имеют возможности выбрать английское право, если отсутствует какая-либо разумная связь сторон или договора с Англией. Как правило, одного факта местонахождения стороны по договору в определенном штате достаточно, чтобы имела место разумная связь выбранного сторонами права такого штата в качестве применимого[1]. Во-вторых, такой выбор не должен противоречить фундаментальным публичным политикам штата, право которого применялось бы в отсутствие соглашения сторон о выборе права[2]. В частности, такая фундаментальная политика может выражаться в положениях законодательства, направленных на защиту слабой стороны договора от злоупотреблений другой стороны, обладающей превосходящими переговорными возможностями, в частности на защиту прав потребителей.

Если выбранное сторонами право не будет соответствовать указанным ограничениям, то оно может быть проигнорировано[3] и вместо него подлежит применению право штата, которое бы применялось в отсутствие соглашения сторон о выборе применимого права (так называемое объективно применимое право), т.е. право того штата, которое имеет наиболее существенную связь со сделкой и ее сторонами с учетом принципов, указанных в § 6 *Restatement 2nd on Conflict of Laws*. При этом § 188 ориентирует суды на необходимость принятия во внимание таких обстоятельств, как место заключения договора, место проведения переговоров, место исполнения договора, местонахождение предмета договора, местонахождение сторон, в зависимости от значимости каждого из указанных факторов в контексте конкретной ситуации.

Данный подход был принят на вооружение Принципами договорного права в сфере программного обеспечения (*ALI Principles of the Law of Software Contracts*) применительно к сделкам, связанным с предоставлением прав на стандартизированное программное обеспечение, распространяемое в электронной форме. Они предусматривают возможность сторон выбрать право, применимое к их отношениям, при условии, что имеет место разумная связь между такими

[1] Nedlloyd Lines B.V. v. Superior Court, 3 Cal 4th (1992).

[2] § 187 (2) Restatement (Second) on Conflict of Laws.

[3] Правда, оно все же может иметь некоторое значение для толкования договора как выражающее направленность воли сторон.

отношениями и выбранным правопорядком (§ 1.13). Однако, если результат применения выбранного сторонами права вступает в противоречие с публичным порядком штата, право которого применялось бы в отсутствие соглашения о выборе права в соответствии с п. *b*, применяются положения законодательства такого штата. При этом п. *b* предусматривает применение права местонахождения потребителя или, если потребитель не является стороной договора, – право страны лицензиара[1]. Соответствующие правила сформулированы как «жесткие», не предполагающие учета каких-либо иных обстоятельств при определении применимого права. Как отмечается в официальном комментарии к данным принципам, такой подход в наибольшей степени отвечает сложившейся практике и ожиданиям сторон[2].

Необходимость наличия определенной связи между выбранным правом и регулируемым им правоотношением является отличительной чертой американского коллизионного права по сравнению с европейским (в том числе и российским), которое не содержит подобного ограничения. Считается, что данное ограничение было введено для того, чтобы исключить выбор иностранного права в отношении внутренних договоров, не осложненных иностранным элементом, и избежать проблем с разграничением внутренних и трансграничных договоров[3]. В качестве другой причины упоминается также вероятность злоупотреблений сторон, которые путем выбора права третьего государства, никак не связанного с договором, могут обойти фундаментальные политики в сфере договорного права, свойственные всем связанным с договорам правопорядкам[4].

Правила, сходные с положениями § 187 Свода, содержатся также в § 1-105 ЕТК США, имплементированного в виде отдельного закона в большинстве штатов США, согласно которому «если иное не предусмотрено кодексом, стороны вправе в случаях, когда сделка имеет разумную связь как с данным, так и с другим штатом или государством, договориться о том, что их права и обязанности будут определяться

[1] Данное правило во многом представляет собой адаптацию к современным цифровым реалиям положений § 109 *(a) UCITA*, согласно которому применительно к сделкам, связанным с распространением цифрового контента, в отсутствие соглашения сторон об ином применяется право страны, где находится лицензиар. Однако если договор заключен с потребителем и предполагается передача копии произведения на материальном носителе, то применяется право штата, где должна была быть осуществлена такая доставка.

[2] ALI Principles of the Law of Software Contracts. Proposed final draft. 2009. P. 88.

[3] *Scoles E., Hay P., Borchers P. Symeonides S.* Conflict of Laws. 4th ed. St. Paul. MN. 2004. P. 975.

[4] Ibid. P. 976.

по праву либо данного, либо другого штата или государства. При отсутствии такого соглашения настоящий кодекс применяется к сделкам, имеющим надлежащую связь с данным штатом». В 2001 г. в рамках пересмотра ряда положений ETK была предпринята попытка внесения изменений в том числе и в данную статью. В соответствии с положениями § 1-301 ETK, призванного заменить § 1-105 ETK, соглашение сторон сделки с иностранным элементом о выборе права по общему правилу действительно даже в отсутствие разумной связи сделки с соответствующим правопорядком[1], за исключением договоров с участием потребителей. В последнем случае по-прежнему необходимо наличие разумной связи между выбранным правом и правоотношением.

Однако большинство штатов отказались вносить изменения в свои редакции кодекса, отдавая предпочтение устоявшемуся правилу необходимости наличия разумной связи между выбранным правом и правоотношением[2]. В итоге разработчики ETK отказались от новой редакции § 1-301 ETK.

Таким образом, необходимость наличия разумной связи между выбранным правом и правоотношением продолжает составлять одну из наиболее принципиальных особенностей американского коллизионного права[3], хотя в настоящее время роль данного ограничения снижается в связи с тенденцией расширительного толкования американскими судами понятия «разумная связь», которые усматривают ее наличие во всех случаях, когда имеют место хотя бы незначительные контакты с выбранным правом[4].

Отдельные штаты содержат собственное регулирование по вопросам необходимости наличия разумной связи между выбранным правом и правоотношением. Так, например, в соответствии с § 1646.5 Гражданского кодекса штата Калифорния стороны вправе выбрать в качестве применимого право, которое не имеет связи с правоотношением.

---

[1] UCC Article 1, General Provisions (2001) Summary. 2013. The National Conference of Commissioners on Uniform State Laws // http://www.uniformlaws.org/ActSummary.aspx?title=UCC%20Article%201,%20General%20Provisions%20(2001)

[2] 2006 Uniform Commercial Code Survey: Introduction // The Business Lawyer. No 62. August 2007. P. 1555–1558. Единственной территорией, имплементировавшей новую редакцию § 1-301 ETK, были Американские Виргинские острова.

[3] Специалисты в области международного частного права отмечают, что схожее правило содержится лишь в колизионном праве Польши, Макао (административной единицы Китая с особой правовой системой), Анголы и Мозамбика (см.: *Асосков А.В.* Указ. соч. С. 264).

[4] *Rühl G.* Party Autonomy in the Private International Law of Contracts: Transatlantic Convergence and Economic Efficiency // Conflict of Laws in a Globalized World / ed. E. Gottschalk, R. Michaels, G. Rühl, & J. von Hein. Cambridge University Press. 2007. P. 163.

Однако такая свобода допускается лишь в договорах, сумма которых превышает 250 000 долл., и не распространяется на потребительские договоры, трудовые договоры и некоторые иные виды соглашений. Схожие положения содержатся в законодательстве штата Флорида. Таким образом, объем имеющейся у сторон свободы усмотрения в вопросах выбора применимого права зависит от законодательства штата, в котором рассматривается дело.

Рассмотрев общие принципы определения применимого права в сфере договорных отношений, необходимо сказать несколько слов о принципах определения применимого права в спорах, связанных с нарушением прав интеллектуальной собственности.

Специфика данных споров заключается в том, что права на объекты интеллектуальной собственности носят сугубо территориальный характер. Иными словами, такие права существуют в той мере и в том объеме, в которых государство их признает. Содержание, ограничения, действительность, сроки, порядок защиты таких прав определяются по общему правилу в соответствии с законодательством, где произошло их нарушение, безотносительно к тому, где был создан соответствующий объект интеллектуальной собственности[1]. Таким образом, некорректно говорить о том, что существует некое международное право интеллектуальной собственности[2]. Существует авторское право США, авторское право Германии, авторское право России и т.д., каждое из которых применяется к деятельности, связанной с такими правами, на территории соответствующего государства. Объекты интеллектуальной собственности, права на которые возникают в силу регистрации (изобретения, полезные модели, промышленные образцы, товарные знаки, наименования места происхождения товара, топологии интегральных микросхем, селекционные достижения и др.), тесно связаны с государством, где была осуществлена такая регистрация, поскольку такие права были порождены именно его правопорядком.

---

[1] Intellectual Property: Principles Governing Jurisdiction, Choice of Law, and Judgments in Transnational Disputes. ALI. 2007. P. 144. *Ginsburg Jane*. Copyright without borders: Choice of forum and choice of law for copyright infringement in Cyberspace // Cardozo Arts & Entertainment Law Journal. No 15. 1997. P. 154.

[2] Конечно, существует множество международных соглашений, направленных на гармонизацию законодательства об интеллектуальной собственности в определенной сфере (Бернская конвенция, *TRIPS* и т.д.). Однако они не создают самостоятельного международно-правового режима для прав интеллектуальной собственности, существующего в отрыве от национального законодательства. Положения таких международных соглашений применяются лишь в системе координат национального законодательства, будучи имплементированными в него либо в редких случаях применяясь напрямую вместо отдельных его положений.

Так, один из судов[1] отказался применять авторское право США к тем нарушениям исключительных прав, которые произошли за рубежом, даже несмотря на то, что им предшествовали действия, совершенные на территории США. Суд мотивировал это тем, что такой подход нарушал бы принцип территориальности исключительного права и необоснованным образом вторгался бы в сферу суверенной власти иных государств, что несовместимо с принципами международной вежливости[2]. По мнению суда, к нарушениям исключительных прав, совершенным за пределами США, должно применяться право страны, где такое нарушение имело место быть.

Иного мнения придерживался суд при рассмотрении спора, связанного с нарушением авторских прав российского информационного агентства «ИТАР-ТАСС», издательством журнала, выходящего и распространявшегося в Нью-Йорке. Как было установлено, издательство журнала использовало около 500 статей без согласия правообладателя. Специфика данного дела заключается в том, что суд отошел от формального применения *lex fori* и указал, что в качестве права, применимого для решения вопроса об авторстве на произведение, должно применяться право страны, где оно было создано, как наиболее тесно связанное с отношением (в данном случае это было российское право). Что же касается права, применимого к факту нарушения авторского права, суд использовал коллизионную привязку из сферы деликтного права – *lex loci delicti*. Соответственно квалификация действия в качестве нарушения авторского права, а также доступные способы защиты должны определяться в соответствии с Законом об авторском праве США, поскольку вредоносные последствия наступили на территории США.

В целом проблематика определения применимого права к трансграничным спорам, связанным с нарушением исключительных прав, является малоразработанной в судебной практике и доктрине США. Как отметил суд по делу *ITAR-TASS*, «опубликованные судебные решения преимущественно обходят стороной вопросы, связанные с выбором права в международных спорах в сфере авторского права, а комментаторы упоминают их лишь поверхностно»[3]. Отсутствие детальной проработки проблематики выбора права в трансграничных спорах в сфере интеллектуальной собственности во многом обусловлено тем

[1] Subafilms, Ltd v. MGM-Path, Commc'n Co., 24 F.3d 1088, 1095 (9th Cir. 1994).

[2] В американской литературе данное решение критикуется по ряду параметров, в числе которых необоснованное смешивание судом вопросов юрисдикции и применимого права (см.: *Frohlich A.* Copyright infringement in the Internet age: A primetime for harmonized conflict-of-laws rules // Berkeley Technology Law Journal. No 24. 2009. P. 256–261).

[3] ITAR-TASS Russian News Agency v. Russian Kurier, Inc., 153 F.3d 82, 88 (2nd Cir. 1998).

фактом, что американские суды не любят рассматривать требования, связанные с нарушением исключительных прав за рубежом, если это сопряжено с применением иностранного права[1].

Определение применимого права в спорах, связанных с защитой чести, достоинства и деловой репутации

В соответствии с § 149 *Restatement 2nd on Conflict of Laws* в качестве права, применимого к такого рода спорам, применяется право штата, в котором имела место публикация материала, за исключением случаев, указанных в § 150, и ситуаций, когда из обстоятельств конкретного дела следует следствие применений принципов § 6, что правоотношение наиболее тесно связано с территорией иного штата (в последнем случае применяется право такого штата). Наибольший интерес в контексте диффамации в сети Интернет имеет § 150, который посвящен определению применимого права в случаях, когда публикация имела место в средствах массовой информации на территории нескольких штатов. В таких случаях, если в качестве потерпевшего выступает физическое лицо, то правом, наиболее тесно связанным с отношением, признается право штата, где он проживает. Если потерпевшим является юридическое лицо, то таким правом будет право штата, где такое лицо осуществляет свою основную деятельность при условии, что публикация имело место и в таком штате. Как видно из данных презумпций, в качестве применимого права в таких случаях выступает право штата, где, как предполагается, репутация потерпевшего сильно пострадала. Данное правило направлено на защиту интересов не только потерпевшего, но и причинителя вреда, освобождая его от ответственности, определяемой по правилам множества различных штатов, где публикация имела место (так называемое правило единой публикации – *single publication rule*).

Существующие прецеденты, связанные с диффамацией в сети Интернет, позволяют сделать вывод, что суды обычно следуют вышеуказанным правилам и применяют право по местонахождению (домицилю) истца[2]. Таким образом, если американский суд найдет основания для установления юрисдикции в отношении ответчика –

[1] См., например: Creative Technology, Ltd. v. Aztech System, Ltd, 61 F.3d 696, 704 (9th Cir. 1995). В данном решении суд признал Сингапур более подходящим местом для рассмотрения спора; Murray v. British Broadcasting Corp., 81 F.3d 287 (1996) (по мнению американского суда, Великобритания была признана более адекватным местом рассмотрения спора); *Dinwoodie G.* International intellectual property legislation: A Vehicle for Resurgent Comparativist Thought // American Journal of Comparative Law. No 49. 2001. P. 440.

[2] Wells v. Liddy 186 F.3d 505 (4th Cir. 1999); Hitchcock v. Woodside Literary Agency 15 F. Supp. 2d 246 (E.D.N.Y. 1998).

иностранного владельца интернет-ресурса, для чего, как отмечалось ранее, требуется наличие определенной направленности такого ресурса на территорию США, в качестве применимого права будет выступать право истца (т.е. право соответствующего штата США), что обусловит целесообразность обращения к услугам местных юридических фирм для представительства интересов ответчика в суде.

2.4. Принудительное исполнение судебного решения в США (jurisdiction to enforce)

После того как суд решит вопрос о допустимости установления своей юрисдикции в отношении ответчика, определит применимое право и рассмотрит дело по существу, он выносит решение по существу спора. В случае если такое решение не может быть исполнено на территории государства, где был рассмотрен спор (например, ответчик проживает на территории другого штата (государства) и у него нет какого-либо имущества на территории данного штата (государства) для обращения взыскания по решению о наложении взыскания), принудительное исполнение вынесенного решения будет осуществляться судом иного штата или государства.

В случае если решение подлежит исполнению на территории другого штата, то проблем не возникает. Конституция США содержит положение, согласно которому все штаты США должны проявлять доверие и уважение к официальным актам и судебным документам любого другого штата (*The Full Faith and Credit Clause, раздел 1, ст. IV)*.

Существенные сложности возникают в случаях, когда принудительное исполнение судебного решения, вынесенного в США, должно осуществляться в иностранном государстве. В силу того, что юрисдикция судебных органов государства носит сугубо территориальный характер, исполнение решения на территории иностранного государства возможно лишь при наличии согласия такого государства с тем, что иностранный судебный акт способен породить последствия на его территории. По общему правилу такое согласие возможно лишь в случаях, прямо предусмотренных международным договором с таким иностранным государством. В настоящее время США не имеет двусторонних договоров о взаимном признании и принудительном исполнении судебных решений ни с одной страной. В свое время предпринимались попытки заключить такое соглашение с Великобританией, однако они не увенчались успехом[1].

[1] Обзор разработанного текста соглашения см.: *Mary Ann Alford*. The effect of the proposed U.S. – U.K. reciprocal recognition and enforcement of civil judgments treaty on current recognition practice in United States // Columbia Journal of Transnational Law. No 18. 1979.

При отсутствии международного договора решение о принудительном исполнении судебного решения, вынесенного судом США, будет определяться в соответствии с процессуальным законодательством страны, где оно подлежит исполнению. В большинстве случаев оно будет определяться принципами взаимности (*reciprocity*) и международной вежливости (*comity*).

В том случае, когда суд иностранного государства сочтет возможным рассмотреть по существу возможность принудительного исполнения судебного решения, обычно проверке подвергаются следующие обстоятельства: 1) обладал ли суд юрисдикцией по рассмотрению такого спора; 2) была ли обеспечена надлежащая процедура рассмотрения спора; 3) непротиворечие такого решения публичному порядку. Так, например, решения американских судов о взыскании штрафных убытков (убытков, которые взыскиваются наряду с компенсационными убытками и носят карательный характер за совершение умышленных недобросовестных действий – *punitive damages*) не были принудительно исполнены на территории Германии[1], Швейцарии[2].

Условия и пределы допустимости признания и принудительного исполнения иностранных судебных решений на территории США определяются в соответствии с законодательством соответствующего штата. Федеральные суды также применяют по общему правилу положения законодательства того штата, где они расположены[3]. Федеральное законодательство может быть применено в виде исключения и в случаях, когда применение законодательства штата может повлечь осложнение международных отношений.

Общие условия исполнения иностранных судебных решений обозначены в § 98 *Restatement 2nd on Conflict of Laws*. Данный параграф предусматривает общее правило о допустимости признания и принудительного исполнения действительных решений иностранных судов, вынесенных в пределах их компетенции в рамках справедливого состязательного процесса.

Данное правило основано на прецеденте *Hilton v. Guyot*[4], в котором стоял вопрос о признании и исполнении на территории США решения

[1] Entscheidungen des Bundesgerichtshofs (Zivilsachen) BGHZ 118, 312 (1993); *Nettesheim & Stahl*. Recent Development, Bundesgerichtshof Rejects Enforcement of United States Punitive Damages Award // 28 Texas Intellectual Law Journal. No 415 (1993).

[2] *Bernet M*. Recognition and enforcement in Switzerland of US judgments containing an award of punitive damages // International Business Lawyer. No 22. 1994. P. 272.

[3] Erie Railroad Co. v. Tompkins, 304 U.S. 64 (1938); Restatement 3rd Foreign Relations Law. § 481a (1987).

[4] 150 U.S. 113, 202 (1895).

французского суда. Согласно позиции Верховного суда США американский суд не признает иностранного судебного решения, пока не будет убежден в наличии у иностранного суда юрисдикции по рассмотрению такого спора[1] и не будет убежден в том, что «при рассмотрении дела судом была обеспечена справедливая процедура рассмотрения спора с надлежащим извещением ответчика и в рамках правовой системы, обеспечивающей беспристрастное рассмотрение спора с участием иностранных лиц при отсутствии оснований полагать о наличии какого-либо предубеждения или обмана в процессе отправления правосудия». Таким образом, если судебное решение было вынесено судом, действующим в рамках правовой системы, не обеспечивающей надлежащей судебной процедуры (*Due Process*) в ее американском понимании, то в признании и принудительном исполнении такого судебного решения может быть отказано[2]. Сам по себе факт допущения ошибки в применении закона или толковании факта не является основанием для отказа в признании иностранного судебного решения при условии соответствия его вышеуказанным критериям. Равно как в качестве основания для отказа не может использоваться ссылка на различия между законодательством иностранного государства и законодательством штата, где исполняется решение. Как отметил судья Кардозо, «американские суды не настолько провинциальны, чтобы утверждать, что предложенное решение проблемы неверно, так как мы у себя такие дела решаем иначе»[3].

Дело *Hilton v. Guyot* знаменито также и тем, что в нем впервые был установлен принцип международной вежливости (*comity*) как основание для признания и приведения в исполнение решений иностранных судов на территории США. Однако было отмечено, что американский суд не обязан проявлять такую вежливость в тех случаях, когда иностранное государство сохраняет за собой право пересмотра решения суда США по существу (что имело место во Франции). Правда, принцип взаимности понимался ограничительно и был направлен на защиту американских граждан от исков, предъявленных к ним за рубежом. В связи с чем данный принцип не мог применяться в спорах между двумя иностранцами либо против стороны – гражданина США. Впоследствии, впрочем, США отошли от применения принципа взаимности в качестве условия для признания и исполнения иностранных судебных

[1] При этом американский суд может проанализировать обоснованность установления юрисдикции над ответчиком в соответствии с доктриной «минимальных контактов» (см.: Koster v. Automark Industries, Inc., 640 F.2d 77 (7th Cir. 1981)).

[2] Int'l Transactions, Ltd. v. Embotelladora Agral Regiomontana, S.A., 347 F.3d 589, 593-97 (5th Cir. 2003).

[3] Loucks v. Std. Oil Co. 120 N.E. 198, 201 (N.Y. Ct. App. 1918).

решений по причине его несправедливости по отношению к участнику процесса (он расплачивается не за свое поведение, а за поведение властей своего государства), а также возможных помех для признания судебных решений США за рубежом[1].

В большинстве своем сложившиеся в судебной практике подходы нашли свое отражение в Единообразном законе о признании иностранных решений о присуждении денежных сумм 1962 г. (*Uniform Foreign Money-Judgements Recognition Act*), который был принят в той или иной форме приблизительно в половине штатов США[2]. Иностранные судебные решения, вступившие в законную силу, по общему правилу признаются и исполняются в США, за исключением следующих случаев, указанных в ст. 4: 1) такое судебное решение было вынесено судом в рамках правовой системы, не обеспечивающей беспристрастное рассмотрение спора с участием иностранных лиц; 2) иностранный суд не имел юрискдиции в отношении ответчика или предмета спора; 3) отсутствовало надлежащее уведомление ответчика об инициированном процессе; 4) заявленное требование противоречит публичному порядку штата; 5) такое судебное решение противоречит другому вступившему в законную силу судебному решению; 6) разбирательство в иностранном суде противоречило согласованному в договоре порядку судебного разбирательства. В отсутствие таких обстоятельств иностранное судебное решение пользуется полным доверием и уважением (*full credit and faith*) подобно решениям соседних штатов. В качестве примера применения данного Закона можно привести дело, в котором судом Калифорнии было принудительно исполнено решение китайского суда о взыскании с американской компании 6,5 млн долл.[3]

В некоторых случаях иностранное судебное решение может противоречить публичному порядку США. Так, в контексте споров в сети Интернет со ссылкой на публичный порядок может быть отказано в признании иностранных судебных решений, которые противоречат закрепленной в I поправке к Конституции США свободе слова[4].

---

[1] *Danford B.* The Enforcement of Foreign Money Judgments in the United States and Europe: How Can We Achieve a Comprehensive Treaty? // The Review of Litigation. Vol. 23:2. 2004. P. 387.

[2] В остальных штатах суды руководствуются положениями Третьего свода законов об иностранных отношениях (Restatement Third of Foreign Relations Law), § 481 (1) содержит в большинстве своем схожие положения с текстом рассматриваемого Единообразного закона (см.: *Danford B.* Op. cit. P. 388).

[3] Hubei Gezhouba Sanlian Undustrial Co Ltd. & Hubei Pinghu Cruise Co Ltd v. Robinson Helicopter Company Inc., 2:06-cv-01798-FMC-SSx, 22 July 2009.

[4] Yahoo!, Inc. v. La Ligue Contre Le Racisme et L'Antisemitisme 145 F. Supp. 2d 1168 (N.D. Cal. 2001).

В связи с этим в США в 2010 г. был принят отдельный Закон о защите конституционного наследия США[1], согласно которому иностранное судебное решение не подлежит признанию и принудительному исполнению на территории США, если оно было вынесено в странах, где не обеспечивается уровень защиты свободы слова, сопоставимого или более высокого, нежели в США[2]. Ранее подобные законы были приняты в отдельных штатах США (Нью-Йорк, Калифорния, Флорида, Иллинойс и некоторых других).

Как показывает судебная практика, сопоставимость уровня защиты свободы слова определяется наличием или отсутствием в странах, где было вынесено решение, норм, аналогичных тем, которые имеют место в США по вопросам свободы слова. Так, отсутствие в иностранном праве норм, аналогичных тем, которые содержатся в *US Communications Decency Act* 1996 г., может выступить основанием для отказа при признании иностранного судебного решения по вопросу ответственности за распространяемый в сети Интернет контент[3]. Указанный Закон знаменит наличием положения о «добром самаритянине» (*section 230*), согласно которому ни интернет-провайдер, ни пользователь онлайн-сервиса не будут квалифицироваться в качестве публикатора или распространителя сведений, которые были получены от другого контент-провайдера. Данное положение направлено на защиту интернет-провайдеров от ответственности за правонарушения, совершенные иными лицами при использовании их сервисов[4].

В качестве некоторого обобщения существующего в США режима признания и исполнения иностранных судебных решений можно указать следующие его *недостатки*:

1) отсутствие единообразия, обусловленное тем, что данный вопрос во многом регулируется законодательством штатов, в то время как документы, направленные на обеспечение единообразия, носят рекомендательный характер;

2) вышеуказанное отсутствие единообразного подхода существенно затрудняет положение американских истцов, ходатайствующих о признании решения суда США за рубежом, по причине сложности

[1] Securing the Protection of our Enduring and Established Constitutional Heritage (SPEECH) Act, 2010. Pub.L. 111–223.

[2] New York Civil Practice Act § 302 (*d*). Press Release, New York State, Governor Patterson Signs Legislation Protecting New Yorkers Against Infringement of First Amendment Rights by Foreign Libel Judgments (May 1. 2008) // http://www.state.ny.us/governor/press/press 0501082.html

[3] InvestorsHub.com v. Mina Mar Group (N.D. Fla. 2011).

[4] См. подробнее § 4 гл. 5 настоящей книги.

доказывания факта взаимности, что является обычно необходимым условием для такого признания. Иностранные суды смотрят на США и видят 51 правовой режим признания и исполнения иностранных судебных решений[1];

3) наличие у США своих представлений о том, что такое справедливый суд или необходимый уровень обеспечения свободы слова, может приводить к политизации процесса исполнения иностранного судебного решения.

Сложности, связанные с признанием и принудительным исполнением решений, вынесенных судами США в иностранных государствах и наоборот, усиленные потребностями оборота, обусловили заинтересованность США в разработке международного договора, который обеспечивал бы взаимное признание судебных решений судами стран, выступающих основными торговыми партнерами США. Данные усилия завершились разработкой и принятием 30 июня 2005 г. Гаагской конвенции в отношении соглашений о выборе суда (*Hague Convention on Choice of Court Agreements*). Данная Конвенция будет подробнее рассмотрена далее.

§ 3. Юрисдикция в сети Интернет по законодательству Европейского союза

Особенностью законодательства стран Европейского союза по вопросам юрисдикции в сети Интернет является его двухуровневый характер. Помимо национального законодательства отдельно взятой страны существуют также нормы наднационального общеевропейского права, которые представлены в виде документов двух видов: регламентов и директив. Регламент представляет собой нормативный акт, который имеет общее действие, является обязательным в полном объеме и подлежит прямому применению во всех государствах-членах. Регламент представляет собой инструмент унификации национального права стран – участниц Европейского союза по отдельным вопросам.

Директива имеет обязательную силу для каждого государства-члена, кому она адресована (в подавляющем большинстве случаев директивы адресуются сразу всем государствам-членам), в отношении результата, которого требуется достичь. При этом за национальными инстанциями сохраняется компетенция в отношении формы и способов достиже-

[1] *Matthew H. Adler.* If We Build It, Will They Come? The Need for a Multilateral Convention on the Recognition and Enforcement of Civil Monetary Judgments // Law and Policy in International Business. 1994. No 26. P. 96.

ния результата, предписанного директивой. Директива ЕС служит инструментом гармонизации национального права государств-членов (т.е. установления общих рамок правового регулирования в определенной сфере общественных отношений, но без введения полного единообразия).

Если сравнивать директиву с регламентом-законом, то ее можно уподобить основам законодательства, которые действуют не напрямую, а нуждаются в трансформации во внутреннее право государств-членов. Трансформация директивы представляет собой приведение государствами-членами своего законодательства в соответствие с ее нормами путем принятия, изменения или отмены национальных законов и подзаконных актов[1].

3.1. Основные источники регулирования вопросов юрисдикции в Европейском союзе

1. *Регламент ЕС № 44/2001 от 22 декабря 2000 г.* «О юрисдикции, признании и исполнении судебных решений по гражданским и торговым делам» (Брюссель I)[2]. Данный документ определяет порядок взаимодействия судов по гражданским и торговым делам в рамках Европейского союза. Указанный Регламент вступил в силу с 1 марта 2002 г. и заменил собой Брюссельскую конвенцию о юрисдикции и исполнении судебных решений по гражданским и торговым делам от 27 сентября 1968 г. (далее – Брюссельская конвенция), которая была заключена между странами – членами ЕС и в силу ст. 1 также подлежала применению к гражданским и торговым делам.

Несмотря на то что Регламент функционирует в целом успешно, многочисленные исследования и обсуждения выявили необходимость внесения некоторых изменений, в результате которых была принята новая версия Регламента[3]. Основные изменения заключаются в упразднении экзекватуры (промежуточного судебного решения о признании и принудительном исполнении иностранного судебного решения), за исключением некоторых категорий споров (в частности, диффа-

[1] См. подробнее: *Кашкин С.Ю., Четвериков А.О.* Европейский союз: Основополагающие акты в редакции Лиссабонского договора с комментариями // СПС «КонсультантПлюс». 2007.

[2] Council Regulation (EC). No 44/2001 of 22 December 2000 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters // Official Journal of the European Communities. L12/1. 16.1.2001.

[3] Council Regulation (EC) No 1215/2012 of 12 December 2012 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters // Official Journal of the European Communities. L 351/1. 20.12.2012.

мации); расширении сферы действия Регламента в отношении иностранных лиц, не домицилированных в ЕС; гармонизации положений, регламентирующих соглашения о подсудности с положениями Гаагской конвенции в отношении соглашений о выборе суда 2005 г.[1] Подавляющее большинство положений нового Регламента ЕС № 1215/2012 начнет применяться с 10 января 2015 г.

2. Луганская конвенция 2007 г.[2] Данная Конвенция вступила в силу с 1 января 2010 г. и пришла на смену Луганской конвенции 1988 г., которая во многом была аналогична по содержанию Брюссельской Конвенции, в силу чего они официально называются параллельными конвенциями[3]. Смысл ее заключения состоял в том, чтобы распространить принципы определения юрисдикции и признания иностранных судебных решений, принятые в Европейском союзе, на те страны, которые формально не являются членами Европейского союза, но являются членами Европейской ассоциации свободной торговли (*EFTA*): Швейцарию, Норвегию и Исландию. В Конвенции также участвует Дания, которая хотя и является членом ЕС, но в силу определенных политических причин не подпадает под действие регламентов № 44/2001 и 1215/2012. Луганская конвенция открыта для присоединения других государств при условии наличия единогласного согласия всех ее участников.

3. *Регламент ЕС № 593/2008 от 17 июня 2008* «О праве, применимом к договорным отношениям» (Рим I)[4]. Данный документ пришел на смену подписанной 19 июня 1980 г. Римской конвенция о праве, применимом к договорным обязательствам. В 2003 г. Европейской комиссией было предложено не только изменить статус соответствующего акта с международного договора на регламент ЕС, но и дополнить его с учетом накопившейся практики применения Римской конвенции и последних достижений доктрины международного частного права. Данный Регламент затрагивает вопросы определения договорного статута в странах Европейского союза: пределы автономии воли в вопросе выбора применимого права, а также порядок определения применимого права в отсутствие соглашения сторон.

---

[1] Proposal for a Regulation of the European Parliament and of the Council on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters (Recast) – Explanatory memorandum. Brussels. 14.12.2010. COM (2010) 748 Final.

[2] Council Decision 2007/712/EC of 15 October 2007 // Official Journal of the European Communities. L 339. 21.12.2007.

[3] См.: section 6 Preamble to Council Regulation (EC). No 1215/2012 of 12 December 2012.

[4] Regulation EC No 593/2008 of 17 June 2008 «On the Law Applicable to Contractual Obligations» (Rome I) // Official Journal of the European Communities. L 177/6. 04.07.2008.

4. *Регламент ЕС № 864/2007 от 11 июля 2007* «О праве, применимом к внедоговорным обязательствам» (Рим II)[1]. На разработку документа ушло более 30 лет – вопрос об унификации коллизионных норм по внедоговорным обязательствам был поставлен еще в период работы над проектом Римской конвенции[2]. Регламент посвящен вопросам определения права, применимого к деликтам, обязательствам вследствие неосновательного обогащения, ведения чужих дел без поручения и преддоговорной ответственности. Для сферы электронной коммерции данный документ представляет интерес в части вопросов определения применимого права к требованиям, связанным с нарушением прав интеллектуальной собственности и причинением вреда чести, достоинству и деловой репутации.

3.2. Условия установления персональной юрисдикции в отношении иностранного лица (jurisdiction to adjudicate)

Общий принцип установления юрисдикции, закрепленный в Регламенте Брюссель I, состоит в том, что иск может быть предъявлен в суд по месту домициля ответчика.

Домициль ответчика – физического лица определяется в соответствии с национальным законодательством (ст. 59 Регламента Брюссель I), а домициль ответчика – юридического лица определяется самим Регламентом: местом учреждения компании, местом нахождения ее центральных органов либо местом нахождения основного коммерческого предприятия (ст. 60 Регламента Брюссель I). Таким образом, у юридического лица может быть несколько домицилей, каждый из которых будет являться основанием для установления юрисдикции суда по его местонахождению. Главное, чтобы хотя бы один из них находился на территории государства – члена ЕС.

Данные положения имеют приоритет над национальным законодательством в случае, *если ответчиком является лицо, домицилированное в государстве – члене ЕС*. Таким образом, например, правила английского права о допустимости установления юрисдикции английским судом в случае вручения ответчику повестки на территории Англии либо в случае наличия имущества на территории Англии не применяются

[1] Regulation EC No 864/2007 of 11 July 2007 «On the Law Applicable to Non-Contractual Obligations» (Rome II) // Official Journal of the European Communities. L 199. 31.07.2007.

[2] *Kramer X.* The Rome II Regulation on the Law Applicable to Non-Contractual Obligations: The European Private International Law Tradition Continued – Introductory Observations, Scope, System, and General Rules (October 15, 2008). Nederlands Internationaal Privaatrecht (NIPR). No 4. P. 414–424, 2008 // http://ssrn.com/abstract=1314749

в случаях, когда ответчик домицилирован во Франции и отсутствуют иные основания, указанные в Регламенте, для предъявления к нему иска в Англии[1]. Если же ответчик не имеет домициля в государстве – члене ЕС (например, российская компания), то для определения допустимости установления юрисдикции в отношении него применяется национальное процессуальное законодательство.

Суд по месту домициля ответчика обладает *общей юрисдикцией* в отношении него и компетентен рассматривать любые споры, в том числе и не связанные непосредственно с территорией, где рассматривается спор.

Регламент предусматривает закрытый перечень случаев, когда иск может быть предъявлен в иной, нежели по месту домициля ответчика, суд, с установлением тем самым специальной юрисдикции в отношении такого ответчика. Такие случаи относятся как к договорным, так и к деликтным обязательствам.

Применительно к договорным обязательствам таким исключением является возможность предъявления иска в суд по месту исполнения такого обязательства (ст. 5 Регламента Брюссель I). В договорах купли-продажи таким местом обычно считается место, куда товары были доставлены или должны были быть доставлены (ст. 5 (1) (*a*) Регламента Брюссель I); в договорах оказания услуг – место, где услуга была оказана или должна была быть оказана (ст. 5 (1) (*b*) Регламента Брюссель I). Например, если организация, расположенная во Франции, приобретет посредством сети Интернет какой-либо товар у компании, учрежденной на Кипре, с доставкой во Францию, то она имеет возможность предъявить иск как в суды Кипра, так и в суды Франции.

В договорах, связанных с распространением цифрового контента, неизбежно возникает вопрос о том, как определить место исполнения договора, поскольку в нем не предполагается физическая доставка товара или оказание услуги. Учитывая исключительно нематериальный характер такого договора, можно предположить, что он более близок к договору оказания услуг, нежели к классическому договору купли-продажи. Квалификация предоставления цифрового контента в качестве услуги характерна для европейского налогового законодательства[2]. Однако согласно позиции Европейского суда договор, по которому

[1] *Goode R.* Commercial Law. 3rd Ed. London. P. 1079.

[2] EC Commission, E-Commerce and Indirect Taxation (COM(98). 374. 17.06.1998). P. 5. Guideline 2; Organisation for Economic Cooperation and Development (OECD), Electronic Commerce: A Discussion Paper on Taxation Issues, 17.09.1998, available at http://www.oecd.org//daf/fa/e_com/discusse.pdf

правообладатель предоставляет другому лицу на возмездной основе право использовать объект интеллектуальной собственности, не является договором оказания услуг, следовательно, ст. 5 (1) (*b*) Регламента Брюссель I не подлежит применению для определения юрисдикции по спорам из таких договоров[1]. В таких случаях применяется общий подход к определению места исполнения обязательства, включающий в себя три шага: квалификацию договорного обязательства; определение применимого права к такому обязательству (в соответствии с Регламентом Рим I); определение места исполнения обязательства в соответствии с применимым правом[2].

Позиция, согласно которой цифровой контент, предоставляемый не на материальном носителе, не является ни товаром, ни услугой, нашла свое отражение в Директиве ЕС № 2011/83/*EU* «О правах потребителей» (п. 19 преамбулы)[3]. В литературе в качестве места исполнения обязательства по предоставлению цифрового контента предлагается считать по местонахождениию получателя[4].

Другим исключением из общего правила об установлении юрисдикции по домицилю ответчика, применимым к договорным отношениям, является заключение соглашения о подсудности (ст. 23 Регламента Брюссель I). Данное соглашение подчиняется нормам Регламента Брюссель I при условии, что: 1) оно заключено между лицами, как минимум одно из которых является домицилированным в государстве – члене ЕС; 2) устанавливает юрисдикцию определенного суда или судов *государства – члена ЕС* по рассмотрению споров, связанных с конкретным правоотношением. Таким образом, если стороны указали, что споры должны рассматриваться в судах Сингапура, такое соглашение не подпадает под действие Регламента Брюссель I. На практике это может означать, что при предъявлении иска, скажем, во французский суд к ответчику, домицилированному во Франции (ст. 2 Регламента Брюссель I), такой суд не будет иметь возможности со ссылкой на ст. 23 Регламента Брюссель I отказать в принятии спора к рассмотрению.

---

[1] Falco Privatstiftung and Thomas Rabitsch v. Gisela Weller-Lindhorst [2009] ECR, C-533/07.

[2] Gie Groupe Concorde and Others [1999] ECR, C-440/97.

[3] Directive 2011/83/EU of October 2011 on consumer rights mending Council Directive 93/13/EEC and Directive 1999/44/EC of the European Parliament and of the Council and repealing Council Directive 85/577/EEC and Directive 97/7/EC of the European Parliament and of the Council // Official Journal of European Union. 22.11.2011. L 304/64.

[4] *Faye Fangei Wang*. Obstacles and Solutions to Internet Jurisdiction: A Comparative Analysis of the EU and US Laws // Journal of International Commercial Law and Technology. No 3. 2008.

Соглашение о подсудности должно быть заключено в виде письменного документа либо в форме, соответствующей установившейся практике взаимоотношений между сторонами или соответствующей международным торговым обычаям. При этом ст. 23 (2) специально оговаривает возможность существования такого соглашения и в электронной форме, если она обеспечивает надежную фиксацию достигнутых договоренностей. С точки зрения практики Европейского суда положения ст. 23 Регламента Брюссель I образуют самодостаточный перечень условий действительности соглашения о подсудности, не предполагающий субсидиарного применения национального законодательства для оценки его валидности[1]. Данный подход разделяется и в литературе[2].

Регламент предусматривает презумпцию исключительной юрисдикции, устанавливаемой на основании соглашений о подсудности, заключенных в порядке ст. 23 Регламента Брюссель I. Исключительность юрисдикции предполагает как невозможность выбранного суда отказать в принятии спора к рассмотрению, если все необходимые формальные критерии соблюдены, так и невозможность иных судов рассматривать такой спор.

Особенностью европейского законодательства в области юрисдикции является наличие правила *lis pendens*, согласно которому из нескольких судов, в каждом из которых было возбуждено дело по рассмотрению идентичного спора и каждый из которых согласно нормам применимого права имеет полномочия на рассмотрение данного спора, приоритет будет иметь суд, в производство которого спор поступил первым по времени (ст. 27). Данное правило направлено на минимизацию параллельных процессов и несовместимых между собой решений.

Таким образом, если в обход существующего соглашения о подсудности иск был подан в иной суд и такой суд не откажет в установлении юрисдикции, обозначенной в соглашении, суд не имеет права рассматривать спор. Подобные недобросовестные действия (иск был предъявлен в итальянский суд вопреки заключенному соглашению о подсудности споров австрийским судам) стали предметом рассмотрения Европейского суда, вследствие чего получили в литературе символическое название «итальянская торпеда». Европейский суд

[1] Case 25/76 Galeries Segoura SPRL v Firma Rahim Bonakdarian [19761 ECR 1851; Case 24/76 Estasis Salotti v RUWA [1976] ECR 1831 [7] cited with approval by the ECJ in Case C-106/95 MSG v Les Gravieres [1977] ECR 911 [15] and Case C-387/98 Coreck Maritime GmbH v Handelsveem [2000] ECR 9337 [13].

[2] *Merrett L.* Article 23 of the Brussels I Regulation: A Comprehensive Code for Jurisdiction Agreements? // International and Comparative Law Quarterly. No 58. 2009.

указал, что запрет на предъявление иска в иной суд, чем указанный в соглашении о подсудности, несовместим с принципом «взаимного доверия», лежащим в основе Брюссельской конвенции[1]. Данный подход подвергся критике в доктрине и на уровне правительств как поощряющий недобросовестное поведение[2]. Одной из целей принятия новой версии Регламента № 1215/2012 от 12 декабря 2012 г. «О юрисдикции, признании и исполнении судебных решений по гражданским и торговым делам» является корректировка правила *lis pendens* применительно к соглашениям о выборе подсудности. По новой редакции Регламента Брюссель I суд, указанный в соглашении о подсудности, будет иметь приоритет в решении вопроса о своей юрисдикции перед другими судами. Любой иной суд, даже если он принял спор к рассмотрению первым, должен будет воздержаться от рассмотрения спора до того момента, как обозначенный в соглашении суд откажет в установлении своей юрисдикции, например, по причине того, что соглашение о подсудности является недействительным (ст. 31 (2) Регламента Брюссель I).

Свобода усмотрения при определении компетентного суда в соглашениях о выборе подсудности значительно ограниченна применительно к договорам, заключенным с потребителями, т.е. лицами, действующими за пределами своей профессии или предпринимательской деятельности[3]. Безотносительно к содержанию такого соглашения потребитель всегда имеет возможность выбора: предъявить иск в суд по своему местонахождению (домицилю) или по местонахождению (домицилю) предпринимателя. Предприниматель такого выбора лишен и имеет возможность предъявления иска к потребителю только по его местонахождению (ст. 16 Регламента Брюссель I). Как видно, юрисдикция в сфере потребительских споров предопределяется преимущественно императивными нормами. Соглашения о подсудности могут лишь предусматривать дополнительные суды, где потребитель вправе предъявить иск.

Как исключение также возможно заключение соглашения о подсудности, в рамках которого спор может быть рассмотрен судом третьей страны, но только при условии, что такое соглашение было заключено уже *после возникновения спора* (ст. 17 Регламента Брюссель I). Таким образом, в Европейском союзе соглашения о подсудности,

[1] Gasser GmbH v MISAT srl (Case C-116/02) [2003] ECR I-14693.

[2] *Savin A.* Op. cit. P. 61.

[3] В соответствии с устоявшейся практикой Европейского суда в качестве потребителя может выступать только физическое лицо. Bertrand v. Ott [1978] ECR C-150/7.

в том числе инкорпорированные в *click-wrap*-соглашения, в которых в качестве компетентных указаны суды третьих стран (не членов ЕС), могут в лучшем случае лишь дополнять существующую у потребителя возможность выбора. Потребитель не может отказаться от своих прав в договорном порядке, даже если право, применимое к такому договору, допускает такой отказ. Если вопреки таким императивным нормам о подсудности все же будет вынесено решение иным судом, то в его принудительном исполнении может быть отказано вследствие противоречия его публичному порядку[1].

Важно отметить, что под действие Регламента подпадают не все потребительские договоры, а лишь договоры, заключенные в процессе осуществления *направленной* предпринимательской или иной профессиональной деятельности на территории государства, где домицилирован потребитель (ст. 15 (1) (*c*) Регламента Брюссель I).

Разумеется, говорить о наличии направленной деятельности можно также и в тех случаях, когда потребителю по электронной почте приходит реклама или иная информация от предпринимателя, которая имеет своей целью побудить потребителя заключить договор[2]. Однако наибольший интерес толкование критерия направленности имеет применительно к деятельности, осуществляемой посредством веб-сайтов, где их владелец не выступает инициатором коммуникаций с потребителем.

В соответствии с разъяснениями Европейской комиссии «критерий направленной деятельности введен для того, чтобы было очевидно, что юрисдикция может быть установлена в случае заключения потребителем договора с использованием интерактивного веб-сайта, доступного на территории страны его проживания. Однако одного только факта того, что потребитель обладал знаниями о товаре или услуге, полученными с пассивного веб-сайта, доступного в месте его проживания, не достаточно для установления защитной юрисдикции»[3]. Таким образом, в отсутствие заключенного на основе такой информации контракта или коммуникаций между потребителем и предпринимателем, осуществленных посредством веб-сайта, говорить о наличии направ-

[1] *Savin A.* Op. cit. P. 62.

[2] *Foss M., Bygrave L.* International Consumer Purchases through the Internet: Jurisdictional Issues pursuant to European Law // International Journal of Law and Information Technology. No 8. 2000. P. 14.

[3] European Commission, Justice and Home Affairs DG, «Statement on Articles 15 and 73» // http://www.europa.eu.int/comm-/justice home/unit/civil/justciv-conseil/justiciv-en.pdf. Данный подход был подтвержден Европейским судом в деле Hotel Alpenhof GesmbH v Oliver Heller (C-144/09), 7 December 2010 (п. 94).

ленной деятельности предпринимателя на территории государства, где потребители имеют доступ к его сайту, по общему правилу нельзя[1]. Возможные критерии направленности деятельности, связанной с использованием веб-сайта, на территорию определенной страны были указаны Европейским судом в решении *Hotel Alpenhoff*[2]:

- потенциально международный характер деятельности (в данном деле – гостиничный бизнес);
- описание маршрута к месту нахождения предпринимателя с территории других стран;
- возможность размещения заказа на ином языке и (или) в иной валюте, нежели принятые в стране учреждения компании предпринимателя;
- указание на сайте телефонов с международными кодами;
- наличие расходов на продвижение сайта, делающее его более заметным для иностранных клиентов;
- использование нейтрального доменного имени (вроде «*.com*», «*.eu*»), а не географического имени, привязанного к стране, где учреждена компания предпринимателя (например, «*.de*»);
- наличие ссылок на положительные отзывы от клиентов из разных стран.

Наличие специальной оговорки на веб-сайте о том, что он не предназначен для ведения коммерческой деятельности с потребителями из других стран (или отдельно взятых стран), вряд ли сможет исключить возможность установления юрисдикции суда по месту жительства потребителя в случае заключения договора с ним. Однако в случае наличия специальных организационных мер в виде предварительной идентификации географического положения потребителя в совокупности с блокированием возможности осуществления заказа из нежелательных юрисдикций таких мер может быть достаточно для вывода об отсутствии целенаправленной деятельности. В случае, когда веб-сайт использует какой-либо язык, на котором говорят в незначительном количестве стран, можно также говорить об отсутствии целенаправленной деятельности в отношении потребителей из стран, где на таком языке не говорят[3].

---

[1] *Gillies L.* Choice-of-Law Rules for Electronic Consumer Contracts: Replacement of the Rome Convention by the Rome I Regulation // Journal of Private International Law. 2007. April. P. 107.

[2] Joined cases: Peter Pammer v Reederei Karl Schlüter GmbH & Co. KG (C-585/08) and Hotel Alpenhof GesmbH v Oliver Heller (C-144/09), 7 December 2010.

[3] Chitty on Contracts. London: Sweet & Maxwell. 30th ed. 2009. § 30-097. P. 2032.

Критерий направленной деятельности предпринимателя как основание для установления юрисдикции судом по месту жительства потребителя пришел на смену старым критериям, изложенным в ст. 13 (3) (*b*) Брюссельской конвенциии предполагающим наличие у потребительского договора или процедуры его заключения дополнительных территориальных связей с правопорядком места жительства потребителя. К ним относились такие обстоятельства, как наличие предшествующего заключению договора специального приглашения или рекламы, сделанных в месте жительства потребителя, при условии, что действия по заключению договора были совершены там же. В современных условиях, когда многие сделки совершаются посредством сети Интернет, применение данных критериев к сделкам в сфере электронной коммерции весьма проблематично. Неясно, может ли информация, размещенная на веб-сайте, доступном в стране проживания потребителя, квалифицироваться в качестве оферты или рекламы; насколько актуальным является требование о совершении действий по заключению договора в стране потребителя, которое в условиях возросшей мобильности потребителей и повсеместного использования ноутбуков и смартфонов приобретает все более и более случайный характер[1]. В связи с этим критерий направленной деятельности позволяет гибко подойти к вопросам юрисдикции в эпоху электронной коммерции.

Общие положения об установлении юрисдикции в сфере деликтных отношений, содержатся в ст. 5 (3) Регламента Брюссель I, согласно которой иск подлежит предъявлению в суд по месту, где произошло или могло произойти вредоносное действие. Причем это может быть как место, где произошло событие, повлекшее вред, так и место, где такой вред наступил[2]. Так, например, в соответствии с устоявшейся практикой Европейского суда иск о возмещении ущерба, причиненного чести, достоинству и деловой репутации, может быть предъявлен по месту распространения публикации (но только в части ущерба, причиненного на данной территории)[3]. В связи с этим представляет интерес дело *eDate Advertising GmbH*[4], которое было связано с нарушением австрийским сайтом личных прав немецкого истца. Суд, толкуя ст. 5 (3) Регламента Брюссель I, указал, что в случае нарушения личных прав истца контентом, размещенным в сети Интернет, истец имеет право предъявить

[1] *Rosner N.* International Jurisdiction in European Union E-Commerce Contracts / Online Contract Formation ed. by S. Kinsella and A. Simpson. 2004. P. 486.

[2] Bier BV v. Mines de Potasse D'Alsace SA [1978] ECR, C-21/76.

[3] Shevill v. Presse Alliance SA [1995] ECR, C-68/93.

[4] eDate Advertising GmbH v Martinez. ECR. 25 October 2011. C-509/09.

иск о возмещении всего причиненного вреда как в суд, где расположен ответчик, так и в суд, где находится центр его интересов. Также истец имеет право предъявить иск в суд каждого государства – члена ЕС, где был доступен данный материал, но только в части вреда, который наступил на территории такого государства. Таким образом, если ответчик признается домицилированным в одном из государств – участников ЕС (иначе Регламент не будет применяться), он может выступать в качестве ответчика по искам о возмещении вреда в любой стране – члене ЕС, где принадлежащий ему сайт был доступен (по крайней мере в части того вреда, который наступил на территории такой страны). Если же ответчик не домицилирован ни в одной из стран ЕС, то основания для установления юрисдикции будут определяться национальным законодательством страны, в которой был предъявлен иск.

Подходы, заложенные в ст. 5 (3) Регламента Брюссель I, могут применяться и в отношении требований, связанных с нарушением исключительных прав, за некоторым изъятием. Так, требования, связанные с регистрацией или действительностью исключительных прав, подлежащих регистрации, относятся к исключительной юрисдикции судов государства, где была осуществлена такая регистрация (ст. 22 (4) Регламента Брюссель I). Но данная статья не касается иных категорий споров в сфере интеллектуальной собственности (помимо тех, которые связаны с регистрацией и действительностью регистрируемого исключительного права). К тому же она *a priori* не касается авторских и смежных прав как не требующих регистрации в принципе. Как отмечается, ст. 5 (3) Регламента вполне может выступать в качестве основания для установления юрисдикции по месту совершения нарушения исключительного права[1].

Так, в соответствии с одним из недавних решений Европейского суда требование правообладателя о защите авторского права, связанное с деятельностью ответчика по распространению контрафактных экземпляров через интернет-магазины, может быть предъявлено в суд по месту нахождения правообладателя. Толкуя положения ст. 5 (3) Регламента, Европейский суд указал, что для установления юрисдикции судом по местонахождению правообладателя достаточно доказать, что вред может быть причинен в стране правообладателя. При этом нет необходимости доказывать ни факт распространения контрафактных экземпляров, ни направленность действий ответчика на потребителей в такой стране. В результате Европейский суд признал обоснованным

[1] *Savin A.* Op. cit. P. 60.

установление юрисдикции французского суда в отношении ответчика с местонахождением в Австрии, записавшего контрафактные диски, распространяемые английскими компаниями через их веб-сайты, которые были доступны во Франции[1].

Не следует забывать о возможности предъявления иска в суд по месту домициля ответчика – нарушителя исключительного права при условии, если домициль ответчика находится в государстве – члене ЕС. Такой суд будет иметь компетенцию в отношении всех фактов нарушений данного права, совершенных ответчиком на территории иных государств, в том числе и не входящих в Европейский союз.

3.3. Определение применимого права к отношениям в сети Интернет (jurisdiction to prescribe)

Основными документами, унифицирующими законодательства стран – участниц ЕС по вопросам определения применимого права к договорным и деликтным отношениям, являются Регламент Рим I[2] (в части договорных обязательств) и Регламент Рим II[3] (в части внедоговорных обязательств).

Регламент Рим I применяется ко всем договорным обязательствам гражданского и коммерческого характера, за исключением возникающих из норм публичного права (налогового, таможенного, административного), семейного права, корпоративного права, оборотных ценных бумаг (векселей, чеков, коносаментов и т.п.), преддоговорным обязательствам и отдельным видам страховых договоров (ст. 2 Регламента Рим I). Для применения положений Регламента Рим I не имеет значение, относится определенное в соответствии с ними применимое право к одному из государств – членов ЕС либо нет.

Основной принцип, на котором основан Регламент Рим I, заключается в свободе выбора сторонами права, применимого к их договорным отношениям. Данное правило конкретизируется диспозитивными нормами на случай отсутствия такого выбора, а также императивными нормами, направленными на защиту прав потребителей.

В соответствии со ст. 3 Регламента Рим I право, применимое к договорным отношениям сторон, может явно следовать из их соглашения либо из обстоятельств дела. Стороны вправе впоследствии изменить

[1] Peter Pinckney v KDG Mediatech AG, ECR. 3 October 2013. C-170/12.

[2] Regulation EC No 593/2008 of 17 June 2008 «On the Law Applicable to Contractual Obligations» (Rome I) // Official Journal of the European Communities. L 177/6. 04.07.2008.

[3] Regulation EC No 864/2007 of 11 July 2007 «On the Law Applicable to Non-Contractual Obligations» (Rome II) // Official Journal of the European Communities. L 199. 31.07.2007.

выбранное право при условии, что такое изменение не приводит к недействительности договора и не нарушает прав третьих лиц. Действительность выбранного сторонами права контролируется положениями ст. 10, 11 и 13 Регламента Рим I.

В случае если стороны прямо не определили в договоре применимое право и наличие такого выбора прямо не следует из обстоятельств дела, суд определяет применимое право, руководствуясь правилами, указанными в ст. 4 Регламента Рим I, которые предусматривают следующий порядок действий.

На первом этапе суд должен определить исполнение, характерное для данного вида договора (*characteristic performance*). Под исполнением, характерным для договора, обычно понимается обязательство, которое «дает договору его имя» и «за которое причитается оплата»[1]. Применительно к наиболее распространенным типам договоров ст. 4 (1) Регламента Рим I содержит перечень презумпций, в которых определено, какое обязательство является характерным для такого договора. Соответственно право государства, где имеет местонахождение сторона, осуществляющая такое исполнение, и будет применимым. Так, для договора купли-продажи характерным является обязательство по передаче вещи в собственность, поэтому применимым будет право страны местонахождения продавца; для договоров оказания услуг характерным является обязательство по оказанию услуги, поэтому применимым будет право страны местонахождения услугодателя и т.д. В тех случаях, когда заключенный договор не подпадает ни под один из указанных в ст. 4 (1) Регламента Рим I типов либо когда договор носит смешанный характер, суд должен сам определить, какое обязательство выражает исполнение, характерное для такого договора, и применить право страны места жительства стороны, осуществляющей исполнение такого обязательства.

На втором этапе суд проверяет, действительно ли выбранное на первом этапе применимое право является наиболее тесно связанным с данной страной. Если из всех обстоятельств дела будет очевидно, что договор явным образом более тесно связан со страной иной, нежели та, которая была определена на первом этапе, то право такой иной страны подлежит применению.

Наконец, если в силу какой-либо причины невозможно определить право на основании теста характерного исполнения (например,

[1] См.: The Report on the convention on the law applicable to contractual obligations by Mario Giuliano, Professor, University of Milan, and Paul Lagarde, Professor, University of Paris. 1980. OJ C-282/01.

в договоре мены равноценных объектов), то подлежит применению право страны, с которой договор наиболее тесно связан (ст. 4 (4) Регламента Рим I).

Регламент Рим I содержит положения, направленные на предотвращение злоупотреблений, связанных с обходом «неудобных» императивных положений определенного правопорядка. Так, если исходя из обстоятельств дела будет установлено, что договор реально связан лишь с одной страной, то выбор сторонами в качестве применимого права другой страны не может предотвратить применение императивных положений права страны, с которой договор связан (ст. 3 (3) Регламента Рим I). Аналогичным образом выбор сторонами в качестве применимого права третьей страны (не члена ЕС) к договору, который реально связан лишь со страной (странами) ЕС, не влияет на применение общеевропейского законодательства (*Community law*) к такому договору (ст. 3 (4) Регламента Рим I). Разумеется, положения применимого права не могут вступать в противоречие со сверхимперативными нормами (ст. 9) и публичным порядком (ст. 21) законодательства места рассмотрения спора.

Особое значение в контексте проблематики юрисдикции и применимого права в сети Интернет имеют императивные правила ст. 6 Регламента Рим I, направленные на защиту прав потребителей. Основной их целью является защита потребителя как заведомо более слабой стороны от одностороннего навязывания предпринимателем в разработанных им стандартных условиях договора заведомо более выгодного ему права. Под потребителем в контексте Регламента Рим I понимается физическое лицо[1], заключающее договор для целей, не связанных с его профессиональной или предпринимательской деятельностью. Нетрудно заметить, что определение потребителя в Регламенте Рим I идентично тому, которое приведено в Регламенте Брюссель I, что в значительной степени предопределено единством политики, направленной на защиту потребителей и осуществляемой в Европейском союзе. Для применения защитных положений Регламента Рим I необходимо, чтобы в качестве контрагента потребителя выступал предприниматель-профессионал, заключающий договор в рамках

[1] В Европе общепринятым является мнение, согласно которому защитные механизмы потребительского законодательства, реализованные в регламентах Брюссель I и Рим I, не должны распространяться на малый и средний бизнес (см.: Max Planck Institute for Comparative and International Private Law, Comments on the European Commission's Proposal for a Regulation of the European Parliament and the Council on the Law Applicable to Contractual Obligations (Rome I). Mohr Siebeck. 2007. P. 271).

осуществления своей предпринимательской профессиональной деятельности. Таким образом, договоры, заключаемые в сегменте *C2C* (между двумя физическими лицами – непрофессионалами, например, заключаемые на интернет-аукционах вроде *eBay*), не подпадают под действие положений ст. 6.

Основное правило определения права, применимого к договорам с потребителем, заключается в том, что такие договоры подчиняются праву страны проживания потребителя (а не праву наиболее тесной связи с договором, определяемому в соответствии со ст. 4) при условии, что предприниматель осуществляет (*pursues*) свою деятельность на территории такой страны либо любым иным образом направляет (*directs*) такую деятельность на ее территорию. Первый случай (предприниматель осуществляет свою деятельность на территории страны) охватывает достаточно простые ситуации, когда договор заключен на территории страны, где проживает потребитель[1].

Критерий направленности подобно Регламенту Брюссель I был введен специально для электронной коммерции, осуществляемой посредством веб-сайтов. Учитывая единую цель соответствующих положений, в литературе при определении критериев направленности для целей определения применимого права предлагается использовать те же критерии, которые были обозначены Европейским судом в деле *Hotel Alpenhoff* применительно к положениям ст. 15 (1) (*c*) Регламента Брюссель I об установлении юрисдикции.

Общее правило Регламента Рим I о применении к потребительским договорам права страны проживания потребителя не означает в принципе невозможности включения в потребительские договоры соглашений о выборе права. Однако применение выбранного в соответствии с таким соглашением права не может лишать потребителя тех гарантий, которые он имел бы в отсутствие такого соглашения (т.е. предоставляемых ему «родным» законодательством о защите прав потребителей).

Примечательно, что достаточно жесткое и последовательное европейское законодательство в области защиты прав потребителей все же имеет свои лакуны. Так, в соответствии со ст. 6 (4) (*a*) Регламента Рим I вышеприведенные «защитные» положения о праве, применимом к потребительским договорам, не распространяются на те из них, в рамках которых услуги подлежат оказанию в стране иной, нежели страна проживания потребителя. В качестве примера таких услуг можно привести различного рода туристические услуги. Причем не важно, были такие

[1] *Gillies L.* Op. cit. P. 104.

услуги заказаны посредством сети Интернет либо в офлайн-режиме. Примечательно, что данное исключение Регламента Рим I не согласуется с положениями ст. 15 Регламента Брюссель I, который допускает установление специальной юрисдикции в судах по месту исполнения договора, не делая никаких исключений относительно характера такого договора. Таким образом, получается интересная ситуация. При приобретении потребителем туристической путевки на зарубежный маршрут через интернет-магазин он все равно может предъявить иск в суд по месту своего жительства, но при этом применимое право будет определяться по иным принципам: или в соответствии с условиями договора, или в соответствии с принципами характерного исполнения и тесной связи, изложенными выше. Достаточно сложно объяснить причины, по которым операторы туристических услуг получили такие преимущества по сравнению с иными субъектами электронной коммерции, но пока соответствующее положение является частью европейского законодательства.

Основные положения, касающиеся порядка определения права, применимого к внедоговорным обязательствам (деликтам, неосновательному обогащению, действиям в чужом интересе без поручения, преддоговорным обязательствам), содержатся в Регламенте Рим II.

Главным принципом определения права является *lex loci damni*, в соответствии с которым применяется право страны, где наступил вред безотносительно к тому, где было совершено действие, повлекшее такой вред, либо где наступили косвенные последствия данного действия (ст. 4 (1) Регламента Рим II). Как отмечается, такой подход обусловлен тем, что основной задачей права в данном случае является адекватная компенсация потерпевшей стороны, а не наказание причинителя вреда[1]. Данное правило не предполагает альтернативы, как это имеет место при решении вопросов юрисдикции (как ранее отмечалось, в соответствии со ст. 5 (3) Регламента Брюссель I истец вправе выбрать суд как по месту совершения противоправного действия, так и по месту наступления последствий). Таким образом, если противоправное действие повлекло вредоносные последствия на территории сразу нескольких стран, то должно применяться право каждой из таких стран в отношении вреда, наступившего в ней.

Применяя в совокупности правила о юрисдикции и о выборе применимого права, можно прийти к следующему выводу. Если потерпевший предъявляет иск в суд по месту наступления вреда, то такой

[1] *Bogdan M.* Torts in Cyberspace. The Impact of the New Regulation Rome II // Masaryk University Journal of Law and Technology. No 2. 2005. P. 5.

суд будет иметь юрисдикцию в отношении части вреда, наступившего в такой стране, и в качестве применимого будет использовать свое право (*lex fori*). Если потерпевший предъявит иск в суд по месту домициля причинителя вреда либо в суд по месту совершения противоправного действия, то суд установит свою юрисдикцию в отношении возмещения всего вреда и будет применять право каждой из стран, где такой вред наступил, т.е. «чужое» право.

Как отмечается, правило *lex loci damni* будет весьма редко применяться по отношению к деликтам, совершенным в сети Интернет (диффамации, нарушение права на частную жизнь, нарушение исключительных прав). Дело в том, что некоторые из них (диффамация и нарушение права на частную жизнь) под влиянием сильного лобби со стороны медиабизнеса были исключены из-под действия Регламента Рим II (ст. 1 (2) (*g*))[1]. Порядок определения права, применимого к нарушению исключительных прав, определяется в соответствии с *lex loci protectionis* (применение права страны, для которой истребуется защита). По сути *lex protectionis* является иным названием известной привязки *lex loci delicti* (закон места совершения правонарушения), специально предназначенным для применения в сфере нарушений прав интеллектуальной собственности[2]. Если же речь идет о нарушении единого исключительного права, признаваемого Европейским сообществом (товарный знак, селекционные достижения, наименования места происхождения товара), то применяется принцип *lex loci delicti*: право страны, где было совершено нарушение.

Наконец, необходимо сказать несколько слов о том, как будет определяться право, применимое к случаям защиты чести, достоинства и деловой репутации в сети Интернет.

В деле *Shevill v. Press Alliance*, рассмотренном в 1995 г. Европейским судом, была установлена презумпция применения закона страны суда (*lex fori*) к диффамационным искам, предъявленным за пределами страны, где домицилирован ответчик[3]. Таким образом, применимое

[1] Первоначальный проект предполагал применение к таким деликтам права страны, где проживает или расположен потерпевший (ст. 7). Данный подход был отклонен как существенно ограничивающий свободу слова и подчиняющий владельцев информационных ресурсов праву стран с низким уровнем защиты свободы слова. См.: Proposal for a Regulation of the European Parliament and the Council on the Law Applicable to Non-contractual Obligations (Rome II) COM (2003). 427 final. 22.07.2003.

[2] Final Report on the Study on Intellectual Property and the Conflict of Laws. Second Part: Analysis of Divergences and Conflicts. April 18. 2000. P. 11. http://ec.europa.eu/internal_market/copyright/docs/studies/etd1999b53000e16_en.pdf

[3] *Kunke C.* Rome II and Defamation: Will the Tail Wag the Dog // Emory International Law Review. No 18. 2005. P. 1744.

право по спорам, связанным с распространением сведений, порочащих честь, достоинство и деловую репутацию в сети Интернет, в которых потерпевшим выступает иностранное лицо, определяется в соответствии с национальным законодательством страны, где рассматривается спор. А учитывая, что сведения, размещенные в сети Интернет, являются доступными во многих странах мира, у потерпевшего появляется неплохая выбора удобного правопорядка.

В связи с этим особого упоминания заслуживает законодательство Англии, которое является наиболее благоприятным по отношению к истцам по искам о диффамации. В частности, согласно английскому праву истцу достаточно лишь доказать факт сообщения ответчиком третьему лицу сведений, порочащих честь и достоинство истца. Доказывать наличие какого-либо ущерба при этом истец не должен. Доказать соответствие таких сведений действительности обязан ответчик. Причем английское право не признает в качестве защиты ссылок на ошибки, совершенные в состоянии добросовестного заблуждения. В отличие от законодательства США английское право не имеет специальных правил в отношении «публичной фигуры»[1]. Наконец, размер убытков в Англии присуждает жюри (а не судья), которое обычно присуждает достаточно высокие суммы. В некоторых случаях возможно и присуждение штрафных убытков (*punitive damages*)[2].

Одним из самых обсуждаемых английских дел, связанных с выбором наиболее благоприятной юрисдикции для рассмотрения диффамационных исков, является дело *Berezovsky v. Michaels*[3]. Еще во времена, когда Б. Березовский проживал в России (1997 г.) он предъявил иск к журналу «*Forbes*» в связи с размещенной в нем статьей, посвященной освещению событий в России. Сам журнал был издан в США. Иск был предъявлен в Англии. Палата лордов признала допустимым установление юрисдикции английских судов и применение английского права к данному спору, поскольку в данном случае была затронута репутация истца, сложившаяся в Англии. В результате в пользу истца были присуждены убытки, а ответчик был обязан опубликовать опровержение.

---

[1] В США иск истца, являющегося публичной фигурой, удовлетворяется только в случаях, когда имело место злоумышленное распространение диффамационных сведений (см.: *Libel* Tourism: Hearing on H.R. 6146 Before the Subcomm. on Commercial and Admin. Law of the H. Comm. on the Judiciary, 111th Cong. 46 (2009) (statement of attorney Laura R. Handman, a partner in the firm Davis Wright Tremaine LLP)).

[2] *Garfinkel T.* Jurisdiction over Communication Torts: Can You Be Pulled into Another Country's Court System for Making a Defamatory Statement Over the Internet? A Comparison of English and U.S. Law // Transnational Law. No 9. 1996. P. 489, 512.

[3] [2000] 1 W.L.R. 1004 (H.L.).

Данное дело примечательно тем, что ни одна из сторон не была английским резидентом, обстоятельства спора были преимущественно связаны с территорией США и России, а в Англии распространялось только порядка 0,02% от всего тиража данного журнала.

Из последних дел, непосредственно связанных с Интернетом, в связи с этим следует упомянуть дело *Bin Mahfouz v. Ehrenfeld*[1], в котором бывший глава Национального коммерческого банка Саудовской Аравии и двое его сыновей (все граждане Саудовской Аравии) предъявили иск к американскому гражданину в связи с тем, что его книга[2], где описывались различные схемы финансирования исламской экстремистской деятельности, порочит честь и достоинство истцов утверждением о том, что семья истца является одним из основных спонсоров *Al-Quaeda* и иных террористических организаций. В качестве обоснования для установления своей юрисдикции и применения английского права к данному спору Высокий суд Лондона сослался на то, что 23 экземпляра книги были приобретены в Англии с использованием различных сайтов, в том числе «*Amazon.com*», а первая глава книги была доступна в сети Интернет, т.е. и на территории Англии. Поскольку истцы имеют жилье и ведут бизнес на территории Англии, они обладают репутацией, которая подлежит защите на территории Англии.

Таким образом, субъектам, осуществляющим деятельность в сети Интернет, следует максимально аккуратно подходить к размещению информации, которая может быть интерпретирована как порочащая честь, достоинство или деловую репутацию лиц, имеющих достаточно ресурсов для того, чтобы организовать процесс в Англии или в иных благоприятных для истцов по подобного рода спорам местах.

В 2011 г. Европейский парламент выдвинул предложение дополнить Регламент Рим II положениями, содержащими принципы определения права, применимые к данным видам деликтов. В качестве общего правила подлежит применению право страны, где права потерпевшего непосредственно и существенно затронуты. Однако если лицо, причинившее вред, не могло разумно предвидеть возможность наступления существенных последствий своих действий в такой стране, то применяется право страны, где проживает (расположено) лицо, причинившее вред. В данном предложении отражено основное требование представителей медиабизнеса, заключающееся в необходимости учета при определении применимого права фактора предвидимости

[1] [2005] EWHC 1156 (QB).

[2] *Ehrenfeld R.* Funding Evil: How Terrorism is Financed and How to Stop It. Bonus Books. 2003.

возможных последствий своих действий[1]. В отношении права на опровержение и иных подобных мер применяется право страны, где проживает (расположен) издатель (публикатор). В настоящее время предложение все еще находится в стадии рассмотрения.

В завершение рассмотрения вопроса о применимом праве необходимо сказать несколько слов о принципе страны происхождения (*country of origin principle*), закрепленном в ст. 3 Директивы ЕС «Об электронной коммерции».

Суть данного принципа заключается в том, что коль скоро интернет-услуга соответствует требованиям законодательства государства – члена ЕС, откуда она «исходит», такая услуга может свободно оказываться на территории других государств – членов ЕС. В европейской доктрине продолжаются дискуссии о природе принципа «страны происхождения» и многие авторитетные ученые признают за ним значение нормы, регламентирующей применимое право (право страны учреждения провайдера услуги)[2].

Однако далеко не все разделяют данную позицию. По мнению ряда специалистов, данное правило носит публично-правовой характер и фактически распределяет законодательную юрисдикцию между различными государствами – членами ЕС. Его цель заключается в обеспечении свободного перемещения услуг в рамках общего рынка и предотвращении его фрагментации вследствие различного правового регулирования. Страны, принимающие услугу (*host states*), могут устанавливать дополнительные требования и регулирование только в той степени, в какой это необходимо из соображений публичной политики, охраны здоровья, безопасности, защиты прав потребителей.

Данная позиция разделяется Европейским судом, по мнению которого принцип страны происхождения не относится к числу коллизионных (т.е. регулирующих вопрос выбора применимого права), а означает недопустимость подчинения провайдера информационных услуг более строгому правовому режиму по сравнению с тем, который существует в стране, где он учрежден, за исключением случаев, прямо указанных в Директиве[3]. При этом Европейский суд также сослался на ст. 1 (4) Директивы, согласно которой она не устанавливает дополнительных правил, касающихся юрисдикции судов либо международного частного права.

Ни в коей мере не оспаривая выводы Европейского суда по данному вопросу, полагаю, что принцип «страны происхождения» мог бы быть

[1] *Kunke C.* Op. cit. P. 1752.
[2] *Savin A.* Op. cit. P. 71–75.
[3] eDate Advertising GmbH v Martinez, ECR. 25 October 2011. C-509/09.

одним из возможных подходов при построении единого регуляторного пространства применительно к деятельности, осуществляемой в сети Интернет. Но это уже тема для отдельного исследования.

3.4. Принудительное исполнение судебного решения в Европейском союзе (jurisdiction to enforce)

Как известно, неопределенность, существующая в вопросах взаимного признания и исполнения судебных решений, в значительной степени препятствует развитию оборота, поскольку свобода движения товаров, работ и услуг между различными юрисдикциями предполагает столь свободный же «оборот» судебных решений. Поскольку одной из основных целей создания Европейского союза являлось создание общего рынка, на обеспечение функционирования которого преимущественно и направлено большинство норм общеевропейского законодательства, неудивительно, что вопросы взаимного признания и приведения в исполнение судебных решений стали предметом особого внимания со стороны европейских законодателей.

В Европе существует несколько правовых режимов, установленных общеевропейскими актами, в рамках которых осуществляется взаимное признание судами государств – членов ЕС вынесенных судебных решений и которые могут представлять интерес в контексте освещения проблематики электронной коммерции.

Основным правовым режимом являются положения Регламента Брюссель I, который пришел на смену Брюссельской конвенции, которая в свою очередь заменила запутанную систему двусторонних договоров между отдельными странами – участниками ЕС. Для того чтобы иностранное судебное решение, вынесенное судом государства – члена ЕС, могло принудительно исполняться, необходимо, чтобы оно: 1) обладало юридической силой на территории государства, где оно было вынесено; 2) было признано судом на территории исполняющего государства; 3) отсутствовали основания для отказа в признании такого решения. К таким основаниям относится: а) противоречие публичному порядку признающего государства; б) отсутствие заблаговременного извещения ответчика о начале процесса, что не позволило ему организовать свою защиту; в) противоречие данного решения вынесенному в судах признающего государства решению по спору между теми же сторонами; г) противоречие данного решения вынесенному в судах иных государств решению по тому же спору между теми же сторонами при условии, что такое решение удовлетворяет критериям, необходимым для его принудительного исполнения (ст. 34 Регламента Брюссель I).

Для обеспечения оперативности рассмотрения небольших требований гражданско-правового характера (не превышающих 2000 евро), носящих трансграничный характер (т.е. где хотя бы одна из сторон домицилирована в ином государстве, где расположен признающий суд), и минимизации издержек по их рассмотрению в Европейском союзе была учреждена специальная процедура рассмотрения небольших требований (*European Small Claims Procedure*)[1]. Процесс, предусмотренный данной процедурой, носит документарный характер. Регламент предусматривает требования, предъявляемые к представляемым документам и доказательствам, представительству сторон, срокам рассмотрения спора, порядку его обжалования, и иные процессуальные аспекты. Процессуальные документы максимально стандартизированы: в них содержатся разъяснения и поля, в которых необходимо отразить суть спора.

Представительство сторон профессиональным юристом не является обязательным, равно как и личное присутствие сторон перед судом: суд при необходимости может пообщаться со сторонами посредством видеоконференции. Вынесенное решение подлежит исполнению на территории всех государств – членов ЕС без необходимости получения предварительной процедуры его признания (*экзекватуры*). Исполнение такого решения осуществляется в соответствии с законодательством государства, где происходит исполнение в порядке, применимом к его собственным судебным решениям.

Представляется, что указанная процедура представляет собой интерес и вне рамок Европейского союза. Это хороший пример того, как можно обеспечить доступность правосудия в современных реалиях, в том числе с привлечением современных информационно-телекоммуникационных технологий. Учитывая, что в сфере электронной коммерции достаточно много требований, размер которых носит незначительный характер, наличие такой упрощенной процедуры весьма актуально, и что-то подобное может быть со временем имплементировано и в отечественное процессуальное законодательство. До этого момента многие положения подобной процедуры могут быть имплементированы в рамках альтернативного рассмотрения споров (*ADR*).

§ 4. Юрисдикция в сети Интернет: российский подход

В России компетенция судов по рассмотрению гражданско-правовых споров определяется гражданским процессуальным (ГПК РФ)

[1] Regulation EC № 861/2007 of the European Parliament and of the Council of 11 July 2007 establishing a European Small Claims Procedure // OJ 2007. 1199/1.

и арбитражным процессуальным законодательством (АПК РФ). Для того чтобы суд считался компетентным рассматривать определенный спор, необходимо, чтобы были соблюдены правила подведомственности и подсудности.

Правила о подведомственности разграничивают компетенцию по рассмотрению спора между различными звеньями судебной системы (главным образом между судами общей юрисдикции и арбитражными судами, в том числе судом по интеллектуальным правам). Нормы о подсудности определяют, какой именно суд в рамках определенного звена судебной системы обладает компетенцией по рассмотрению и разрешению данного спора.

Как следует из положений п. 3 ст. 22 ГПК РФ, суды общей юрисдикции рассматривают гражданские споры и споры, вытекающие из публичных правоотношений, за исключением тех из них, которые отнесены законодательством к компетенции арбитражных судов. Подведомственность спора арбитражному суду определяется двумя критериями: его характером (связь с предпринимательской и иной экономической деятельностью) и субъектным составом (по общему правилу – юридические лица и индивидуальные предприниматели) (п. 2 ст. 27 АПК РФ).

4.1. Условия установления персональной юрисдикции в отношении иностранного лица (jurisdiction to adjudicate)

В контексте тематики споров, возникающих в сети Интернет, нас прежде всего интересуют специальные положения процессуального законодательства, посвященные основаниям и порядку рассмотрения споров с участием иностранных лиц (которые в американской доктрине именуются «*long-arm statutes*»).

В соответствии со ст. 402 ГПК РФ суды в Российской Федерации рассматривают дела с участием иностранных лиц, если организация-ответчик находится на территории Российской Федерации или гражданин-ответчик имеет место жительства в Российской Федерации.

В ч. 3 ст. 402 ГПК РФ содержатся специальные основания для рассмотрения споров с участием иностранных лиц, из которых потенциально применимыми к сфере электронной коммерции являются следующие:

1) орган управления, филиал или представительство иностранного лица находится на территории Российской Федерации;

2) ответчик имеет имущество, находящееся на территории Российской Федерации;

5) по делу о возмещении вреда, причиненного имуществу, действие или иное обстоятельство, послужившие основанием для предъявления

требования о возмещении вреда, имело место на территории Российской Федерации;

6) иск вытекает из договора, по которому полное или частичное исполнение должно иметь место или имело место на территории Российской Федерации;

7) иск вытекает из неосновательного обогащения, имевшего место на территории Российской Федерации;

9) по делу о защите чести, достоинства и деловой репутации истец имеет место жительства в Российской Федерации.

Основания для установления юрисдикции российских арбитражных судов в отношении споров с участием иностранных лиц закреплены в ч. 1 ст. 247 АПК РФ, из которых особого упоминания заслуживают следующие:

1) ответчик находится или проживает на территории Российской Федерации либо на этой территории находится имущество ответчика;

2) орган управления, филиал или представительство иностранного лица находится на территории Российской Федерации;

3) спор возник из договора, по которому исполнение должно иметь место или имело место на территории Российской Федерации;

4) требование возникло из причинения вреда имуществу действием или иным обстоятельством, имевшими место на территории Российской Федерации либо при наступлении вреда на территории России;

5) спор возник из неосновательного обогащения, имевшего место на территории Российской Федерации;

6) истец по делу о защите деловой репутации находится в Российской Федерации;

9) спор возник из отношений, связанных с государственной регистрацией имен и других объектов и оказанием услуг в международной ассоциации информационно-телекоммуникационных сетей «Интернет» на территории Российской Федерации;

10) в других случаях при наличии тесной связи спорного правоотношения с территорией Российской Федерации.

Рассмотрим подробнее, как данные положения могут быть применены к решению вопроса о юрисдикции российских судов применительно к спорам, возникшим в связи с использованием сети Интернет.

Договорные отношения

Как видно из положений подп. 6 ч. 3 ст. 402 ГПК РФ и подп. 3 ч. 1 ст. 247 АПК РФ, иск к иностранному лицу может быть предъявлен в российский суд не только по месту жительства (местонахождению)

такого лица, но и по месту исполнения договора. Аналогичный подход имеет место в Европе (ст. 5 (2) Регламента Брюссель 1) и при определенных условиях – в США (доктрина минимальных контактов).

Наибольший интерес в контексте договорных отношений в сети Интернет представляет, как отмечалось ранее, вопрос о месте исполнения обязательства по предоставлению цифрового контента, поскольку его решение непосредственно влияет на возможность установления российским судом своей юрисдикции в отношении иностранного лица, не имеющего местонахождения (места жительства) на территории России. Поскольку вопросы исполнения обязательства относятся к «компетенции» гражданского права, необходимо обратиться к соответствующим положениям ГК РФ.

Поскольку специальные положения на сей счет отсутствуют и в части второй, и в части четвертой ГК РФ, место исполнения обязательства по предоставлению цифрового контента должно определяться по общим правилам исполнения обязательства, указанным в ст. 316 ГК РФ, из которой методом исключения следует, что таким местом является место жительства должника (или его местонахождение, если должником является юридическое лицо)[1]. Другой вопрос, насколько российский суд вправе применять положения ГК РФ, регламентирующие место исполнения обязательства для целей решения вопроса о наличии компетенции по рассмотрению спора с участием иностранного лица, в то время как в качестве применимого может выступать иное право (не российское). Принимая во внимание, что вопросы компетентности суда рассматривать определенный спор носят публично-правовой характер и решаются в силу этого по правилам *lex fori*, применение положений ГК РФ является вполне обоснованным. В любом случае вопрос о применимом праве не решается ранее, чем будет решен вопрос о юрисдикции. Таким образом, если стороны прямо в договоре не указали, что местом исполнения обязательства по предоставлению цифрового контента является местонахождение (место жительства) его приобретателя, данное специальное основание для установления юрисдикции не добавляет ничего принципиально нового по сравнению с общим правилом о предъявлении иска в суд по месту жительства (местонахождению) ответчика.

В случае если в качестве стороны договора, заключенного в сети Интернет выступает потребитель, то в соответствии с п. 7 ст. 29 ГПК РФ и п. 2 ст. 17 Закона о защите прав потребителей иск может быть предъ-

[1] Все остальные перечисленные в данной статье варианты явно не подходят к рассматриваемым отношениям.

явлен в суд по месту жительства (месту пребывания) истца, по месту заключения или месту исполнения договора. Потребитель не может быть лишен или ограничен в реализации данного права договором[1]. В отличие от европейского законодательства (ст. 15 Регламента Брюссель I) российское законодательство не содержит критерия направленности деятельности как условия применения специальных защитных правил о юрисдикции. Для целей установления компетенции суда общей юрисдикции по рассмотрению спора потребителя с иностранным интернет-магазином абсолютно неважно, насколько такой магазин направлял свою предпринимательскую деятельность на территорию места жительства потребителя, а равно насколько он мог предвидеть возможность предъявления к нему иска на такой территории. В значительной степени здесь сказывается время принятия соответствующих положений: ГПК РФ был принят в 2002 г., Закон о защите прав потребителей – в 1992 (!) г., когда об электронной коммерции не задумывались.

К тому же древность российских законов о защите прав потребителей проявляется также и в том, что отношения, связанные с распространением цифрового контента, при излишне формальном толковании таких законов могут «выпасть» из-под сферы их применения. С одной стороны, приобретение цифрового контента обычно осуществляется в личных, семейных, домашних и иных нуждах, не связанных с осуществлением предпринимательской деятельности, но, с другой стороны, оно не укладывается в «прокрустово ложе» триады «товар – работа – услуга», которая обозначена в преамбуле к Закону о защите прав потребителей при описании сферы его действия. Как будет показано далее, цифровой контент нередко предоставляется на основании лицензионных договоров, являясь тем самым имущественным правом. Однако принимая во внимание имеющуюся в последнее время тенденцию к расширительному толкованию триады «товары – работы – услуги», проявляющуюся в разъяснениях Верховного Суда РФ, есть основание полагать, что суд не будет столь формально подходить к вопросу о распространении на такие отношения норм законодательства о защите прав потребителей[2].

[1] Пункт 22 постановления Пленума Верховного Суда РФ от 28 июня 2012 г. № 17 «О рассмотрении судами гражданских дел по спорам о защите прав потребителей»; п. 7 информационного письма Президиума ВАС РФ от 13 сентября 2011 г. № 146 «Обзор судебной практики по некоторым вопросам, связанным с применением к банкам административной ответственности за нарушение законодательства о защите прав потребителей при заключении кредитных договоров».

[2] В частности, долгое время Верховный Суд РФ отказывал в признании отношений по страхованию, подпадающих под действие Закона о защите прав потребителей

Рассматривая вопрос о юрисдикции судов по спорам, связанным с договорными отношениями, следует принимать во внимание, что подавляющее большинство договоров, заключаемых в сети Интернет, будут так или иначе иметь соглашение о выборе суда (пророгационное соглашение), в связи с чем необходимо рассмотреть те правила, которые применимы к такого рода соглашениям по российскому праву.

Согласно ст. 249 АПК РФ, если стороны, хотя бы одна из которых является иностранным лицом, заключили письменное соглашение, где определили, что арбитражный суд России обладает компетенцией по рассмотрению возникшего или могущего возникнуть спора, связанного с осуществлением ими предпринимательской и иной экономической деятельности, арбитражный суд России будет обладать исключительной компетенцией по его рассмотрению, при условии, что такое соглашение не изменяет исключительную компетенцию иностранного суда. При этом не обязательно, чтобы одной из сторон такого пророгационного соглашения выступало российское лицо, оно может быть заключено и между двумя иностранными лицами[1], например между зарубежными аффилированными лицами российских компаний.

Российская судебная практика выработала ряд положений, направленных на обеспечение баланса интересов сторон при заключении пророгационных соглашений. Так, такие соглашения не могут носить «ассимметричный» характер, т.е. не могут одну сторону наделять альтернативным арбитражному разбирательству правом на обращение в суд, а другую – нет. Несмотря на наличие арбитражной оговорки, сторона всегда может подать иск в государственный суд, если таким правом наделена другая сторона[2].

со ссылкой на то, что страхование не является ни товаром, ни работой, ни услугой. По мнению суда, целью заключения договора имущественного страхования является погашение за счет страховщика риска имущественной ответственности перед другими лицами или риска возникновения иных убытков в результате страхового случая (см.: Обзор законодательства и судебной практики Верховного Суда Российской Федерации за первый квартал 2008 года, утв. Постановлением Президиума Верховного Суда РФ от 28 мая 2008 г. // Бюллетень Верховного Суда РФ. 2008. № 8). Однако впоследствии Верховный Суд РФ отошел от такого формального толкования положений преамбулы Закона о защите прав потребителей и распространил его и на договоры страхования имущества, заключенные гражданами для личных, семейных, домашних и иных нужд, не связанных с осуществлением предпринимательской деятельности. (См. п. 2 постановления Пленума Верховного Суда РФ от 27 июня 2013 г. № 20 «О применении судами законодательства о добровольном страховании имущества граждан»).

[1] Пункт 1 информационного письма Президиума ВАС РФ от 9 июля 2013 г. № 158 «Обзор практики рассмотрения арбитражными судами дел с участием иностранных лиц».

[2] Постановление Президиума ВАС РФ от 19 июня 2012 г. № 1831/12.

Нередко *click-wrap*-соглашения и иные договоры, заключаемые в сфере электронной коммерции, содержат пророгационное соглашение в пользу иностранного суда. Если в качестве одной из сторон такого соглашения выступает потребитель, то подобные положения не лишают его возможности предъявления иска по своему месту жительства. Если такое соглашение содержится в договоре между предпринимателями, возникает вопрос, препятствует ли наличие такого пророгационного соглашения в пользу иностранного суда установлению компетенции отечественного суда. Формальное толкование положений ст. 249 АПК РФ позволяет сделать вывод об отсутствии препятствий для российского арбитражного суда признать себя компетентным рассматривать данный спор по общим правилам определения международной подсудности даже при наличии пророгации в пользу иностранного суда. Такой подход, как отмечается, с одной стороны, расширяет пределы юрисдикции Российской Федерации, но, с другой стороны, противоречит принципу автономии воли сторон и дестабилизирует хозяйственный оборот, поскольку лишает стороны элемента предсказуемости в вопросе о компетентной юрисдикции.

Данные соображения были приняты во внимание ВАС РФ, который установил, что «арбитражный суд не признает себя компетентным, если по заявлению стороны установит, что между сторонами правоотношения заключено исполнимое и юридически действительное соглашение о рассмотрении спора исключительно судом иностранного государства». В качестве основания для такого решения была применена аналогия закона п. 5 ч. 1 ст. 148 АПК РФ (о праве арбитражного суда оставить заявление без рассмотрения при наличии соглашения о рассмотрении такого спора в третейском суде)[1].

Таким образом, российское законодательство допускает широкую степень усмотрения сторон предпринимательского договора по выбору компетентного суда: они могут выбрать как российский арбитражный суд, так и зарубежный суд. В обоих случаях, за редким исключением, российский арбитражный суд будет придерживаться волеизъявления сторон. В связи с этим вряд ли стоит упускать возможность урегулировать данный вопрос субъектам электронной коммерции, осуществляющим деятельность в *B2B*-сегменте. Соответствующие положения могут быть, в частности, включены в стандартные договоры, размещенные на сайте (*click-wrap*-соглашения).

[1] Пункт 6 информационного письма Президиума ВАС РФ от 9 июля 2013 г. № 158 «Обзор практики рассмотрения арбитражными судами дел с участием иностранных лиц».

Деликтные отношения

Юрисдикция российских судов применительно к спорам с участием иностранных лиц, возникшим из деликтов, определяется различным образом применительно к арбитражным судам и судам общей юрисдикции. В соответствии с п. 4 ч. 1 ст. 247 АПК РФ российский арбитражный суд вправе рассматривать подобного рода споры, если требование возникло из причинения вреда имуществу действием или иным обстоятельством, имевшими место на территории Российской Федерации либо при наступлении вреда на территории России. В соответствии с п. 5 ч. 3 ст. 402 ГПК РФ суд общей юрисдикции принимает к рассмотрению споры в случаях, если действие или иное обстоятельство, послужившие основанием для предъявления требования о возмещении вреда, имели место на территории Российской Федерации. В отличие от АПК РФ ГПК РФ не предусматривает возможности установления судом общей юрисдикции своей компетенции в отношении иностранного ответчика в случае, если вред наступил на территории Российской Федерации, но само действие, повлекшее такой вред, было совершено за рубежом.

Проиллюстрируем данное различие на примере иска о взыскании российским правообладателем компенсации за нарушение его исключительного права. Как известно, внедоговорное использование объектов интеллектуальной собственности является деликтом[1]. В случае если соответствующее нарушение имело место посредством распространения контрафактных экземпляров произведения с сервера, расположенного за пределами территории России, то суд общей юрисдикции не сможет на основании п. 5 ч. 3 ст. 402 ГПК РФ принять к рассмотрению такой иск. Ведь на территории России наступили лишь вредоносные последствия, в то время как само действие, повлекшее вред, было совершено за рубежом. Напротив, арбитражный суд может в такой ситуации принять к рассмотрению иск в отношении иностранного ответчика, поскольку АПК РФ допускает установление юрисдикции в силу факта наступления вреда на территории Российской Федерации.

При решении вопросов о наличии юрисдикции российских судов по рассмотрению споров, связанных с интеллектуальной собственностью, не следует забывать о положениях ст. 248 АПК РФ, согласно которым споры, связанные с регистрацией или выдачей патентов, ре-

[1] Комментарий к части четвертой Гражданского кодекса Российской Федерации (поглавный) / под ред. А.Л. Маковского. М., 2008. С. 375; Комментарий к Гражданскому кодексу Российской Федерации части четвертой (постатейный) / отв. ред. Л.А. Трахтенгерц. М., 2009. С. 106.

гистрацией и выдачей свидетельств на товарные знаки, промышленные образцы, полезные модели или регистрацией других прав на результаты интеллектуальной деятельности, которые требуют регистрации или выдачи патента либо свидетельства в Российской Федерации, относятся к исключительной юрисдикции арбитражных судов России. Так, например, иск корпорации «*Microsoft*» к российскому лицу в связи с неправомерным использованием им товарного знака «*Windows*», зарегистрированного в России, относится к исключительной юрисдикции российского арбитражного суда[1]. Исключительная компетенция предполагает в данном случае не только невозможность ее изменения соглашением сторон, но и невозможность передачи рассмотрения данного спора в третейский суд. Если иностранный суд или арбитраж все же вынесет решение по такому вопросу, арбитражный суд отказывает в признании и приведении в исполнение этого решения на территории Российской Федерации (п. 3 ч. 1 ст. 244 АПК РФ).

Что касается компетенции российских судов по рассмотрению споров, связанных с распространением сведений, порочащих честь, достоинство и деловую репутацию в сети Интернет, следует отметить, что и ГПК РФ, и АПК РФ содержат специальные положения на сей счет, допускающие установление юрисдикции суда по месту жительства (местонахождению) истца (п. 9 ч. 3 ст. 402 ГПК РФ, п. 6 ч. 1 ст. 247 АПК РФ). Таким образом, если соответствующий материал был размещен в сети Интернет иностранным лицом, требование к такому лицу может быть предъявлено в российский суд (суд общей юрисдикции, если речь идет о защите чести и достоинства, арбитражный суд, если иск заявлен по поводу защиты деловой репутации). При этом в отличие от подхода, демонстрируемого некоторыми американскими судами, не важно, направлял ли ответчик свою деятельность на территорию России. Значение имеют исключительно формальные моменты: расположение истца на территории Российской Федерации и характер предъявленного требования. В отличие от общеевропейского законодательства отдельно доказывать факт причинения вреда на территории России не требуется (хотя это и не так сложно, учитывая характер причиненного вреда и его тесную связь с личностью истца).

Рассматривая вопросы, возникающие с юрисдикцией споров, связанных с сетью Интернет, особо следует упомянуть два положения АПК РФ, которые могут быть потенциально применимы к такого рода отношениям.

[1] Постановление ФАС Московского округа от 28 ноября 2012 г. по делу № А40-131680/11-51-1187.

В п. 9 ч. 1 ст. 247 АПК РФ устанавливается, что в компетенцию арбитражных судов входит рассмотрение дел по экономическим и иным делам, связанным с осуществлением предпринимательской и иной экономической деятельности иностранных лиц, международных организаций, в том случае, если спор возник из отношений, связанных с государственной регистрацией имен и других объектов и оказанием услуг в международной ассоциации сетей Интернет на территории Российской Федерации.

Формулировка данного положения является весьма неудачной. Обозначение сети Интернет в качестве международной ассоциации (обозначения, свойственного больше субъектам права, коим Интернет не является) уже не может не вызывать нареканий, как и словосочетание «государственная регистрация имен ...в международной ассоциации информационно-телекоммуникационных сетей Интернет». Как известно, доменные имена как главные и единственные кандидаты на применение данной формулировки регистрируются негосударственными организациями. Так, в России такая регистрация осуществляется аккредитованными регистраторами доменных имен в доменах *RU* и РФ, которые являются коммерческими организациями[1]. Так что, формально говоря, данная норма малопригодна *сама по себе* для обоснования юрисдикции российских арбитражных судов в отношении споров, связанных с регистрацией доменных имен на территории Российской Федерации. Упоминание возможности существования государственной регистрации иных объектов в сети Интернет также вызывает недоумение. Если имелась в виду государственная регистрация каких-либо объектов, которые так или иначе могут фигурировать в сети Интернет, то основной кандидат в виде товарного знака уже охвачен в этой части специальным регулированием (ст. 248 АПК РФ). За вычетом вышеуказанных положений в «сухом остатке» п. 9 ч. 1 ст. 247 АПК РФ остается упоминание о юрисдикции арбитражных судов в отношении услуг, оказываемых в сети Интернет на территории Российской Федерации. Однако и здесь возникает ряд вопросов. Во-первых, почему упоминаются только услуги? Товары и тем более права на объекты интеллектуальной собственности также выступают объектом оборота в сети Интернет. Во-вторых, что реально добавляет это правило к тому, что уже и так есть: ведь если договор оказания услуг, заключенный в сети Интернет, подлежит исполнению на территории Российской Федерации, то в соответствии с положениями

[1] См. подробнее § 5 гл. 5 настоящей книги.

п. 3 ч. 1 ст. 247 АПК РФ иск может быть и так предъявлен по месту исполнения договора безотносительно к использованию сети Интернет при его заключении. Если же договор оказания услуг, заключенный в сети Интернет, подлежит исполнению за пределами Российской Федерации, то такая ситуация противоречит формулировке п. 9 ч. 1 ст. 247 АПК РФ, в которой прямо говорится о территории Российской Федерации. Но даже если эта ситуация и охватывалась бы данной нормой, то обосновать такое специальное основание юрисдикции можно было бы лишь наличием тесной связи договора с территорией Российской Федерации, в противном случае получалась бы абсурдная ситуация при которой любые предпринимательские споры, связанные с оказанием услуг в сети Интернет, оказались бы подведомственными российским арбитражным судам. Но для ситуаций, при которых имеет место тесная связь договора с территорией Российской Федерации, существует специальное основание для установления юрисдикции (п. 10 ч. 1 ст. 247 АПК РФ). Указанные соображения позволяют сделать вывод о том, что положения п. 9 ч. 1 ст. 247 АПК РФ в том виде, в каком они сформулированы сейчас, не обладают какой-либо самостоятельной ценностью и не расширяют перечень оснований для установления юрисдикции арбитражных судов в отношении споров с участием иностранных лиц, содержащихся в иных положениях АПК РФ.

Следующая норма, которая заслуживает упоминания, – это п. 10 ч. 1 ст. 247 АПК РФ, согласно которой установление юрисдикции российским арбитражным судом допустимо в «иных случаях при наличии тесной связи спорного правоотношения с территорией Российской Федерации». Критерий тесной связи обычно используется при решении вопроса о выборе применимого права, но не для определения юрисдикции, в связи с этим подход российского АПК отличается значительной оригинальностью[1]. Исходя из формулировки рассматриваемого пункта все иные основания для установления юрисдикции, упомянутые в п. 1–9 ч. 1 ст. 247 АПК РФ, являются лишь частными случаями реализации данного принципа. Принцип «тесной связи» позволяет уйти от исчерпывающего перечня оснований международной подсудности. Такой перечень, каким бы подробным и детальным он ни был, всегда будет несовершенным. С учетом динамики гражданского оборота, широкого применения в нем принципа диспозитивности заранее очертить

[1] *Батлер У.Э., Ерпылева Н.Ю.* Производство по делам с участием иностранных лиц в международном процессуальном праве России и Кыргызстана // Законодательство и экономика. 2012. № 11.

круг споров, могущих возникнуть из цивилистических отношений, практически невозможно[1].

Анализ небогатой судебной практики позволяет обозначить те критерии, которые принимают во внимание арбитражные суды при установлении наличия тесной связи спора с территорией Российской Федерации: 1) субъектный состав спора; 2) местонахождение основных доказательств по делу; 3) место исполнения судебного решения[2]. При этом должны также приниматься во внимание и прагматические соображения. Тесная связь должна иметь какое-либо практическое обоснование: облегченный порядок исполнения будущего решения, сбора доказательств, защиту слабой стороны, предъявление иска по связи дел, которая распространяет подсудность одного требования на все другие, если их разъединение невозможно (например подача встречного иска, подача иска к нескольким ответчикам, находящимся на территории разных государств) и т.д.[3]

В качестве возможной иллюстрации применения данного критерия можно привести ситуации, когда вред от деятельности иностранного лица в сети Интернет еще не наступил, в силу чего применение п. 4 ч. 1 ст. 247 АПК РФ как специального основания для установления юрисдикции по деликтным спорам невозможно, но в то же время существует реальная угроза наступления такого вреда на территории Российской Федерации. Российскому праву известны превентивные способы защиты прав (например, требования о признании права или пресечении действий, создающих угрозу нарушения права). Однако их реализация возможна только в рамках дела, принятого судом к производству. Безусловно, сохраняются вопросы, связанные с последующим исполнением судебного решения, но иногда сам факт наличия судебного решения по определенному вопросу может иметь важное значение при ведении информационной политики компании в СМИ или общении с контрагентами.

Также критерий тесной связи может быть использован применительно к договорам, по которым распространяются электронные

---

[1] См.: *Мамаев А.А.* Принцип «тесной связи» спорного материального правоотношения с территорией Российской Федерации как основание определения международной судебной юрисдикции по гражданским делам // Арбитражный и гражданский процесс. 2008. № 2.

[2] Постановление Девятого арбитражного апелляционного суда от 18 апреля 2011 г. № 09АП-7645/2011 г. по делу № А40-116933/09-50-926, оставленное в силе постановлением ФАС Московского округа от 8 августа 2011 г. № КГ-А40/6186-11.

[3] Постановление Девятого арбитражного апелляционного суда от 24 марта 2008 г. № 09АП-2750/2008-ГК; *Нешатаева Т.Н.* О вопросах компетенции арбитражных судов в Российской Федерации по рассмотрению дел с участием иностранных лиц // Вестник ВАС РФ. 2004. № 12.

экземпляры произведений. Ранее уже говорилось о том, что в данном случае применение специального основания для установления юрисдикции суда в виде исполнения договора на территории Российской Федерации является проблематичным в силу положений ст. 316 ГК РФ о месте исполнения обязательства. Тем не менее факт места нахождения или местажительства приобретателя в России может служить основанием для вывода о тесной связи договора с территорией Российской Федерации в отсутствие пророгационных или третейских соглашений в соответствующем договоре.

4.2. Определение применимого права к отношениям в сети Интернет (jurisdiction to prescribe)

Прежде чем перейти к вопросам, связанным с определением применимого права к трансграничным отношениям в сети Интернет, необходимо еще раз подчеркнуть необходимость четкого отграничения вопросов определения юрисдикции суда по рассмотрению спора (*jurisdiction to adjudicate*) от вопросов, связанных с определением права, применимого к такому спору. Некоторые авторы, к сожалению, имеют неверные представления о том, что первично: юрисдикция или применимое право. Так, Н.А. Дмитрик пишет, что «для договорных отношений в сети Интернет более важным является вопрос о применимом к таким отношениям праве, т.е. о действии закона в пространстве и по кругу лиц. Вопрос о подведомственности и подсудности возникающих споров также важен, но он *производен* (выделено мной. – *А.С.*) от вопроса о применимом праве»[1]. Сразу возникает вопрос, как можно определить применимое право, если предварительно не решен вопрос о том, кто же его будет определять и применять. Но дело даже в другом. Данные вопросы решаются в соответствии с различными принципами. При этом «разграничение принципов установления подлежащего применению права и правил определения компетентного суда выступает основой современной концепции международного частного права»[2]. При решении вопроса о своей компетентности по рассмотрению спора суд руководствуется правом своей страны (*lex fori*), при решении вопроса о применимом праве суд руководствуется в том числе и правилами коллизионного регулирования, допускающими широкую автономию

[1] *Дмитрик Н.А.* Осуществление субъективных гражданских прав с использованием сети Интернет. М., 2006. С. 73.

[2] *Batiffol H., Lagarde P.* Traite de droit international prive. T. II. No 668. P. 446. Цит. по: *Крохалев С.В.* Категория публичного порядка в международном гражданском процессе. СПб., 2006. § 350.

воли по выбору иностранного права. Установление судом своей юрисдикции в отношении спора само по себе не влечет применения законодательства страны суда к такому спору[1].

Положения о выборе применимого права, которыми будет руководствоваться российский суд, положительно решивший вопрос о наличии своей юрисдикции по рассмотрению спора с участием иностранного лица, содержатся в разд. VI части третьей «Международное частное право» ГК РФ. Не ставя перед собой цель переписывания основ международного частного права, следует обозначить основные подходы к выбору применимого права к договорным и внедоговорным отношениям, которые могут иметь значение в контексте сети Интернет.

Договорные обязательства

Основным принципом выбора применимого права к договорам, осложненным иностранным элементом, является принцип автономии воли. Согласно ст. 1210 ГК РФ стороны вправе выбрать право, применимое к их правам и обязанностям по договору. Такое право должно быть прямо выражено или должно определенно вытекать из условий договора либо совокупности обстоятельств дела. Так, при решении вопроса о наличии соглашения сторон о выборе применимого права, вытекающего из условий договора, суд может принять во внимание имеющиеся в договоре ссылки на нормы права определенной страны; использование терминологии, характерной для определенной правовой системы, в некоторых случаях – валюту и язык договора. Соглашение сторон о выборе применимого права может следовать и из иных, кроме собственной условий договора, обстоятельств дела. В частности, из сложившейся договорной практики сторон (ранее заключенные договоры содержали оговорку о выборе применимого права); ссылки сторон на нормы одного и того же правопорядка в ходе судебного разбирательства[2], связь договора с иными договорами, содержащими условие о применимом праве[3].

Таким образом, по общему правилу оговорки о применимом праве, сделанные в договорах, заключаемых посредством сети Интернет, в том числе *click-wrap*-соглашениях, подлежат признанию со стороны российских судов[4]. Российское гражданское право не ограничивает

[1] Пункт 12 информационного письма Президиума ВАС РФ от 9 июля 2013 г. № 158 «Обзор практики рассмотрения арбитражными судами дел с участием иностранных лиц».

[2] Там же.

[3] *Асосков А.В.* Указ. соч. С. 126 и далее.

[4] Правовой статус и условия действительности подобных соглашений будут подробно рассмотрены далее.

выбор применимого права требованиями о наличии разумной связи между таким правом и регулируемым им правоотношением, как это отчасти имеет место в США.

Однако существуют определенные ограничители свободы усмотрения сторон в выборе применимого права. Одним из таких ограничителей является норма п. 5 ст. 1210 ГК РФ, согласно которой «если в момент выбора сторонами договора подлежащего применению права все касающиеся существа отношений сторон обстоятельства связаны только с одной страной, выбор сторонами права другой страны не может затрагивать действие императивных норм права той страны, с которой связаны все касающиеся существа отношений сторон обстоятельства». Данное правило направлено на противодействие обходу закона посредством выбора применимого права к отношениям с искусственно «притянутым за уши» иностранным элементом, например, в виде ссылок в договоре на то, что он был подписан за рубежом.

Другим ограничителем являются сопутствующие выбору применимого права обременения, связанные с последующим определением и доказыванием содержания такого иностранного права в суде. Бремя такого доказывания может быть возложено судом на стороны соответствующим определением в соответствии с ч. 2 ст. 14 АПК РФ и п. 2 ст. 1191 ГК РФ. Чем более экзотическим является выбранное право, тем сложнее (и дороже) установить его содержание. Неисполнение же сторонами обязанностей по определению содержания иностранного права может повлечь применение судом российского права. При этом сторона, не исполнявшая возложенную на нее судом обязанность по представлению сведений о содержании норм иностранного права, не вправе впоследствии ссылаться на неустановление арбитражным судом содержания иностранного права, если арбитражный суд предпринял достаточные меры для его установления[1]. Поэтому сторонам (или стороне, разрабатывающей форму договора присоединения) имеет смысл максимально трезво оценивать свои возможности при выборе применимого права и выбирать лишь то иностранное право, которое хорошо известно или по крайней мере может быть установлено без особых сложностей и затрат[2].

[1] Пункт 18 информационного письма Президиума ВАС РФ «Обзор практики рассмотрения арбитражными судами дел с участием иностранных лиц».

[2] В идеале выбор иностранного права должен сопровождаться третейской оговоркой или пророгационным соглашением в пользу суда, для которого такое право является родным. Это обеспечит его корректное применение. Сочетание «иностранное право» и «российский арбитражный суд» не является в связи с этим оптимальным и должно использоваться скорее как исключение, лишь при наличии на то веских причин.

Правом, применимым к договору (договорным статутом), определяются в соответствии со ст. 1215 ГК РФ вопросы его толкования, права и обязанности сторон, исполнение договора, последствия его неисполнения или ненадлежащего исполнения, прекращение договора, последствия его недействительности. За рамками договорного статута решаются вопросы, связанные с формой договора (определяемой по правилам ст. 1209 ГК РФ), право- и дееспособности сторон (определяемые личным законом: ст. 1195, 1202 ГК РФ и др.). По этой причине ст. 1215 ГК РФ не содержит в числе вопросов, определяемых договорным статутом, оснований недействительности договора, поскольку они настолько многообразны, что могут быть обусловлены причинами, связанными со статусом сторон договора, несоблюдением его формы и т.п.

В отсутствие соглашения сторон о выборе применимого права к договору до недавних изменений, внесенных в ст. 1211 ГК РФ, применялось право страны, с которой договор наиболее тесно связан. При этом по общему правилу правом страны, с которой договор наиболее тесно связан, считалось право страны, где находилось место жительства или основное место деятельности стороны, которая осуществляет исполнение, имеющее решающее значение для содержания договора.

С 1 ноября 2013 г. вступили в силу ряд изменений в части третьей ГК РФ[1], в числе которых и новая редакция ст. 1211 ГК РФ, которая упростила критерии выбора права в случае отсутствия соглашения сторон о выборе применимого права. В соответствии с новой редакцией, «если иное не предусмотрено настоящим Кодексом или другим законом, при отсутствии соглашения сторон о подлежащем применению праве к договору применяется право страны, где на момент заключения договора находится место жительства или основное место деятельности стороны, которая осуществляет исполнение, имеющее решающее значение для содержания договора». Таким образом, отпадал достаточно дискуссионный вопрос о соотношении критериев тесной связи и решающего исполнения при решении вопроса о выборе применимого права[2].

Как уже отмечалось ранее, применительно к положениям Регламента Рим I под исполнением, имеющим решающее значение для договора, обычно понимается обязательство, которое дает договору его имя и за которое причитается оплата. ГК РФ содержит конкретизацию того, как данное правило применяется к определенным видам договоров (п. 3 ст. 1211 ГК РФ). Так, по общему правилу такое исполнение,

[1] Федеральный закон от 30 сентября 2013 г. № 260-ФЗ «О внесении изменений в часть третью Гражданского кодекса Российской Федерации».

[2] Подробный анализ см.: *Асосков А.В.* Указ. соч. С. 418–437.

имеющее решающее значение для содержания договора, осуществляет, в частности, продавец по договору купли-продажи; даритель – в договоре дарения; подрядчик – в договоре подряда; агент – в агентском договоре и т.д.

Изменения в ст. 1211 ГК РФ также устранили пробел относительно того, кто является стороной, осуществляющей исполнение, имеющее решающее значение, в договоре возмездного оказания услуг. В соответствии с подп. 16 п. 3 ст. 1211 ГК РФ такой стороной является исполнитель[1].

Определенные изменения коснулись и правил определения применимого права к лицензионному договору. Вместо права страны лицензиара как стороны, осуществляющей исполнение, имеющее решающее значение для содержания договора, к лицензионному договору применяется право страны, на территории которой лицензиату разрешается использование результата интеллектуальной деятельности или средства индивидуализации. Однако, если такое использование разрешается на территории одновременно нескольких стран, как и ранее, применяется право страны, где находится место жительства или основное место деятельности лицензиара (п. 8 ст. 1211 ГК РФ). Таким образом, если лицензионный договор предусматривает так называемую всемирную (*worldwide*) лицензию, то в отсутствие оговорки о применимом праве будет подлежать применению право страны лицензиара. Поскольку многие стандартные программные продукты и иные объекты авторских прав, распространяемые посредством сети Интернет, предполагают обычно именно всемирную лицензию, то предлагаемые в проекте изменения не затронут сложившегося *status quo* в части определения права, применимого к лицензионным договорам. И хотя большинство коммерческих лицензионных соглашений так или иначе будут содержать оговорку о применимом праве, нормы ст. 1211 ГК РФ, содержащие восполняющее регулирование на случай ее отсутствия, могут быть весьма актуальными для многих свободных (*open source*) лицензий, которые не содержат такой оговорки.

Рассматривая вопрос о праве, применимом к лицензионным договорам, не следует забывать, что особенностью данного типа договоров, как, впрочем, и всех договоров, связанных с распоряжением правами на интеллектуальную собственность, является тесная взаимосвязь договорного статута и статута исключительного права, которому подчиняются вопросы, определяющие пределы действия исключитель-

[1] Подпункт «б» п. 12 ст. 3 проекта федерального закона № 47538-6 «О внесении изменений в части первую, вторую, третью и четвертую Гражданского кодекса Российской Федерации, а также в отдельные законодательные акты Российской Федерации».

ного права. При этом автономия воли, как это признается в доктрине и практике, ограничена лишь рамками договорного статута[1], поэтому статут исключительного права носит преимущественно императивный характер, о чем следует помнить. Подробнее вопрос о сфере действия статута исключительного права будет рассмотрен далее.

В контексте электронной коммерции представляет интерес положение п. 5 ст. 1211 ГК РФ, согласно которому в отношении договора, заключенного на аукционе, применяется право страны, где проводится аукцион. Возникает вопрос, насколько данное правило применимо к договорам, заключаемым на различного рода интернет-аукционах. С одной стороны, ГК РФ содержит достаточно широкое понятие аукциона, под которым в соответствии с п. 4 ст. 448 ГК РФ признается форма торгов, где выигравшим признается лицо, которое предложило наиболее высокую цену. Процесс заключения договора на аукционе вроде *eBay* вполне укладывается в данные рамки. С другой стороны, как отмечается в литературе, смысл правила подп. 3 п. 4 ст. 1211 ГК РФ обусловлен тем, что эффективное функционирование аукциона возможно лишь в том случае, когда все совершаемые сделки подчиняются одному праву[2]. Представляется, что данный аргумент справедлив в отношении классических аукционов вроде *Sotheby's*, но вряд ли применим ко всем интернет-аукционам. Так, если речь идет о предоставлении площадки, где происходит аукцион, но ее владелец не управляет ходом ведения аукциона (типичный пример – *eBay*), а продавец сам отбирает и оценивает заявки, то безоговорочное применение рассматриваемой коллизионной нормы (применение к заключаемым договорам права места проведения аукциона) вряд ли обоснованно. Тем более что в электронной среде достаточно сложно, если не невозможно, определить, что же следует понимать под «местом проведения аукциона».

К сожалению, новая редакция ст. 1211 ГК РФ исключила диспозитивность коллизионной привязки (ранее в таких случаях при определении применимого права допускалось принятие во внимание существа, условий обязательства и совокупности обстоятельств дела), поэтому учесть специфику заключения договоров на аукционах в сети Интернет уже не получится. В связи с этим при заключении договора на интернет-аукционе целесообразно прямо прописывать применимое право во избежание последующих неожиданностей в данном вопросе.

---

[1] См.: Международное частное право: Постатейный комментарий раздела VI Гражданского кодекса Российской Федерации / под ред. П.В. Крашенинникова. М., 2010. С. 186–187.

[2] *Асосков А.В.* Указ. соч. С. 452.

Необходимо подчеркнуть, что вышеуказанные презумпции являются ориентиром и подлежат применению, если иное не вытекает из закона, условий или существа договора либо совокупности обстоятельств дела. Поэтому сторона договора, не согласная с применением права, определенного в соответствии с данными презумпциями, может привести доказательства того, что договор наиболее тесно связан с другой страной и вследствие этого должно применяться именно ее право.

В случае, если одной из сторон по договору, осложненному иностранным элементом, является потребитель, то свобода определения применимого права договором ограничена защитными положениями ст. 1212 ГК РФ.

По ранее действовавшей редакции данной статьи установление в таком договоре применимого права не может повлечь за собой лишение такого физического лица (потребителя) защиты его прав, предоставляемой императивными нормами права страны места жительства потребителя, при условии, что имеет место хотя бы одно из следующих обстоятельств (п. 1 ст. 1212 ГК РФ):

1) заключению договора предшествовала в этой стране оферта, адресованная потребителю, или реклама и потребитель совершил в этой же стране действия, необходимые для заключения договора;

2) контрагент потребителя или представитель контрагента получил заказ потребителя в этой стране;

3) заказ на приобретение движимых вещей, выполнение работ или оказание услуг сделан потребителем в другой стране, посещение которой было инициировано контрагентом потребителя в целях побуждения потребителя к заключению договора.

Как отмечается, все перечисленные обстоятельства указывают на то, что потребитель, заключая договор или совершая заказ, как правило, отвечает на инициативу, проявленную в той или иной форме предпринимателем-контрагентом: либо отвечает на оферту, либо реагирует на рекламу, либо посещает другую страну, чтобы в ней совершить заказ на приобретение товаров (работ, услуг), по инициативе, исходящей от предпринимателя-контрагента. При таких обстоятельствах указание в договоре в качестве применимого права иного, чем право страны, места жительства потребителя могло бы повлечь нарушение его интересов по причине отсутствия в законодательстве выбранной страны тех гарантий, которые предоставляет потребителю его «родное» право[1].

[1] Комментарий к Гражданскому кодексу Российской Федерации, части третьей (постатейный) / под ред. Н.И. Марышевой, К.Б. Ярошенко. 3-е изд., испр. и доп. М., 2010.

Следует отметить, что указанные положения ст. 1212 ГК РФ несколько устарели, поскольку были заимствованы из ст. 5 Римской конвенции, действовавшей до вступления в силу Регламента Рим I. Как отмечалось ранее, в настоящее время Регламент Рим I оперирует иными критериями применения специальных защитных положений в отношении потребителей – критерием направленности, поскольку положения ст. 5 Римской конвенции были признаны слишком сложными в применении и в недостаточной степени учитывающими современные реалии электронной коммерции[1].

Еще до принятия Регламента Рим I российскими авторами отмечалась сложность применения указанных критериев к отношениям в сети Интернет. Так, С.А. Бабкин отмечает, что все события, указанные в п. 1 ст. 1212 ГК РФ, оказываются непригодными для регулирования интернет-отношений, так как они могут происходить в совершенно разных государствах, в том числе не совпадающих ни с государством нахождения потребителя, ни с государством нахождения его контрагента[2]. Однако, как представляется, причина малопригодности критериев, указанных в ранее действовавшей редакции п. 1 ст. 1212 ГК РФ, крылась все же несколько в ином.

Во-первых, в условиях высокой мобильности пользователей сети Интернет достаточно сложно определить их местонахождение в момент заключения договора, а равно место его исполнения. Как справедливо отмечает А.Н. Ошноков, при совершении потребителем сделки в Интернете его географическое нахождение в момент «нажатия клавиши» не должно быть решающим фактором для определения применимого к договору права. Равно, как нельзя во всех случаях считать страну, в доменной зоне которой зарегистрирован веб-сайт контрагента-потребителя, местом получения заказа[3]. В связи с этим однозначно определить, где же был получен заказ от потребителя при размещении его в сети Интернет, не представляется возможным.

Во-вторых, специфика деятельности в сети Интернет такова, что с технической точки зрения инициатива по установлению договорных отношений исходит все же от потребителя: именно он вводит запрос

[1] Max Planck Institute for Comparative and International Private Law, «Comments on the European Commission's Proposal for a Regulation of the European Parliament and the Council on the Law Applicable to Contractual Obligations (Rome I). Mohr Siebeck. 2007. P. 272–273.

[2] См.: *Бабкин С.А.* Право, применимое к отношениям, возникающим при использовании сети «Интернет»: Основные проблемы. М., 2003. С. 57.

[3] Комментарий к Гражданскому кодексу Российской Федерации, части третьей (постатейный) / под ред. Т.Е. Абовой, М.М. Богуславского, А.Г. Светланова. М., 2004.

в поисковую систему, вводит адрес веб-сайта в браузер, формирует заказ. Говорить о том, что предприниматель «сам пришел» к нему, во многих случаях можно лишь с определенной долей натяжки либо при полном игнорировании технической стороны вопроса.

В-третьих, сам по себе факт наличия веб-сайта, доступного потребителю, не позволяет говорить ни об оферте со стороны предпринимателя, ни о рекламе. Оферта требует наличия всех существенных условий и выражения намерения лица, сделавшего ее, считать себя заключившим договор с акцептантом (ст. 435 ГК РФ). В ряде случаев применительно к электронной коммерции оферентом будет выступать именно потребитель, поскольку от его волеизъявления зависит определение существенных условий договора (наименование и количество товара и т.п.), а также от него исходит намерение заключить договор, которое акцептуется принятием размещенного заказа предпринимателем. Что же касается рекламы, то по общему правилу информация о производимых или реализуемых товарах, размещенная на официальном сайте производителя или продавца данных товаров, а также на страницах производителя или продавца данных товаров в социальных сетях в Интернете, если указанные сведения предназначены для информирования посетителей сайта или соответствующей страницы в социальной сети об ассортименте товаров, условиях их приобретения, ценах и скидках, правилах пользования, не является рекламой[1].

Таким образом, обстоятельства, указанные в подп. 1 п. 1 ст. 1212 ГК РФ, далеко не всегда имели место применительно к электронной коммерции. Однозначно определить место получения заказа при его размещении в сети Интернет для целей подп. 2 п. 1 ст. 1212 ГК РФ также было в большинстве случаев невозможно. А обстоятельства подп. 3 п. 1 ст. 1212 ГК РФ и вовсе являлись «экзотикой» для электронной коммерции. В связи с этим можно констатировать, что в отсутствие расширительного «творческого» толкования данных положений правоприменительными органами применять их на практике к отношениям в сфере электронной коммерции было практически невозможно. А следовательно, довольно проблематично защитить права потребителя по договору, который заключен посредством сети Интернет с иностранным контрагентом-предпринимателем и в котором содержалась оговорка об иностранном применимом праве, лишающая потребителя ряда гарантий и прав, доступных ему «дома».

[1] Письмо ФАС России от 13 сентября 2012 г. № АК/29977 // СПС «КонсультантПлюс».

В связи с этим можно всячески поддержать изменения, внесенные в п. 1 ст. 1212 ГК РФ, согласно которым выбор права, подлежащего применению к договору, стороной которого является потребитель, не может повлечь за собой лишение потребителя защиты его прав, предоставляемой императивными нормами права страны места его жительства, если контрагент потребителя (профессиональная сторона) осуществляет свою деятельность в стране места жительства потребителя либо любыми способами *направляет свою деятельность* на территорию такой страны или нескольких стран, включая территорию страны места жительства потребителя, при условии, что договор связан с такой деятельностью профессиональной стороны.

Положения ст. 1212 ГК РФ не означают, впрочем, невозможности выбора сторонами потребительского договора применимого права и недействительности оговорки о применимом праве с последующим механическим применением норм законодательства о защите прав потребителей, существующих в стране места жительства потребителя. Просто при наличии такой оговорки о применимом праве нормы страны места жительства потребителя становятся своего рода надстройкой к договорному статуту, определенному такой оговоркой и обеспечивают гарантированный минимум прав потребителя. Как отмечает А.В. Асосков, конструкция ст. 1212 ГК РФ позволяет суду выбрать, применение норм какого правопорядка приводит к наиболее благоприятному для потребителя результату, причем принимая во внимание весь комплекс императивных норм договорного права, потенциально применимых к отношениям с участием потребителей, а не только узконаправленные нормы собственно потребительского законодательства[1]. Например, если право, применимое к договору, допускает возможность немотивированного отказа от договора в течение 14 дней, а российское право – в течение только 7 дней, то для российского потребителя в этой части будет более благоприятным применение иностранного права и его применение не будет противоречить ст. 1212 ГК РФ.

Если же потребительский договор не содержит условия о применимом праве, то при наличии обстоятельств, указанных в п. 1 ст. 1212 ГК РФ (направленной деятельности профессиональной стороны), к такому договору применяется право страны места жительства потребителя. Если же договор был заключен лицом, имеющим статус потребителя в отсутствие направленной деятельности профессиональной стороны на территорию его места жительства, применимое право определяется по общим правилам ст. 1211 ГК РФ.

[1] *Асосков А.В.* Указ. соч. С. 174.

Право, применимое к деликтным обязательствам

По общему правилу к обязательствам, возникающим вследствие причинения вреда, применяется право страны, где имело место действие или иное обстоятельство, послужившее основанием для требования о возмещении вреда. В случае когда в результате такого действия или иного обстоятельства вред наступил в другой стране, может быть применено право этой страны, если причинитель вреда предвидел или должен был предвидеть наступление вреда в этой стране (ст. 1219 ГК РФ). Однако если обе стороны обязательства, возникшего вследствие причинения вреда, имеют место жительства или основное место деятельности, применяется право страны, гражданами или юридическими лицами которой являются стороны обязательства. Факт причинения или наступления вреда на территории другой страны в таких случаях не имеет значения для выбора применимого права.

Статья 1220 ГК РФ очерчивает сферу действия права, подлежащего применению к обязательствам, возникшим вследствие причинения вреда (деликтного статута). Им определяются, в частности:

1) способность лица нести ответственность за причиненный вред; 2) возложение ответственности за вред на лицо, не являющееся причинителем вреда; 3) основания ответственности; 4) основания ограничения ответственности и освобождения от нее; 5) способы возмещения вреда; 6) объем и размер возмещения вреда. При этом перечень не является исчерпывающим. В соответствии с правом, применимым к обязательству, может определяться, например, степень вины потерпевшего и причинителя вреда.

Что следует считать под местом совершения действия, выступившего основанием для требования о возмещении вреда применительно к отношениям в сети Интернет? Здесь возможно несколько вариантов: 1) место нахождения оборудования (сервера), посредством которого было совершено вредоносное деяние; 2) место нахождения компьютера, с использованием которого была отправлена информация на сервер причинителем вреда (что будет совпадать с местонахождением делинквента в момент совершения вредоносного деяния). Оба варианта являются малопригодными в отношении сети Интернет, так как, с одной стороны, их установление сопряжено со значительными трудностями, а с другой стороны, подобные привязки носят слишком «случайный» характер в условиях высокой динамики отношений, связанных с размещением информации в сети Интернет. К тому же, поскольку оба вышеуказанных варианта связаны с высокой степенью зависимости от действий делинквента, это создает условия для недобросовестных

действий с его стороны по выбору благоприятного *для него* права. В связи с этим сложно согласиться с С.А. Бабкиным, предлагающим считать наиболее целесообразным в качестве места причинения вреда именно место нахождения оконечного устройства (компьютера), с которого производится помещение в сеть либо рассылка вредоносных программ или информации, порочащей честь, достоинство и деловую репутацию[1]. При этом упускается из внимания, что определить такое местонахождение (а вместе с ним – и применимое право) в условиях, когда размещение информации осуществлялось с ноутбука, а главное, доказать его с использованием допустимых в понимании российских судов доказательств – задача практически нереальная.

Более приемлемым вариантом представляется использование другого положения ст. 1219 ГК РФ, согласно которому «в случае, когда в результате такого действия или иного обстоятельства вред наступил в другой стране, может быть применено право этой страны, если причинитель вреда предвидел или должен был предвидеть наступление вреда в этой стране». Данный подход более благоприятен для потерпевшего: он нейтрализует возможные попытки делинквента выбрать удобное для него право путем манипуляций со своим местонахождением либо местонахождением сервера, а также данный подход гораздо проще с точки зрения определения применимого права и его содержания. Учитывая техническую специфику сети Интернет, есть основания для применения презумпции о том, что в силу общедоступности ее ресурсов лицо, размещающее информацию в данной сети, должно было предвидеть возможность наступления вреда в любой стране, где Интернет является потенциально доступным[2].

В требованиях, связанных с защитой чести, достоинства и деловой репутации, применение данного подхода влечет синхронизацию юрисдикции и применимого права в случаях, когда российский истец предъявляет иск в российский суд в связи с распространением в сети Интернет информации, порочащей его честь, достоинство и деловую репутацию (подп. 9 п. 3 ст. 402 ГПК РФ, подп. 6 п. 1 ст. 247 АПК РФ). В таком случае со ссылкой на вышеупомянутое положение ст. 1219 ГК РФ суд может применять российское право, так как всегда можно утверждать о том, что лицо, разместившее подобную информацию в сети Интернет, могло предполагать возможность причинения ею вреда в стране, где проживает или располагается потерпевший

[1] См.: *Бабкин С.А.* Право, применимое к отношениям, возникающим при использовании сети «Интернет»: Основные проблемы. С. 50.

[2] Там же. С. 51.

(вспомним приведенное ранее австралийское дело *Dow Jones & Co. Inc. v. Gutnik*).

Следует отметить, что ст. 1219 ГК РФ претерпела некоторые изменения, которые могут иметь интерес в контексте электронной коммерции. В частности, если обязательство, возникающее вследствие причинения вреда, тесно связано с договором, заключенным в ходе осуществления предпринимательской деятельности, применяется право, которое регулирует соответствующий договор. Данная норма может иметь определенное значение для случаев недобросовестной конкуренции, при которой затронуты исключительно права потерпевшего[1], использования объектов интеллектуальной собственности в сети Интернет с нарушением условий лицензионных договоров (внедоговорное использование). Однако вопросы, связанные с определением права, применимого к отношениям, связанным с интеллектуальной собственностью и осложненным иностранным элементом, на практике обычно гораздо сложнее.

В силу п. 2 ст. 1231 ГК РФ при признании исключительного права на результат интеллектуальной деятельности или на средство индивидуализации в соответствии с международным договором Российской Федерации содержание права, его действие, ограничения, порядок его осуществления и защиты определяются ГК РФ независимо от положений законодательства страны возникновения исключительного права, если таким международным договором или настоящим Кодексом не предусмотрено иное.

Данное правило отражает принцип территориальности действия исключительных прав. Как отмечает В. Канашевский, «общим для авторских, смежных и промышленных прав является то, что они носят строго территориальный характер, то есть признаются и защищаются только на территории того государства, где они впервые возникли – опубликованы, зарегистрированы. Территориальный характер действия таких прав исключает коллизионный вопрос»[2]. Данная позиция является достаточно традиционной для российского права[3].

---

[1] В противном случае будет применяться специальная коллизионная норма, в соответствии с которой к обязательствам, возникающим вследствие недобросовестной конкуренции, применяется право страны, рынок которой затронут или может быть затронут такой конкуренцией, если иное не вытекает из закона или существа обязательства (ст. 1222 ГК РФ). О видах недобросовестной конкуренции см. ст. 14 Федерального закона от 26 июля 2006 г. № 135-ФЗ «О защите конкуренции» (далее – Закон о защите конкуренции).

[2] *Канашевский В.А.* Международное частное право: учебник. М.: Международные отношения, 2006. С. 458–459.

[3] См., например: *Лунц Л.А.* Курс международного частного права. Особенная часть. 2-е изд., перераб. и доп. М., 1975. С. 383

Таким образом, большинство элементов, составляющих правовой режим объекта интеллектуальной собственности, определяются в соответствии с нормами российского права (главным образом части четвертой ГК РФ) независимо от положений законодательства страны возникновения исключительного права. Исключением из данного правила являются следующие случаи.

Так, в соответствии с п. 3 ст. 1256 ГК РФ автор или иной первоначальный правообладатель произведения определяется по закону государства, на территории которого имел место юридический факт, послуживший основанием для приобретения авторских прав (*lex originis*). Если произведение, скажем, было создано на территории США в рамках трудовых отношений, для определения личности правообладателя необходимо обратиться к законодательству США. Согласно § 201 (*b*) Закона США об авторском праве в отношении произведений, созданных по найму (*work for hire*), автором в силу закона (*statutory author*) является работодатель. Следует подчеркнуть, что в данном случае речь идет именно о возникновении *первоначального* авторского права у работодателя, а не о переходе к нему изначально возникшего у работника авторского права[1]. А вот особые сроки действия исключительных прав на произведения, созданные по найму, установленные в § 302 (*c*) Закона об авторском праве США, – 95 лет с момента первой публикации или 120 лет с момента создания в зависимости от того, какой срок истекает раньше, – не подлежат применению на территории Российской Федерации. Вместо них в соответствии с п. 2 ст. 1231 ГК РФ применяется срок, установленный в ст. 1281 ГК РФ.

В литературе отмечается, что положения п. 3 ст. 1256 ГК РФ применяются не только в случаях, когда охрана произведению предоставляется на основании международных договоров Российской Федерации иностранным лицам, но и в случаях, когда произведения создаются российскими гражданами за рубежом. В отношении таких произведений авторы или первоначальные правообладатели определяются по закону того государства, где они проживают или работают[2]. Текст п. 3 ст. 1256 ГК РФ не дает оснований для такого вывода. Напротив, как следует из подп. 2 п. 1 ст. 1256 ГК РФ, исключительное право на произведения, обнародованные за пределами территории Российской Федерации или не обнародованные, но находящиеся в какой-либо

[1] *Progoff S., Halpern M., Feinberg I.* Understanding the Intellectual Property License. Practicing Law Institute. 2004. P. 613.

[2] *Гаврилов Э.* Решение вопросов международного частного права в части четвертой Гражданского кодекса Российской Федерации // Хозяйство и право. 2008. № 3.

объективной форме за пределами территории Российской Федерации, признается за авторами, являющимися гражданами Российской Федерации. Как видно, в данном случае одного факта наличия у автора российского гражданства достаточно для применения российского закона. Как отмечает А.Л. Маковский, российский ГК в принципе (хотя, вопреки распространенному мнению, все же не абсолютно) исключает действие на территории России иностранного права, регламентирующего исключительные права, если только возможность применения иностранного права не вытекает из международного договора Российской Федерации[1]. Таким образом, анализ вопросов принадлежности исключительного права российскому автору или его зарубежному работодателю должен осуществляться по нормам ГК РФ (ст. 1295).

Проект изменений в ГК РФ предлагает включить в разд. VI ГК РФ ст. 1207[2], специально посвященную статуту права интеллектуальной собственности[2]:

«1. *Если иное не предусмотрено законом, исключительные права на результаты интеллектуальной деятельности и средства индивидуализации юридических лиц, товаров, работ, услуг и предприятий определяются по праву страны, в отношении которой испрашивается охрана соответствующего исключительного права.*

2. Правом, подлежащим применению к исключительным правам, определяются, в частности:

1) охраняемые результаты интеллектуальной деятельности и средства индивидуализации;

2) виды исключительных прав;

3) содержание исключительных прав;

4) ограничения исключительных прав;

5) действие исключительных прав;

6) осуществление исключительных прав, в том числе допустимые способы распоряжения исключительными правами;

7) внедоговорные способы защиты исключительных прав».

По сути, предлагаемая статья выполняет те же функции, что и ныне действующая ст. 1231 ГК РФ, однако прямо закрепляет принцип *lex loci protectionis* – применения права страны, где испрашивается охрана. Таким образом, если нарушение исключительного права произошло

[1] См.: Комментарий к части четвертой Гражданского кодекса Российской Федерации (поглавный) / под ред. А.Л. Маковского. М., 2008. С. 305.

[2] Пока данная статья не была принята в составе иных поправок в части третьей ГК РФ. Не исключено, что это связано с ее тесной связью с положениями части четвертой ГК РФ, поправки к которой еще не приняты.

на территории России, то подлежит применению российское право. Если нарушение исключительного права произошло на территории России, Германии и Украины, то в случае рассмотрения спора в российском суде (например, по причине того, что ответчик является российским гражданином) суд должен будет применить право каждого из указанных государств к каждому факту нарушения. В случае если нарушение исключительного права было совершено в сети Интернет, данное правило является явно неудобным, поскольку будет вынуждать суд устанавливать содержание и применять право многих зарубежных государств в отношении одного и того же факта нарушения. К сожалению, предлагаемая редакция ст. 1207[2] никак не учитывает этот факт, впрочем, как и специфику сети Интернет в принципе.

4.3. Принудительное исполнение иностранного судебного решения в России (jurisdiction to enforce)

Условия и порядок признания и принудительного исполнения иностранных судебных решений на территории Российской Федерации регламентируются АПК РФ и ГПК РФ.

В соответствии с ч. 1 ст. 241 АПК РФ решения судов иностранных государств, принятые ими по спорам и иным делам, возникающим при осуществлении предпринимательской и иной экономической деятельности, признаются и приводятся в исполнение в России арбитражными судами, если признание и приведение в исполнение таких решений предусмотрены международным договором Российской Федерации и федеральным законом. Схожая норма содержится и в ч. 1 ст. 409 ГПК РФ. Далеко не со всеми странами Российская Федерация имеет международные договоры о взаимном признании и приведении в исполнение судебных решений[1]. Некоторые суды достаточно формально подходят к данному вопросу и рассматривают отсутствие международного соглашения как безусловное основание для отказа при признании и принудительном исполнении иностранного судебного решения. Так, например, по причине отсутствия такого договора Арбитражный суд г. Москвы отказал в признании и принудительном исполнении решения израильского суда[2]. Аналогичная судьба постигла и решение американского суда[3].

---

[1] Актуальный перечень существующих двусторонних международных соглашений по вопросам правовой помощи с участием России можно найти на сайте МИД России по ссылке www.mid.gov.ru

[2] Определение ВАС РФ от 19 мая 2008 г. № 5105/08 по делу № А40-73830/06-25-349.

[3] Постановление ФАС Московского округа от 17 февраля 2009 г. № КГ-А40/12786-08-П по делу № А40-7480/08-68-127.

Однако не все суды разделяют столь формальный подход. Нередко признание и принудительное исполнение иностранных судебных решений возможно на основании принципов взаимности и международной вежливости, которые являются общепризнанными принципами международного права, а следовательно, – составной частью правовой системы Российской Федерации (ч. 4 ст. 15 Конституции РФ). Так, в Определении Судебной коллегии по гражданским делам Верховного Суда РФ от 7 июня 2002 г. № 5-Г02-64 было отмечено следующее: «ходатайство о признании и исполнении иностранного судебного решения может быть удовлетворено компетентным российским судом и при отсутствии соответствующего международного договора, если на основе взаимности судами иностранного государства признаются решения российских судов».

Некоторые арбитражные суды также разделяют данную позицию. Так, в одном из споров ключевую роль сыграл подтвержденный документально факт признания и приведения в исполнение решений российских судов в Королевстве Нидерланды, что, по мнению суда, «является безусловным основанием для признания и приведения в исполнение в Российской Федерации решений нидерландских судов на основании общепризнанных принципов международного права – принципов взаимности и международной вежливости»[1]. В отсутствие доказательств, подтверждающих факт исполнения российских судебных решений на территории иностранного государства, суд которого вынес соответствующее решение, ссылки на принцип взаимности, скорее всего, не будут приняты во внимание[2].

Представляется, что основной смысл во введении концепции взаимности как условия признания и приведения в исполнение иностран-

[1] Определение ВАС РФ от 7 декабря 2009 г. № ВАС-13688/09 по делу № А41-9613/09.

[2] Постановление ФАС Московского округа от 17 февраля 2009 г. № КГ-А40/12786-08-П по делу № А40-7480/08-68-127: «Наличие соответствующего международного договора является обязательным условием для признания и приведения в исполнение иностранного судебного решения на территории РФ. Между тем такой договор между Российской Федерацией и Соединенными Штатами Америки отсутствует. Кроме того, заявителем не представлено доказательств следования судами США международному принципу взаимности в вопросе исполнения российских судебных решений». Постановления ФАС Московского округа от 19 октября 2005 г., 12 октября 2005 г. № КГ-А40/8581-05-П: «между Россией и ФРГ или Германией международный договор о правовой помощи, федеральный закон отсутствуют. Следуя принципам международной вежливости и международной взаимности при рассмотрении заявления в отсутствие международного договора России и федерального закона, арбитражный суд проверил, исполнялись ли подобные решения российских судов на территории указанных государств. Таких сведений арбитражным судом получено не было».

ных судебных решений заключается все же не в том, чтобы осложнить жизнь истцу, а в том, чтобы создавать стимулы для иностранных государств в свою очередь также признавать и исполнять иностранные судебные решения. Исходя из этого не следует бояться сделать первый шаг и поступить с другим так, как хотел бы, чтобы поступали с тобой. Поэтому в отсутствие доказательств того, что законодательство иностранного государства не позволяет признавать и приводить в исполнение российские судебные решения, либо ссылок на случаи, когда суды такого государства не признали российское судебное решение, отказ в признании и приведении в исполнение судебного решения такого иностранного государства вряд ли будет соответствовать духу требования взаимности.

Если суд установит наличие международного договора или взаимности и признает тем самым наличие возможности признания судебного решения, исходящего из данного государства, он должен также проверить отсутствие установленных в законе оснований для отказа в принудительном исполнении такого иностранного решения. Соответствующие основания в виде исчерпывающего перечня содержатся в ст. 412 ГПК РФ и ст. 244 АПК РФ. К ним относятся случаи, когда:

1) решение по закону государства, на территории которого оно принято, не вступило в законную силу. Российский суд не обязан придавать иностранному судебному решению бóльшую силу, чем та, которая имеет место быть на территории страны, где оно было вынесено;

2) сторона, против которой принято решение, не была своевременно и надлежащим образом извещена о времени и месте рассмотрения дела или по другим причинам не могла представить в суд свои объяснения. В частности, суд при рассмотрении вопроса об извещении стороны, против которой принято решение, проверяет, не была ли она лишена возможности защиты в связи с отсутствием фактического и своевременного извещения о времени и месте рассмотрения дела. Если российский суд установит, что уведомление о месте и времени судебного разбирательства в иностранном суде была направлено по иному адресу, чем тот, который был указан в договоре (в отсутствие доказательств его последующего изменения), в признании иностранного решения может быть отказано[1];

[1] Пункт 6 информационного письма Президиума ВАС РФ от 22 декабря 2005 г. № 96 «Обзор практики рассмотрения арбитражными судами дел о признании и приведении в исполнение решений иностранных судов, об оспаривании решений третейских судов и о выдаче исполнительных листов на принудительное исполнение решений третейских судов».

3) рассмотрение дела в соответствии с международным договором Российской Федерации или федеральным законом относится к исключительной компетенции суда в Российской Федерации;

4) имеется вступившее в законную силу решение суда в Российской Федерации, принятое по спору между теми же лицами, о том же предмете и по тем же основаниям. В таких случаях признание и приведение в исполнение на территории Российской Федерации решения иностранного арбитража приведут к существованию на территории Российской Федерации судебных актов равной юридической силы, содержащих взаимоисключающие выводы, и вступят в противоречие с принципом обязательности судебных актов российского суда[1];

5) на рассмотрении суда в Российской Федерации находится дело по спору между теми же лицами, о том же предмете и по тем же основаниям, производство по которому возбуждено до возбуждения производства по делу в иностранном суде, или суд в Российской Федерации первым принял к своему производству заявление по спору между теми же лицами, о том же предмете и по тем же основаниям. Данную норму можно рассматривать в качестве аналога правила *lis pendens*, которое принято в европейских странах и которое направлено на избежание параллельных судебных разбирательств по одному и тому же спору с возможностью последующего существования несовместимых судебных решений;

6) истек срок давности приведения решения иностранного суда к принудительному исполнению и этот срок не восстановлен арбитражным судом;

7) исполнение решения иностранного суда противоречило бы публичному порядку Российской Федерации.

Как видно, большинство оснований, указанных в данном перечне, носят процессуальный характер. Неверное определение применимого права или неверное применение применимого материального права иностранным судом не является по общему правилу основанием для отказа в признании и принудительном исполнении иностранного судебного решения, если только такое решение не нарушает публичного порядка Российской Федерации, о котором следует сказать несколько подробнее.

Российское законодательство не содержит дефиниции публичного порядка[2]. По мнению Верховного Суда РФ, под публичным порядком

---

[1] См., например: постановление ФАС Уральского округа от 29 декабря 2003 г. по делу № А71-288/2002-Г10.

[2] Подробный обзор существующих в доктрине и судебной практике точек зрения по данному вопросу см.: *Богатина Ю.Г.* Оговорка о публичном порядке в международном частном праве: теоретические проблемы и современная практика. М., 2010.

Российской Федерации понимаются основы общественного строя России. Оговорка о публичном порядке возможна лишь в тех отдельных случаях, когда применение иностранного закона могло бы породить результат, недопустимый с точки зрения российского правосознания[1]. При этом Верховный Суд РФ признал неправильным вывод Московского городского суда о противоречии решения МКАС публичному порядку Российской Федерации лишь на том основании, что это решение не соответствует законодательству Российской Федерации.

Схожей позиции придерживаются и арбитражные суды. Так, ВАС РФ разъяснил, что под публичным порядком понимаются фундаментальные правовые начала (принципы), которые обладают высшей императивностью, универсальностью, особой общественной и публичной значимостью, составляют основу построения экономической, политической, правовой системы государства. К таким началам, в частности, относится запрет на совершение действий, прямо запрещенных сверхимперативными нормами законодательства Российской Федерации (ст. 1192 ГК РФ), если этими действиями наносится ущерб суверенитету или безопасности государства, затрагиваются интересы больших социальных групп, нарушаются конституционные права и свободы частных лиц[2]. Оценка арбитражным судом последствий исполнения иностранного судебного решения на предмет нарушения публичного порядка Российской Федерации не должна вести к его пересмотру по существу (п. 4 ст. 243 АПК РФ). Важнейшим следствием запрета пересмотра иностранного судебного решения по существу является отсутствие у судьи, решающего вопрос о его признании и приведении в исполнение, полномочий по оценке обоснованности судебного решения как в вопросах факта, так и в вопросах права.

Сам факт отсутствия в российском законодательстве норм, аналогичных тем, которые были применены иностранным судом при разрешении спора, не означает нарушения публичного порядка Российской Федерации вследствие приведения в исполнение такого решения на территории Российской Федерации. Наличие в договоре, по спору из которого было вынесено иностранное судебное решение, обязательств и мер ответственности, нехарактерных для российской право-

[1] Определения Судебной коллегии по гражданским делам Верховного Суда РФ от 25 сентября 1998 г. по делу № 5-Г98-60.

[2] Информационное письмо Президиума ВАС РФ от 26 февраля 2013 г. № 156 «Обзор практики рассмотрения арбитражными судами дел о применении оговорки о публичном порядке как основания отказа в признании и приведении в исполнение иностранных судебных и арбитражных решений» (п. 1).

вой системы, или с несколько иным содержанием, нежели принятым в Российской Федерации, например заранее оцененных убытков (*liquidated damages*) или гарантий и заверений (*representations and warranties*), не противоречит по общему правилу публичному порядку Российской Федерации[1]. Однако, если иностранное судебное решение вынесено с нарушением принципа соразмерности мер гражданско-правовой ответственности, являющегося основополагающим принципом российского права, и взысканные меры ответственности имеют тем самым карательный характер, в признании и принудительном исполнении такого иностранного судебного решения может быть отказано со ссылкой на его противоречие публичному порядку Российской Федерации.

По итогам рассмотрения дела о признании и приведении в исполнение иностранного решения суд выносит определение по правилам, установленным для принятия решения. В нем должны быть указаны установленные фактические обстоятельства дела; доказательства, на которых основаны выводы суда об обстоятельствах дела, и доводы в пользу итогового вывода по делу; мотивы, по которым суд отверг те или иные доказательства, принял или отклонил приведенные в обоснование своих требований и возражений доводы лиц, участвующих в деле; законы и иные нормативные правовые акты, которыми руководствовался суд при принятии определения, и мотивы, по которым суд не применил законы и иные нормативные правовые акты, на которые ссылались лица, участвующие в деле.

Таким образом, основным препятствием для признания и приведения в исполнение иностранного судебного решения, принятого по спору в сфере электронной коммерции, является возможное отсутствие международного договора между Россией и государством, на территории которого было принято такое решение, и обусловленные этим сложности доказывания взаимности. В случае успешного прохождения данного барьера перечень возможных оснований для отказа российского суда в признании и принудительном исполнении такого решения крайне узок. Судья не вправе ставить под сомнение ни установленные иностранным судом факты, ни осуществленную им юридическую квалификацию спорных отношений. Российский судья должен лишь проверить, не является ли признание и приведение в исполнение резолютивной части иностранного решения противоречащим фундаментальным принципам национального правопорядка.

[1] Пункт 5 Информационного письма Президиума ВАС РФ от 26 февраля 2013 г. № 156.

Если попытаться представить себе такие ситуации, то, представляется, что в зоне риска могут оказаться случаи, при которых исполнение иностранного решения может вступать в противоречие с антимонопольным законодательством Российской Федерации; ситуации, когда иностранный суд присудит штрафные убытки, размер которых явно несоразмерен характеру нарушения, тем самым придав мерам гражданско-правовой ответственности карательный характер вместо компенсационного. Но в подавляющем большинстве случаев решения иностранных судов по спорам в сфере электронной коммерции вряд ли будут хоть как-то противоречить публичному порядку Российской Федерации. Главное, что сам по себе выбор иностранного права и места рассмотрения спора, в том числе по причине недоверия к российскому праву или правосудию, не может рассматриваться в качестве нарушения публичного порядка.

§ 5. Международное сотрудничество по вопросам юрисдикции в сети Интернет

Трансграничный характер сети Интернет приводит многих авторов к выводу о целесообразности регулирования вопросов юрисдикции на международном уровне. В частности, предлагается заключение международного договора, которое определяло бы применимую юрисдикцию к деятельности, связанной с использованием Интернета, фиксировало бы соответствующие коллизионные нормы для определения применимого права или даже содержало бы унифицированные правила по отдельным вопросам[1].

Кроме того, представлены и более радикальные позиции о необходимости разработки и принятии международной конвенции, которая установила бы зоны национальной юрисдикции в Интернете по аналогии с Арктикой, космическим пространством, Луной, другими небесными телами[2]. По мнению сторонников данного подхода, Интернет фактически является особой информационной зоной мира и сотруд-

[1] *Наумов В.Б.* Право и Интернет: Очерки теории и практики. М., 2003. С.16; *Калятин В.О.* Проблемы установления юрисдикции в Интернете // Законодательство. 2001. № 5. С. 42; *Глушков А.В.* Проблемы правового регулирования интернет-отношений: автореф. дис. ... канд. юрид. наук. СПб., 2007. С. 6; *Рассолов И.М.* Право и Интернет. Теоретические проблемы. 2-е изд., доп. М., 2009; *Незнамов А.В.* Особенности компетенции по рассмотрению интернет-споров / науч. ред. В.В. Ярков. М., 2011. § 3.3.

[2] См., например: *Menthe D.* Jurisdiction In Cyberspace: A Theory of International Spaces // Mich. Telecomm. Tech. L. Rev. 69. 1998. 4. www.mttlr.org/html/volume_four.html/menthe.html; *Дашян М.С.* Право информационных магистралей (*Law of Information Highways*): вопросы правового регулирования в сфере Интернет. М., 2007. С. 86.

ничества, находящейся вне пределов географического пространства, и общечеловеческим наследием. Глобальный характер предлагаемых для сопоставления объектов (Антарктика, космическое пространство и т.д.) и сферы Интернета предполагает, по их мнению, возможность использования схожих подходов к их правовому регулированию[1].

Не отрицая определенную теоретическую ценность данных предложений, приходится констатировать, что на практике перспективы принятия подобных международных соглашений крайне невелики. Процесс принятия директив и регламентов в Европейском союзе наглядно демонстрирует всю сложность попыток договориться по отдельным, не самым принципиальным вопросам даже членам, принадлежащим к одной группе государств. Чем более амбициозным и унифицирующим будет подобное соглашение, тем меньше потенциальных участников из категории «развитых» и прочих стран будут готовы к нему присоединиться.

Правда, отдельные успехи на почве создания международных инструментов, которые могли бы иметь непосредственное значение для решения существующих проблем в области интернет-юрисдикции, все же имеются.

Одним из важнейших шагов в данной области является принятие 30 июня 2005 г. на XX заседании Гаагской конференции по международному частному праву Гаагской конвенции в отношении соглашений о выборе суда (*Hague Convention on Choice of Court Agreements*). Предложение о включении в повестку дня Гаагской конференции по международному частному праву вопроса о разработке конвенции о признании и принудительном исполнении иностранных судебных решений поступило от США еще в 1992 г. Европейские страны поддержали данное предложение, будучи заинтересованными в ограничении юрисдикции американских судов в отношении иностранных лиц. Однако, как по-

[1] Представляется, что аналогии в данном случае проводить нельзя, так как ситуации принципиально различны. Территории Арктики и космическое пространство в достаточной степени обособлены от территорий отдельно взятых государств, чтобы не препятствовать последним осуществлять полноценную регулятивную и судебную функции на своей территории. То, что происходит в Арктике, если и влияет, то весьма мало на то, что происходит в большинстве стран (возможные экологические катастрофы не в счет). Поэтому договориться по вопросу правового режима таких территорий гораздо проще, нежели по вопросам правового режима Интернета как некоего «интернационального пространства», поскольку в последнем случае отношения, возникающие в нем, слишком «вплетены» в отношения, подпадающие под юрисдикцию отдельно взятых государств, что слишком остро ставит вопрос о суверенитете государства. Интернет слишком важен, чтобы ограничить свой суверенитет в пользу международных соглашений и отказаться от возможности одностороннего воздействия на него со стороны отдельно взятого государства в соответствии со своим пониманием национальных интересов.

казала практика работы над данным документом, задача оказалась чересчур амбициозной для своего времени. Достаточно сложно найти консенсус по столь чувствительным вопросам, связанным с национальным суверенитетом, как признание на своей территории иностранных судебных решений. Проблема усложнялась и существующими различиями между подходами стран общего и континентального права, а также повсеместным распространением электронных коммуникаций с различными мнениями относительно необходимости создания в отношении них специальных правил[1]. В итоге сфера Конвенции сузилась и стала охватывать лишь вопросы признания и приведения в исполнение судебных решений, вынесенных судами, указанными в пророгационных соглашениях между предпринимателями (*B2B*).

Конвенция открыта для подписания всеми государствами и вступает в силу в первый день месяца, следующего по истечении трех месяцев после представления второго документа, удостоверяющего ее ратификацию, принятие, утверждение или присоединение. По состоянию на 1 мая 2013 г. данная Конвенция была подписана со стороны США, Европейского союза и Мексики[2] и пока не вступила в силу[3].

Гаагская конвенция применяется исключительно к предпринимательским договорам (*B2B*) и не распространяется на потребительские договоры. По своей функциональной направленности Конвенция выполняет функции, сходные с Нью-Йоркской конвенцией 1958 г. о признании и приведении в исполнение иностранных арбитражных решений, однако по сравнению с ней является более современной, поскольку допускает действительность соглашений о выборе суда в электронной форме, в том числе в форме *click-wrap*-соглашений[4].

Конвенция особым образом регламентирует сферу своего действия в отношении споров, связанных с объектами интеллектуальной собственности, что представляет особый интерес в контексте тематики оборота цифрового контента в сети Интернет. Так, из-под сферы действия Конвенции изъяты споры, связанные с 1) действительностью исключительных прав на объекты интеллектуальной собственности,

[1] *Schulz A.* The 2005 Hague Convention on Choice of Court Clauses // ILSA Journal of International and Comparative Law. No 12. 2006. P. 433–434.

[2] Текст Конвенции на английском языке: http://www.hcch.net/index_en.php?act=conventions.text&cid=98

[3] Статус Конвенции можно проследить на официальном сайте Гаагской конференции по международному частному праву по ссылке: www.hcch.net/index_en.php?act=conventions.status&cid=98

[4] См.: *Faye Fangrei Wang.* Internet Jurisdiction and Choice of Law: Legal Practices in the EU, US and China. P. 20.

за исключением случаев, когда речь идет об авторских и смежных правах; 2) нарушением исключительных прав, за исключением случаев, когда оно связано с нарушением договора, касающегося предоставления таких прав. Таким образом, Конвенция может быть применима к спорам, связанным с нарушениями порядка использования объекта интеллектуальной собственности, предоставленного на основании лицензионного договора, несмотря на тот факт, что такие споры могут сами по себе носить деликтный (внедоговорный характер). Отсутствуют препятствия и для заключения предварительных или последующих соглашений об исключительной подсудности споров, связанных с действительностью авторских или смежных прав либо их нарушением, в том числе и в случаях, когда оно не сопряжено с нарушением лицензионного или иного договора. Это связано с тем, что авторские и смежные права не требуют регистрации, и основания для установления исключительной юрисдикции судов государства, в котором была произведена регистрация, в таких случаях отсутствуют. Поскольку именно права на объекты авторских и смежных прав выступают одним из наиболее распространенных видов «товара» в сфере электронной коммерции, применение к данным отношениям положений рассматриваемой Конвенции будет означать легитимизацию содержащихся в различного рода лицензионных договорах и правилах продажи соглашений об исключительной подсудности. Однако для этого необходимо, чтобы такие соглашения не только подпадали под сферу действия Конвенции, но и отвечали определенным требованиям.

В соответствии со ст. 3 Конвенции под соглашением об исключительной подсудности понимается *заключенное двумя или более лицами соглашение, отвечающее требованиям п. «c» и определяющее в качестве компетентных для рассмотрения возникших или потенциальных споров, связанных с определенным правоотношением суды в одном из договаривающихся государств либо один или несколько конкретных судов одного из договаривающихся государств при исключении юрисдикции любых иных судов*. Пункт «*c*» в свою очередь предусматривает, что соглашение должно быть заключено или оформлено в письменном виде или иным способом, который делает информацию доступной, способом, обеспечивающим возможность ее последующего использования. Указанное положение было заимствовано из ст. 6 Типового закона ЮНСИТРАЛ «Об электронной торговле» и направлено на обеспечение возможности заключения соглашений об исключительной подсудности в электронной форме (в частности, путем обмена электронными сообщениями или принятия условий *click-wrap*-соглашения).

Таким образом, для того чтобы пророгационное соглашение было действительным для целей применения Конвенции, оно должно удовлетворять пяти условиям:

1) наличие соглашения между двумя или более лицами, соответствующего требованиям формы;

2) такое соглашение должно указывать в качестве компетентных либо суды определенного государства в общем (например, суды США), либо один или несколько *конкретных* судов такого государства (например, суд Южного Округа штата Нью-Йорк либо Федеральный окружной суд штата Калифорния и Федеральный окружной суд штата Нью-Йорк);

3) компетенция обозначенного суда (или судов) должна быть исключительной, т.е. из соглашения сторон явно не должно следовать, что такие споры могут быть рассмотрены иными судами (ст. 3 (*b*))[1];

4) обозначенные суды должны быть расположены в государстве – участнике Конвенции;

5) пророгационное соглашение должно быть привязано к конкретному правоотношению.

Данные условия должны иметь место в совокупности. Например, если условия соглашения предусматривают, что споры подлежат рассмотрению в судах Англии или США, то на такое соглашение не будут распространяться положения Конвенции, поскольку не выполнено условие 3 (суды должны быть расположены на территории одного государства – участника Конвенции).

Основные последствия заключения соглашения об исключительном выборе суда сводятся к следующим трем правилам, адресованным трем различным судам:

1) *указанный в соглашении сторон суд не имеет права отказать в установлении юрисдикции в отношении спора*, если только такое соглашение не является ничтожным в соответствии с *lex fori* (например, по причине отсутствия правоспособности, обмана, введения в заблуждение, принуждения и прочих порочащих соглашение фактов), а также не нарушает правил предметной юрисдикции[2], относящихся к такому

[1] Включение в Конвенцию презумпции исключительного характера соглашения о подсудности направлено на расширение сферы ее применения и гармонизацию существующих подходов в разных странах. См.: *Schulz A.* Op. cit. P. 436. Так, например, в США отсутствие прямого указания на исключительный характер пророгационного соглашения означает его неисключительность (см.: *Faye Fangrei Wang.* Internet Jurisdiction and Choice of Law: Legal Practices in the EU, US and China. P. 26).

[2] Следует подчеркнуть, что автономия воли сторон по заключению пророгационных соглашений не может изменить существующие правила процессуального законодатель-

суду (например, стороны обозначили в качестве компетентного суда мировой суд, которому возникший спор не подведомственен в принципе);

2) *все остальные суды должны воздерживаться от осуществления своей юрисдикции*, за исключением случаев, когда соглашение о выборе суда является ничтожным по законодательству страны суда, выбранного сторонами; отказ в рассмотрении спора противоречит публичному порядку и является явно несправедливым; выбранный сторонами суд отказался рассматривать дело;

3) *вынесенное компетентным судом решение подлежит признанию и принудительному исполнению иностранными судами*, за исключением случаев, когда соглашение о выборе суда является недействительным в соответствии с законодательством выбранного суда; у сторон отсутствовала правоспособность для заключения такого соглашения; судебное решение было получено с применением обмана; признание и принудительное исполнение судебного решения будет противоречить публичному порядку страны суда обращения; судебное решение несовместимо с судебным решением в отношении спора между теми же сторонами, ранее вынесенным судом в стране обращения либо судом иного государства, решение которого может быть исполнено в стране обращения.

Конвенция содержит в себе некоторые положения коллизионного права в части права, применимого к действительности соглашения об исключительной подсудности. Таким правом является право страны суда, выбранного сторонами. Таким образом, каждый из трех судов, потенциально вовлеченных в сферу действия Конвенции (компетентный суд, любой иной суд и суд, осуществляющий признание и принудительное исполнение решения), должен оценивать действительность такого соглашения по праву страны суда, выбранного сторонами, что направлено на минимизацию неопределенности и предотвращение ситуаций, когда соглашение является действительным по праву страны суда, выбранного сторонами, но является недействительным либо по праву иного суда, куда одна из сторон подала иск в нарушение условий пророгационного соглашения, либо по праву суда, приводящего иностранное решение в исполнение.

Несмотря на то что формально такой подход является отражением принципа автономии воли, он лишает слабую сторону договора тех защитных механизмов, которые может содержать его «родное» законодательство либо иное законодательство, связанное с отношением. К таким механизмам могут относиться не только традиционные по-

ства, касающиеся предметной юрисдикции, т.е. компетентности суда по рассмотрению споров соответствующего вида в принципе. См. ст. 5 (3) Конвенции.

ложения договорного права об ошибке, о введении в заблуждении, недолжном влиянии или насилии, но и специализированные механизмы контроля справедливости договора *ex post* (контроль над стандартными условиями, недобросовестными условиями и т.п.). Поскольку феномен слабой стороны не является исключительным достоянием лишь потребительских договоров, но имеет место и в договорах *B2B*, Конвенция во имя большей предсказуемости может осложнить жизнь предпринимателей со слабыми переговорными возможностями.

Возникает вопрос, насколько целесообразно России присоединяться к указанной Конвенции. С одной стороны, она дает формальные основания для признания на территории других государств – участников Конвенции судебных решений, вынесенных российскими судами, исключительной компетенции которых стороны подчинили свои споры. С другой стороны, смотря правде в глаза, вряд ли стоит ожидать, что таких случаев будет много: при прочих равных стороны (или хотя бы одна из них, представленная иностранной компанией) будут стремиться выбрать в качестве компетентного суда иностранный суд, а не российский. И чем больше будет вероятность признания такого решения на территории Российской Федерации, тем больше будет стимулов у сторон, чтобы выбрать именно иностранный суд. Таким образом, на практике присоединение России к Конвенции будет представлять собой «игру в одни ворота»: открытие своей территории для действия решений иностранных государств. Существует и еще один момент, на который следует обратить внимание. Как отмечалось ранее, вопросы действительности исключительного пророгационного соглашения решаются по праву страны суда. Возможность включения таких соглашений в договоры присоединения вроде *click-wrap*-соглашений в совокупности с выбором в качестве компетентного суда страны, формально и уважительно подходящей к вопросам свободы договора (вроде Англии или США), повлечет массовое навязывание российским участникам оборота иностранных судов с лишением их более-менее реальной возможности проведения переговоров по данному вопросу. Так что в целом положительно оценивая роль данной Конвенции в развитии электронной коммерции, представляется, что присоединение к ней возможно лишь с оговорками, позволяющими обеспечивать эффективную защиту российских участников оборота от навязывания им невыгодных пророгационных соглашений[1]. Возможно, осторожное

[1] Конвенция допускает возможность присоединяющегося государства сделать оговорку о неприменении отдельных положений Конвенции к определенным отношениям при наличии на то «серьезного интереса» (ст. 21).

отношение к Конвенции со стороны других стран, в частности Китая, Индии, Бразилии и других развивающихся стран, вызвано в том числе и этими соображениями[1].

Однако не только вопросы признания и принудительного исполнения решений иностранных судов стоят остро в контексте проблематики электронной коммерции. В ряде случаев необходима выработка принципиально иных подходов к юрисдикции в виде обеспечения возможности координации рассмотрения интернет-споров судами различных государств. Это особенно актуально применительно к спорам, возникающим в связи с совершением правонарушений в сети Интернет (нарушение исключительных прав, распространение диффамационных сведений и т.д.), но в принципе не исключено и при рассмотрении споров, возникших из нарушения условий договоров в сети Интернет, носящих массовый характер.

Принципы определения юрисдикции, применимого права и принудительного исполнения судебных решений в сфере интеллектуальной собственности, подготовленные Американским институтом права, содержат в себе модель возможного взаимодействия различных судов по вопросам так называемого повсеместного (*ubiquitous*) нарушения исключительных прав, которое имеет место в сети Интернет[2].

В таких случаях возникает целый ряд вопросов. Какой суд должен рассматривать спор? Каковы пределы его компетенции? Охватывают ли они нарушения, имевшие место на территории иностранных государств?

В целях упрощения процесса рассмотрения трансграничных споров и минимизации издержек, связанных с их рассмотрением, Принципы предлагают использовать механизм координации деятельности различных судебных инстанций в связи с рассмотрением трансграничного спора о нарушении исключительного права (§ 221–223)[3]. Для реа-

[1] Так, в литературе отмечается, что присоединение Китая к Конвенции во многом зависит от обеспечения адекватной защиты интересов китайских граждан и компаний (см.: *Faye Fangrei Wang*. Internet Jurisdiction and Choice of Law: Legal Practices in the EU, US and China. P. 33–34).

[2] Данные принципы являются не единственными в своем роде. Существуют также Принципы коллизионного регулирования в интеллектуальной собственности, подготовленные в Институте Макса Планка в 2011 г. (*The European Max Planck Group on Conflict of Laws in Intellectual Property* (*CLIP*)), однако они не рассматриваются в данной работе по причине того, что несколько выходят за ее тематику. Представляется, что для иллюстрации тенденций и перспектив развития законодательства в области юрисдикции в сети Интернет достаточно принципов *ALI*.

[3] Во многом данные подходы были вдохновлены наработками, полученными в области правового регулирования трансграничного банкротства (см.: UNCITRAL Model

лизации предлагаемого механизма Принципы используют механизмы *lis pendens* (Европейский союз) и *forum non conveniens* (США). Координация возможна в виде консолидации требований, при которой множество различных трансграничных споров, возникших из одного эпизода (*occurrences*), рассматриваются одним судом. При кооперации один суд координирует рассмотрение совокупности взаимосвязанных споров различными судами. Возможно сочетание обоих форм.

Вопрос о том, в какой форме будет осуществляться координация, решается судом, в котором был инициирован спор, по ходатайству одной из сторон или (в порядке исключения) по собственной инициативе. При этом принимаются во внимание, в частности, удобство и эффективность централизованного судопроизводства по сравнению с кооперационным судопроизводством; возможные временны́е и материальные издержки, ресурсы сторон, перспективы вынесения несовместимых решений, перспективы признания и принудительного исполнения иностранных судебных решений (§ 222 (1)). Если координирующий суд, оценив указанные обстоятельства, приходит к выводу о целесообразности кооперации, то такой суд должен проинформировать все остальные заинтересованные суды о принятом решении и обязать стороны спора составить план рассмотрения спора. Если суд приходит к выводу о целесообразности консолидированного судопроизводства, то он должен решить вопрос о том, кто его должен проводить: либо он сам, либо суд иного государства, которое наиболее тесно связано со спором.

Все другие суды, в которых находятся соответствующие требования, должны приостановить их рассмотрение до решения вопроса о форме координации. В случае установления кооперационного судопроизвод-ства такие суды должны провести консультации со сторонами процесса и координирующим судом с целью определения своей компетенции по таким требованиям. При выборе консолидированного судопроизводства такие суды должны приостановить рассмотрение требований. Однако, если консолидирующий суд отказывается от установления юрисдикции либо в течение разумного периода времени никакой активности в консолидирующем суде не происходит, такие суды вправе возобновить разбирательство. Данное правило направлено на предотвращение использования координационных процедур с целью затягивания процесса. Если суды не соблюдают указанные ограничения, их решения не могут

Law on Cross-Border Insolvency 1997; American Law Institute's Guidelines Applicable to Court-to-Court Communications in Cross-Border Cases 2001).

быть принудительно исполнены на территории других государств как противоречащие Принципам[1].

Принципы определения юрисдикции, применимого права и принудительного исполнения судебных решений в сфере интеллектуальной собственности также содержат ряд положений, касающихся применимого права. В соответствии с § 301 в качестве права, применимого к определению вопросов существования, действительности, продолжительности, содержания, способов защиты прав интеллектуальной собственности, подлежащих регистрации, применяется право страны регистрации такого права, а если право возникает без регистрации, – право страны, для которой истребуется защита (*lex protectionis*). Таким образом, Принципы закрепляют в качестве общего правила ту привязку, которая давно применяется на практике: применение права страны, в которой произошло нарушение исключительного права. Однако чем ценны данные Принципы, так это предлагаемыми исключениями из действия указанного принципа, которые установлены в § 302 и 321–323.

Первое исключение касается вопроса определения личности правообладателя, который должен решаться в соответствии с правом страны, в которой был создан соответствующий объект интеллектуальной собственности, что отражает подход, принятый американским судом в деле *ITAR-TASS*.

Второе исключение относится к действию принципа автономии воли, согласно которому стороны могут выбрать право, регулирующее их отношения на случай нарушения исключительного права, в любой момент – даже после возникновения спора, при условии, что такой выбор не нарушает прав третьих лиц.

Третье исключение специально посвящено случаям нарушения исключительного права в сети Интернет (*ubiquitous infringement*). В случае, когда нарушение исключительного права носит глобальный характер, сопряженный с применением законодательства множества стран, суд может применить к таким нарушениям право страны или стран, которые имеют наиболее тесные связи со спором. При этом принимаются во внимание такие обстоятельства, как местонахождение сторон, основной центр взаимоотношений сторон (при наличии такового), масштабы деятельности и инвестиций сторон, основные рынки, на которые направлена деятельность сторон. Таким образом, если стороны являются резидентами одной страны, то может быть применено право такой страны, независимо от того, где имели место нарушения исклю-

[1] Intellectual Property: Principles Governing Jurisdiction, Choice of Law, and Judgments in Transnational Disputes. ALI. 2007. § 403 (2) (*c*) & (*d*).

чительного права. В иных случаях может быть применено право той страны, где был причинен наибольший ущерб. В качестве запасного варианта у суда всегда есть возможность применить *lex fori*, если по каким-либо причинам установить наиболее подходящее применимое право с использованием вышеуказанных критериев не удалось. Такой подход позволяет избежать необходимость применения права каждой из стран, где имело место нарушение, минимизировав тем самым временны́е и материальные издержки и приводя в итоге к более эффективной защите нарушенных прав правообладателя.

Целесообразность и разумность вышеуказанных подходов к определению применимого права к отношениям, связанным с нарушением исключительных прав, не позволяют в полной мере согласиться с С.А. Бабкиным в том, что существующие коллизионные нормы в целом способны адекватно регулировать такие отношения, в силу чего разработка специальных коллизионных норм «для Интернета» нецелесообразна[1]. Как видно, наличие таких специальных норм весьма желательно для применения защиты исключительных прав от нарушений в сети Интернет, где последовательное применение правила *lex protectionis* приводит к значительным сложностям, судебным издержкам и судебным ошибкам.

Остается надеяться, что подходы, изложенные в Принципах *ALI*, найдут свое отражение в законодательствах отдельных стран, а возможно, и в нормах наднационального законодательства.

§ 6. Некоторые компаративные выводы и перспективы развития норм о юрисдикции в сети Интернет

Анализ законодательства и судебной практики по вопросам юрисдикции в сети Интернет, как в части определения вопросов компетентности суда по рассмотрению спора, так и собственно регулирования отдельно взятой страной отношений, возникающих в сети Интернет, со всей очевидностью демонстрирует несостоятельность так называемого скептического подхода к интернет-юрисдикции. Суть данного подхода сводится к тому, что отсутствуют какие-либо фактические и юридические основания для подчинения отношений, возникающих при использовании сети Интернет, той или иной юрисдикции, основанной на территориальном признаке. Тем самым отрицается не только применимость традиционных критериев определения юрисдикции к интернет-отношениям, но и притязания отдельно взятого государства

[1] См.: *Бабкин С.А.* Право, применимое к отношениям, возникающим при использовании сети «Интернет»: Основные проблемы. С. 45.

регулировать такие отношения[1]. Трансграничный и общедоступный характер сети Интернет приводит с точки зрения сторонников данного подхода к тому, что сфера юрисдикции одного государства в данной области полностью совпадает со сферой юрисдикции любого другого, что влечет их взаимную нейтрализацию.

Практика демонстрируют иную картину. Если принять во внимание роль сети Интернет в экономике и прочих сферах жизни общества, становится очевидным, что он слишком важен для того, чтобы государства смогли просто так его отпустить «в свободное плаванье» абсолютного саморегулирования[2]. При этом Интернет не является абсолютно виртуальным пространством: его пользователи – живые люди, которые находятся на определенной территории, а также компании, которые обладают активами, расположенными на определенной территории. Инфраструктура Интернета (кабели, серверы и иное оборудование) также физически локализована на определенной территории. Все это создает условия для применения классических оснований для установления судами своей юрисдикции в отношении субъектов интернет-отношений.

Как следствие, суды нередко весьма успешно применяют традиционные подходы для решения вопросов установления своей юрисдикции в отношении иностранных ответчиков по спорам, возникающим в связи с использованием сети Интернет. Безусловно, имеет место определенная их адаптация к специфике сети Интернет, но в остальном это все те же «минимальные контакты», «место исполнения договора», «место совершения правонарушения или наступления его вредоносных последствий».

Критерий направленности осуществляемой в сети Интернет деятельности на определенное государство приобретает все большее значение при решении вопросов, связанных с юрисдикцией судов такого государства или выбора права такого государства в качестве применимого. В Европейском союзе данный критерий ограничен *B2C*-сегментом – трансграничными потребительскими договорами, обеспечивая потребителей не только возможностью предъявления исков из таких договоров в свой «родной» суд, но и гарантиями, предоставляемыми их «родным» правом.

---

[1] Емкий и краткий анализ на русском языке данного подхода см.: *Бабкин С.А.* Интеллектуальная собственность в сети Интернет. С. 231 и далее.

[2] Достаточно красочно и убедительно это продемонстрировано в известной работе: *Goldsmith J., Wu T.* Who Controls the Internet: Illusions of a Borderless World. Oxford University Press. 2006.

В США критерий направленности деятельности не ограничен лишь сферой потребительских договоров, но носит характер одного из факторов, принимаемых во внимание при определении наличия минимальных контактов с территорией штата, необходимых для установления юрисдикции. В настоящее время некогда популярный тест скользящей шкалы, выработанный в деле *Zippo*, практически не применяется, уступив место критерию направленности деятельности.

Российскому праву критерий направленности деятельности как условие установления юрисдикции российского суда или выбора применимого права пока чужд. Предусмотренные в ГПК РФ и АПК РФ основания для установления юрисдикции российского суда в отношении спора с участием иностранного лица не в полной мере учитывают специфику отношений в сети Интернет, в частности, по распространению цифрового контента. Содержащиеся в АПК РФ специальные основания, разработанные для применения в сети Интернет (ч. 9 ст. 247), сформулированы весьма неудачно и мало что добавляют к уже имеющимся основаниям. В некоторой степени эти недостатки могут быть компенсированы включенным в АПК РФ положением о возможности установления юрисдикции в иных случаях, когда между спорным правоотношением и территорией Российской Федерации имеется тесная связь (ч. 10 ст. 247). Понятие «тесной связи» в контексте основания для установления юрисдикции достаточно гибкое и позволяет охватывать используемый за рубежом критерий направленности деятельности, который пока не нашел своего отражения в российском праве, а также выступать в качестве экстраординарного основания для установления юрисдикции арбитражного суда по отношению к тем интернет-спорам, которые затрагивают интересы Российской Федерации, но в то же время которые не могут быть приняты арбитражным судом к рассмотрению по иным основаниям.

Однако, даже несмотря на все несовершенство российского законодательства в области интернет-споров, представляется нецелесообразной выработка неких специальных критериев для установления юрисдикции в сети Интернет (например, по месту нахождения сервера или географической принадлежности домена). В условиях развития облачных технологий место размещения сервера и уж тем более информации на нем приобретает все более случайный и малопредсказуемый характер и может учитываться лишь в качестве дополнительного обстоятельства, принимаемого во внимание при установлении юрисдикции, но уж никак не в качестве основного юрисдикционного критерия[1]. Аналогично вряд

[1] Данный критерий предлагается, в частности, в следующих работах: *Войниканис Е.А.*, *Якушев М.В.* Информация. Собственность. Интернет: Традиция и новеллы

ли можно согласиться с предложениями об ограничении юрисдикции государства лишь сферой Интернета, охватываемой национальными доменными именами либо в случае с функциональными доменами вроде «*.com*» – национальной принадлежности регистратора домена[1]. Существующие правила регистрации доменных имен не могут являться сколько-нибудь надежным индикатором принадлежности веб-сайта к определенному государству. Ничто не мешает российскому лицу зарегистрировать доменное имя в другой географической зоне либо в функциональной доменной зоне («*.com*», «*.net*» и др.) с использованием услуг иностранных регистраторов. Легкость осуществления таких действий не должна сопровождаться легкостью выхода из-под юрисдикции российских судов и иных правоприменительных органов. Реализация предлагаемого подхода возможна лишь при условии кардинального ужесточения правил регистрации доменных имен в зоне «*.ru*», позволяющей обеспечить реальную привязку деятельности под таким доменным именем к территории Российской Федерации, с одновременным запретом российским лицам регистрировать доменные имена в иных зонах в отсутствие предварительно зарегистрированного домена в зоне «*.ru*» и установлением полной ответственности за деятельность таких сайтов.

Местонахождение сервера и географическая принадлежность доменного имени[2] могут использоваться в качестве критериев для применения классических оснований для установления юрисдикции (по месту причинения вреда, по месту нахождения имущества ответчика, по месту исполнения договора и пр.), но не в качестве специализированных оснований установления юрисдикции в отношении интернет-споров.

Важно не забывать и тот факт, что даже самых развитых и продуманных норм, регламентирующих компетентность национального суда по рассмотрению того или иного интернет-спора с участием иностранного лица, недостаточно, если отсутствует реальная возможность последующего исполнения судебного решения. Проблематика реализации *jurisdiction to enforce* является одной из наиболее сложных в сфере электронной коммерции. Мало кого радует перспектива потратить

в современном праве. М., 2004; *Зажигалкин А.В.* Международно-правовое регулирование электронной коммерции: автореф. дис. ... канд. юрид. наук. СПб., 2005. С. 10.

[1] *Терентьева Л.В.* Сетевое пространство и государственные границы: вопросы юрисдикции в сети Интернет // Российское право: состояние, перспективы, комментарии. М., 2010. С. 64–65.

[2] Как справедливо указывает В.О. Калятин, регистрируя доменное имя в географическом домене, лицо тем самым выражает желание установить определенную связь с данной страной (см.: *Калятин В.О.* Доменные имена. С. 58).

несколько месяцев, а то и лет в совокупности с немалым размером издержек и в итоге убедиться в том, что все это было зря.

Гаагская конвенция по вопросам в отношении соглашений о выборе суда 2005 г. является важным шагом в обеспечении «оборотоспособности» судебных решений на международной арене. Но она имеет достаточно ограниченную сферу действия (предпринимательские отношения) и касается лишь случаев, когда стороны заранее позаботились о регламентации в своем договоре места рассмотрения спора. К тому же пока данную Конвенцию ратифицирует достаточное количество участников, хотя бы сопоставимое с количеством участников Нью-Йоркской конвенции 1958 г., пройдет немало времени. Интернет к тому времени уже будет иным, во многом благодаря тому, что туда, где право оказалось бессильным или малоэффективным, придет технология, которая задаст определенные правила поведения и «юрисдикция» которой *a priori* распространяется на всю сеть[1]. Технология также будет в основе создания особого свода норм, носящих внетерриториальный характер, а исполнение вынесенного на их основе решения будет осуществляться посредством компьютеров и технических средств[2]. Уже сейчас имеют место примеры успешной реализации данного подхода в виде Единообразной политики рассмотрения доменных споров (*UDRP*)[3]. В условиях, когда большинство стран не могут собраться и договориться по вопросам демаркации своей юрисдикции в Интернет, соответствующая неопределенность будет восполнена иными доступными способами. Насколько удачно – покажет время.

§ 7. Возможные меры по минимизации юрисдикционных рисков

Применение критерия направленности деятельности позволяет предпринимателям в сфере электронной коммерции осуществлять определенное планирование и заранее предпринимать меры по минимизации риска привлечения их в качестве ответчика в судах нежелательных стран. Для этого необходимо иметь доказательства того, что их деятельность в сети Интернет не была направлена на соответствующую территорию. Существующая в США и Европейском союзе

[1] См. подробнее: *Reidenberg J.* Lex Infromatica: The Formulation of Information Policy Rules Through Technology // Texas Law Review. 1998. No 3. P. 553–594; *Lessig L.* Code and Other Laws of Cyberspace. 1999.

[2] *Mancini A.* Internet Justice: Philosophy of Law for the Virtual World. Buenos Books America. 2005. P. 77 ff.

[3] См. подробнее § 6 гл. 5 настоящей книги.

судебная практика допускает использование следующих аргументов в обоснование данной позиции:

1) наличие специальных оговорок на сайте, из которых можно сделать вывод о том, что он рассчитан лишь на граждан (юридических лиц) из определенных государств, а клиенты из других государств не обслуживаются;

2) использование систем географической идентификации пользователей по *IP*-адресу и (или) банковским картам с блокированием возможности совершения заказа клиентами из нежелательных стран;

3) отсутствие локализации веб-сайта применительно к определенным странам (например, если предприниматель не желает продавать товар клиентам из Англии, веб-сайт не должен предусматривать возможность исчисления цены товара в фунтах стерлингов).

Если бизнес-план предполагает включение определенных стран в сферу деятельности веб-магазина, но такие страны содержат особое регулирование, которое необходимо учитывать в ходе осуществления онлайн-деятельности, то целесообразно зарегистрировать для таких стран отдельный веб-сайт. Такой сайт должен быть под географическим доменом такой страны и обеспечить переадресацию клиентов из такой страны с главного веб-сайта на локальный. Это позволит учесть специфику законодательства такой страны и, например, исключить возможность приобретения товаров, которые запрещены к продаже в такой стране, при сохранении возможности их продажи через другие сайты для клиентов из других стран.

Наконец, необходимо помнить о том, что даже если суд какой-либо страны и инициирует процесс против владельца веб-сайта, реальная угроза возникает лишь в том случае, когда на территории данной страны находятся какие-либо активы, на которые можно обратить взыскание для исполнения решения, либо имеет место международное соглашение о взаимном признании судебных решений между данной страной и страной, где такие активы расположены. В отсутствие данных условий перспективы реального исполнения судебного решения, вынесенного в такой стране, весьма туманны, что обусловливает относительно невысокие риски возникновения судебных исков в них. В связи с этим грамотное планирование мест размещения активов компании, ведущей свою деятельность в сфере электронной коммерции, также играет важную роль в минимизации юрисдикционных рисков.

Помимо использования средств веб-дизайна, позволяющих обосновывать отсутствие направленности сайта на определенную территорию, необходимо также максимально использовать возможности,

предоставляемые договорным правом, для конкретизации применимого права и места рассмотрения возможных споров. Именно средства договорного права признаются на данный момент наиболее эффективным средством решения коллизионных проблем в сети Интернет[1]. Заключаемые в сети Интернет соглашения должны иметь как соглашение о применимом праве, так и пророгационное соглашение или третейскую оговорку. Причем в отсутствие международных соглашений, ратифицированных большим количеством государств по вопросу взаимного признания решений государственных судов, третейская оговорка может быть более предпочтительным вариантом в *B2B*-контрактах, так как Нью-Йоркская конвенция 1958 г. предоставляет дополнительные гарантии возможности принудительного исполнения вынесенного решения в отношении ответчика. Что же касается потребительских договоров, наличие пророгационного соглашения или третейской оговорки также не будет лишним, но необходимо быть готовым к тому, что такие условия могут быть оспорены как нарушающие права потребителя[2]. Чтобы минимизировать такой риск (по крайней мере применительно к США), целесообразно выбрать такой юрисдикционный орган, который был бы удобен и для другой стороны и имеет определенную связь с элементами правоотношения, а также следует обеспечить возможность предварительного ознакомления с содержимым оговорки и сохранения ее для последующих ссылок[3].

Указанные меры, принятые в совокупности, должны позволить эффективно минимизировать риски неожиданного возникновения споров в судах США и странах Европейского союза. Разумеется, они не препятствуют возможности установления иностранными судами юрисдикции на основании традиционных критериев (по местонахождению сервера, по месту осуществления деятельности администратора сайта и т.п.), но могут существенно снизить риски возникновения спора в данных правопорядках лишь на основании того факта, что веб-сайт был доступен на их территории.

---

[1] См., например: *Faye Fangrei Wang*. Internet Jurisdiction and Choice of Law: Legal Practices in the EU, US and China. P. 19.

[2] См., например: Oceano Grupo Editorial SA v. Rociio Murciano Quintero. E.C.R. 2000. I-4941.

[3] Intellectual Property: Principles Governing Jurisdiction, Choice of Law, and Judgments in Transnational Disputes. ALI. 2007. P. 86.

Глава 3. Договорные аспекты электронной коммерции

Договоры, заключаемые в сети Интернет, подчиняются общим положениям о порядке заключения договоров, сформулированным в ГК РФ и берущим свое начало еще со времен римского права. Согласно ст. 432 ГК РФ договор считается заключенным, если между сторонами в требуемой в подлежащих случаях форме достигнуто соглашение по всем существенным условиям договора. Договор заключается посредством направления оферты (предложения заключить договор) одной из сторон и ее акцепта (принятия предложения) другой стороной. Положения об оферте и акцепте составляют фундамент договорного права, обеспечивающий участникам оборота контроль над процессом создания договора: как над фактом его существования, так и над его содержанием[1].

Таким образом, для признания договора заключенным необходимо установить наличие оферты, акцепта, а также соблюдения требований, предъявляемых к форме договора. Также необходимо, чтобы участники договора обладали правосубъектностью, так как в отсутствие оной их действия не могут создать договорных прав и обязанностей.

В целом можно сказать, что к договорам, заключаемым в электронной среде, применяются все те же нормы, что и к традиционным «бумажным», ведь договор не перестает быть договором лишь потому, что он совершен с помощью компьютера. Другое дело, что применение классических положений договорного права к соглашениям, заключаемым в сети Интернет, является порой не такой уж простой задачей, учитывая технологические особенности данной Сети и сложившиеся в ней бизнес-практики.

§ 1. Оферта

В соответствии с п. 1 ст. 435 ГК РФ под офертой понимается адресованное одному или нескольким конкретным лицам предложение, которое достаточно определенно и выражает намерение лица, сделав-

[1] *Smith S.* Contract Theory. Oxford, 2004. P. 169.

шего предложение, считать себя заключившим договор с адресатом, которым будет принято предложение. Оферта должна обладать двумя конститутивными признаками:

1) направленность оферты: она должна выражать намерение лица, которое выступает с предложением, считать себя заключившим договор на условиях, указанных в договоре с адресатом, в случае, если последний примет предложение;

2) определенность оферты: она должна содержать все существенные условия будущего договора[1].

Указанные требования взаимосвязаны и по сути обеспечивают друг друга. Как отмечал Л. Эннекцерус, оферта должна быть настолько определенная, чтобы можно было путем ее принятия достигнуть соглашения об всем договоре.

Что же касается требования об адресности оферты, содержащегося в легальной дефиниции оферты («...адресованное одному или нескольким конкретным лицам»), то оно понимается предельно широко, допуская выступление в качестве адресата оферты не только определенное лицо, но и определимое[2]. В последнем случае ГК РФ предусматривает так называемую публичную оферту, под которой понимается «содержащее все существенные условия договора предложение, из которого усматривается воля лица, делающего предложение, заключить договор на указанных в предложении условиях *с любым, кто отзовется*» (п. 2 ст. 437 ГК РФ). При этом, с точки зрения законодателя, никакой разницы между такой публичной офертой и обычной, адресованной конкретному лицу, нет. Все те последствия, которые вызывает обычная оферта, следуют и из публичной[3].

Однако далеко не каждое предложение, «брошенное в толпу», может быть квалифицировано в качестве публичной оферты. ГК РФ содержит общую презумпцию о том, что реклама и иные предложения, адресованные неопределенному кругу лиц, признаются только приглашением к оферте, но не офертой.

---

[1] *Брагинский М.И., Витрянский В.В.* Договорное право. Общие положения. М., 2005. С. 196; *Kötz H., Flessner A.* European Contract Law. Clarendon Press: Oxford, 2002. P. 17–18.

[2] Существуют, однако, судебные решения, где утверждается о том, что предложение может являться офертой только тогда, когда оно сделано определенному лицу или лицам, а не неопределенному кругу лиц, из чего делается вывод о том, что текст договора, размещенный в сети Интернет, не является офертой (постановление Девятого арбитражного апелляционного суда от 22 мая 2012 г. № 09АП-8366/2012-ГК по делу № А40-131749/11-55-237). Однако, как показано далее, такой подход является неверным, поскольку не учитывает возможности существования публичной оферты.

[3] *Брагинский М.И., Витрянский В.В.* Договорное право. Общие положения. С. 198.

Положения о публичной оферте конкретизируются в ст. 494 ГК РФ. Так, предложение товара в его рекламе, каталогах и описаниях товаров, обращенных к неопределенному кругу лиц, признается публичной офертой, если оно содержит все существенные условия договора розничной купли-продажи. Буквальное толкование данного положения позволяет сделать вывод о том, что наличия другого признака публичной оферты (наличия воли лица, делающего предложение, заключить договор на указанных в предложении условиях с любым, кто отзовется) в данном случае не требуется. Таким образом, если речь идет о договоре розничной купли-продажи, одного факта наличия в предложении всех существенных условий договора достаточно для признания его офертой.

Положения ст. 494 ГК РФ предусматривают также случаи, когда предложения товара, адресованные неопределенному кругу лиц, могут признаваться публичной офертой даже в случае, когда отсутствуют цена и иные существенные условия. Это относится к ситуациям выставления товаров в месте продажи (на прилавке, в витрине и т.п.), демонстрации их образцов или предоставлении сведений о продаваемых товарах (описаний, каталогов, фотоснимков товаров и т.п.). Исключением являются случаи, когда продавец явно для окружающих определил, что соответствующие товары не предназначены для продажи.

Определившись с исходным регулированием, необходимо рассмотреть, как оно применяется в контексте отношений, возникающих в сфере электронной коммерции.

В самой общей форме механизм покупки чего-либо в интернет-магазине можно описать следующим образом. Пользователь заходит на веб-сайт, просматривает доступные товары, откладывает их в корзину, осуществляет оплату, в процессе которой принимает условия продажи (если таковые есть). В связи с этим возникает вопрос: что же считать офертой и акцептом в таких случаях?

Продажа товара потребителю через интернет-магазины подпадает под понятие продажи товаров дистанционным способом, под которой понимается «продажа товаров по договору розничной купли-продажи, заключаемому на основании ознакомления покупателя с предложенным продавцом описанием товара, содержащимся в каталогах, проспектах, буклетах либо представленным на фотоснимках или с использованием сетей почтовой связи, сетей электросвязи, в том числе информационно-телекоммуникационной сети Интернет, а также сетей связи для трансляции телеканалов и (или) радиоканалов, или иными способами, исключающими возможность непосредственного ознаком-

ления покупателя с товаром либо образцом товара при заключении такого договора»[1].

Как следует из данной дефиниции, не всякая продажа товара, осуществляемая с использованием сети Интернет, является дистанционной. Для того чтобы она признавалась таковой, необходимо одновременное выполнение двух условий: 1) у покупателя отсутствовала возможность непосредственного ознакомления с товаром при заключении договора; 2) такое ознакомление было произведено посредством описания, предоставленного продавцом.

Если покупатель сам сообщил продавцу параметры необходимого ему товара, а продавец, руководствуясь им, подобрал товар и продал его покупателю, такой договор не подпадает под понятие дистанционного способа продажи, даже если коммуникации происходили с использованием сети Интернет, поскольку отсутствует условие 2. Например, такая ситуация будет иметь место в случае, когда потребитель обращается в интернет-магазин и в ходе общения с его представителем сообщает параметры необходимых ему запчастей для автомобиля, которые впоследствии были подобраны и предоставлены покупателю, что, однако, не исключает квалификации данного договора в качестве потребительского и в качестве договора розничной купли-продажи[2]. Аналогично не будет являться дистанционной продажа товара, с которым потребитель предварительно ознакомился в салоне магазина, а впоследствии приобрел данный товар через интернет-магазин данного салона, поскольку в данном случае отсутствует условие 1 договора дистанционной продажи[3].

Следует отличать продажу товара дистанционным способом от продажи товара по образцам. По ранее действовавшему законодательству определить, являлась продажа товара посредством сети Интернет продажей

[1] См.: п. 2 постановления Правительства РФ от 27 сентября 2007 г. № 612 «Об утверждении Правил продажи товаров дистанционным способом».

[2] См.: постановление Президиума Верховного суда Удмуртской Республики от 21 мая 2010 г. «из материалов гражданского дела не следует, что ООО «Д» предоставляло Ш.В.Л. описание и характеристики приобретаемого товара и предлагало купить у него данный товар. Напротив, Ш.В.Л. описал продавцу требуемый ему товар и продавец в дальнейшем при исполнении договора руководствовался сделанным покупателем заказом. Следовательно, по делу отсутствуют признаки, характеризующие дистанционный способ продажи товара».

[3] См., например: апелляционное определение Московского городского суда от 12 апреля 2012 г. по делу № 11-4108: «Данные правила [дистанционной продажи товаров. – *А.С.*] обоснованно не были применены судом... из материалов дела усматривается, что истец имел возможность и ознакомился с образцом товара в магазине. Что он подтвердил в заседании суда второй инстанции».

товара по образцам или продажей товара дистанционным способом, было практически нереально. Виной тому были несовершенные дефиниции, содержащиеся в соответствующих правилах. Под продажей товара по образцам понимался любой договор розничной купли-продажи, «заключаемый на основании ознакомления покупателя с предложенными продавцом образцами товаров или их описаниями, содержащимися в каталогах, проспектах, буклетах, представленными в фотографиях и других информационных материалах, а также в рекламных объявлениях о продаже товаров»[1]. Под продажей товаров дистанционным способом понимался договор розничной купли-продажи, заключаемый «на основании ознакомления покупателя с предложенным продавцом описанием товара, содержащимся в каталогах, проспектах, буклетах либо представленным на фотоснимках или посредством средств связи, или иными способами, исключающими возможность непосредственного ознакомления покупателя с товаром либо образцом товара при заключении такого договора». Очевидно, что при осуществлении продаж товаров в интернет-магазине, покупатель, с одной стороны, получал информацию о товаре посредством его описания, содержащегося в «других информационных материалах» (на веб-сайте), а с другой – такое ознакомление происходило посредством средств связи и исключало возможность непосредственного ознакомления покупателя с товаром.

Указанная неопределенность была устранена путем внесения изменений в соответствующие правила[2]. Сейчас под продажей товаров по образцам понимается продажа товаров по договору розничной купли-продажи, заключаемому на основании ознакомления покупателя с образцом товара, предложенным продавцом и выставленным в месте продажи товаров. Существенным признаком данного вида продаж является возможность непосредственного ознакомления покупателя с товаром в месте его продажи (например, в демонстрационном зале). Таким образом, *продажа товаров через Интернет в настоящее время не является продажей товаров по образцам*, что должно учитываться и при применении налогового законодательства, в частности при определении условий применения специальных налоговых режимов (ЕНВД, патентная система налогообложения)[3].

---

[1] См.: п. 2 постановления Правительства РФ от 21 июля 1997 г. № 918 «Об утверждении Правил продажи товаров по образцам».

[2] Постановление Правительства РФ от 4 октября 2012 г. № 1007 «О внесении изменений в некоторые акты Правительства Российской Федерации по вопросам продажи товаров и оказания услуг».

[3] См., например, понятие розничной торговли в ст. 346.27 и 346.43 НК РФ.

Дистанционный способ продажи товара потребителю является разновидностью договора розничной купли-продажи (ст. 497 ГК РФ). В связи с этим к нему в полной мере применимы положения, указанные в п. 1 ст. 494 ГК РФ, которые конкретизируются в п. 12 Правил продажи товаром дистанционным способом: «предложение товара в его описании, обращенное к неопределенному кругу лиц, признается публичной офертой, если оно достаточно определенно и содержит все существенные условия договора. Продавец обязан заключить договор с любым лицом, выразившим намерение приобрести товар, предложенный в его описании». Существенными условиями договора розничной купли-продажи являются наименование и количество товара (п. 3 ст. 455 ГК РФ) и его цена («цена и другие существенные условия договора розничной купли-продажи» – п. 2 ст. 494 ГК РФ). Если договор заключается в рассрочку (что в сфере электронной коммерции встречается не так часто), то к перечисленным существенным условиям добавляются еще и условия о порядке, размере и сроках платежей (п. 1 ст. 489 ГК РФ)

Отсюда следует первый важный вывод: *любое предложение товара в интернет-магазине, содержащее наименование товара и стоимость за единицу, является публичной офертой, если в качестве контрагента выступает потребитель* (физическое лицо, заказывающее либо имеющее намерение заказать товар для личных, семейных, домашних и иных нужд, не связанных с осуществлением предпринимательской деятельности)[1]. Оговорки, сделанные на сайте, о том, что предложение не является публичной офертой, не имеют юридической силы как противоречащие императивным нормам ст. 494 ГК РФ и п. 12 Правил продажи товаров дистанционным способом.

Интересен вопрос о том, может ли быть применен п. 2 ст. 494 ГК РФ о признании публичной офертой выставления товара в витрине или в ином месте продажи в отношении товаров, продаваемых на веб-сайтах интернет-магазинов. При положительном ответе на данный вопрос предложение товара к продаже в интернет-магазине может быть квалифицировано в качестве публичной оферты и в отсутствие всех существенных условий.

В судебной практике существуют прецеденты, где суды не только используют слово «витрина» применительно к веб-сайту с интернет-магазином[2], но и применяют п. 2 ст. 494 ГК РФ к случаям размещению

[1] См.: преамбула к Закону о защите прав потребителей; п. 1 ст. 1212 ГК РФ.

[2] Решение Арбитражного суда г. Москвы от 20 октября 2010 г. по делу № А40-35771/10-26-279.

товара на сайте интернет-магазина с выводом о том, что размещенные в сети Интернет каталоги товаров являются публичной офертой для заключения договора купли-продажи[1].

В доктрине, напротив, высказано мнение, что данное положение неприменимо к традиционным, физическим товарам, так как «электронные витрины, на которых размещено описание товара, не могут быть признаны местом его продажи, за исключением случаев, когда товары (или услуги) представлены в цифровой форме»[2]. Представляется, что данное замечание содержит указание на важный вопрос, от ответа на который во многом зависит возможность применения п. 2 ст. 494 ГК РФ: что следует понимать под местом продажи в случае реализации товара через сеть Интернет?

Возможны два варианта ответа на данный вопрос: либо это место заключения договора купли-продажи, либо это место, где товар переходит в собственность покупателя. В первом случае «место продажи» будет определяться по правилам о месте заключения договора, а следовательно, можно было бы говорить о том, что веб-сайт является местом продажи. Во втором случае «место продажи» определяется по правилам о месте исполнения обязательства, и веб-сайт в таком случае не является местом продажи, так как договор купли-продажи исполняется в другом месте.

Буквальное толкование Правил продажи товаров дистанционным способом, в частности дефиниции такой продажи наталкивают на мысль, что продажа имеет место уже при заключении договора, по крайней мере данная дефиниция не включает в себя в качестве элемента фактическую передачу товара.

Некоторые авторы для ответа на исходный вопрос обращаются к разъяснениям, данным для налоговых целей. В свое время Департамент налоговой политики Минфина России разъяснил, что «помещение офиса организации, где размещены компьютеры с выходом в Интернет и осуществляется сбор заказов и содействие в доставке продаваемых товаров» не может рассматриваться в качестве места совершения сделок купли-продажи[3]. Во многом данный подход обусловлен тем, что налоговое законодательство под местом совершения

[1] Постановление Девятого арбитражного апелляционного суда от 10 июня 2009 г. № 09АП-6710/2009, 09АП-6711/2009 по делу № А40-57513/07-51-378, оставленное без изменения постановлением ФАС Московского округа от 21 сентября 2009 г. № КГ-А40/9045-09-П.

[2] *Левашов С.* Виртуальные сделки – реальные права // эж-Юрист. 2005. № 40.

[3] Письмо Департамента налоговой политики Министерства финансов РФ от 13 апреля 2004 г. № 04-05-11/50.

продажи товара (реализации товара) понимает место, где произошел переход права собственности на товар, т.е. термин «продажа» предполагает не просто заключение договора купли-продажи, но и его исполнение. Из этого некоторые авторы делают вывод, что интернет-страница не является местом заключения договора купли-продажи[1]. С данным выводом можно согласиться, учитывая, что заказ товара через интернет-магазин предполагает разрыв во времени между заключением договора и его исполнением продавцом, а следовательно, и переходом права собственности на товар. Признание веб-сайта местом продажи товара выглядит в таких случаях явно искусственным, да и с политико-правовой точки зрения распространение положений п. 2 ст. 494 ГК РФ на интернет-магазины вряд ли оправданно, учитывая, что российское законодательство и так достаточно жестко подходит к вопросам квалификации информации на таких сайтах в качестве оферты. Невозможно допустить, что в качестве оферты может рассматриваться не только предложение, в котором присутствуют все существенные условия договора и отсутствует воля на заключение договора в случае его принятия, но и предложение, которое не содержит не только воли, но и всех существенных условий.

Положения российского законодательства, квалифицирующие практически любое предложение о продаже товара на веб-сайте в качестве публичной оферты, хотя и встречаются в иных странах[2], но все же разделяются не всеми правопорядками.

Отдельные положения Директивы ЕС № 2000/31/ЕС «Об электронной коммерции» дают основания для вывода о том, что размещение информации о товаре на веб-сайте интернет-магазина не является офертой. Так, ст. 10 (1) Директивы предусматривает ряд информационных обязанностей провайдера услуг до того, как их получатель разместит заказ. Тем не менее решение вопроса о статусе коммуникаций сторон отдается на усмотрение национального законодательства государств – членов ЕС.

Так, в английском праве традиционно считается, что предложение товара на веб-сайте является лишь предложением делать оферты, а сама оферта делается покупателем в момент, когда он окончатель-

[1] *Елин В.М., Жарова А.К.* Правовые аспекты торговли в сети Интернет // Право и государство: Теория и практика. 2012. № 10/94.

[2] Например, в Португалии. Статья 31 португальского Закона об электронной коммерции предусматривает, что предложение товара или услуги на веб-сайте является офертой, если содержит в себе все существенные условия договора. Схожий подход имеет место в Малайзии. См.: Online Contract Formation. Ed. by Stephan Kinsella and Andrew Simpson. Oceana Publications. N.Y., 2004. P. 162.

но формирует «корзину» покупок и приступает к оплате[1]. Данный подход основан на прецеденте *Pharmaceutical Society of Great Britain v. Boots Cash Chemists (Southern) Limited*, согласно которому выставление товара на прилавке в супермаркете не является офертой, а является лишь предложением делать оферты: последняя исходит от покупателя, когда он кладет товар в корзину, а акцепт осуществляется магазином на кассе в момент оплаты. В основе данного подхода лежат преимущественно соображения прагматичного толка: иной подход (квалификация в качестве оферты выставления магазином товара на полку с указанием цены) означал бы, что договор считался бы заключенным в момент, когда покупатель кладет товар в корзину, что повлечет ряд неудобств для него самого. Он не сможет поставить товар на полку обратно и выбрать другой, не оплатив первый, поскольку договор в отношении него уже заключен и подлежит исполнению или расторжению по обоюдному согласию сторон[2]. Разумность применения данного подхода к продажам через Интернет обосновывается тем, что он позволяет осуществлять контроль над объемом своих обязательств и избегать ситуаций, при которых количество заключенных договоров может вдруг многократно превысить количество имеющегося у предпринимателя товара. К этому следует добавить, что нередки ситуации допущения технических ошибок при указании цены. Например, были случаи, когда стоимость телевизора была указана на веб-сайте как 3 ф. ст. вместо 300[3], а фотокамеры – 98 ф. ст. вместо 600[4].

Соображения в пользу нецелесообразности признания информации, размещенной на веб-сайте интернет-магазина, в качестве оферты высказываются и в немецкой доктрине[5], поскольку немецкое право, так же как и английское, не рассматривает выставление товара в витрине и магазинах самообслуживания в качестве оферты[6].

Таким образом, российский подход отличается чрезмерной жесткостью по отношению к интернет-магазинам, что может быть хоть как-то оправдано лишь частыми проявлениями недобросовестности с их сто-

[1] *Reed C., Angel J.* Computer Law: The Law an Regulation of Information Technology. Oxford University Press. 2007. P. 106.

[2] [1953] 1QB 410.

[3] *Stone R.* The Modern Law of Contract. Cavendish Publishing Limited. 2002. P. 55.

[4] *Arthur C.* Can I buy a £ 600 camera for £ 100? // The Guardian. 12 January 2006 // http://www.guardian.co.uk/technology/2006/jan/12/guardianweeklytechnologysection2

[5] Law of E-Commerce in Poland and Germany // ed. B. Heiderhodd. Sellier. Munchen, 2005. P. 34.

[6] BGH. 16.01.1980. NJW 1980, 1388; *Markesinis B.* The German Law of Contract. Oxford and Portland. Oregon. 2006. P. 62.

роны, когда на сайте размещается заведомо ложная информация о цене товара, которого даже иногда нет в наличии, – исключительно с целью заманить посетителей, «отвлекая» их тем самым от сайтов конкурентов с реальными ценами. В таких случаях подобные недобросовестные действия могут закончиться признанием договора действительным с вытекающими из этого санкциями за его неисполнение.

Что же касается заключения договоров посредством сети Интернет между предпринимателями (*B2B*), а также физическими лицами между собой (*C2C*), то здесь вышеуказанные положения ст. 494 ГК РФ и Правил дистанционной продажи товаров не действуют, в связи с чем в указанных сферах существует гораздо больше гибкости в определении статуса предложения, сделанного на веб-сайте. В частности, можно сделать оговорку о том, что размещение информации о товаре или услуге не является публичной офертой (п. 1 ст. 437 ГК РФ). В таком случае за владельцем сайта сохраняется возможность отклонения предложений, сделанных посетителями. Данный подход соответствует положениям Конвенции ООН об использовании электронных сообщений в международных сделках 2005 г., ст. 11 которой предусматривает, что предложение заключить договор, не адресованное конкретным лицам и являющееся общедоступным для сторон, использующих информационные системы (в том числе предложения с использованием интерактивных средств размещения заказа), является приглашением делать оферты, если статус оферты в явной форме не указан в таком предложении.

§ 2. Акцепт

Акцептом в соответствии со ст. 438 ГК РФ является ответ лица, которому сделана оферта, о ее принятии. Такой ответ может принимать различные формы – заявления о принятии предложения, либо он может следовать из поведения лица (акцепт конклюдентными действиями). В последнем случае акцептант приступает к действиям по исполнению договора, например к оплате выбранного товара. Причем для признания акцепта состоявшимся достаточно совершения и части действий, обозначенных в договоре[1]. Следует особенно подчеркнуть, что в качестве конклюдентных действий, свидетельствующих об акцепте, судебная практика рассматривает и фактическое использование

[1] Пункт 58 постановления Пленума Верховного Суда РФ № 6, Пленума ВАС РФ № 8 от 1 июля 1996 г. «О некоторых вопросах, связанных с применением части первой Гражданского кодекса Российской Федерации».

тех благ, о которых говорится в оферте[1]. Таким образом, действия лица по использованию объекта оферты (загрузка или установка компьютерной программы, использование электронной базы данных, просмотр фильма и т.д.) также могут быть истолкованы как акцепт и влечь возникновение договора на условиях, изложенных в оферте.

Главное требование, предъявляемое к акцепту российским гражданским законодательством, заключается в его безоговорочном и полном характере. Акцепт не должен содержать изменений условий оферты или каких-либо дополнительных условий, в противном случае он будет являться встречной офертой. Таким образом, ГК РФ исходит из принципа «зеркального» соответствия акцепта оферте, предполагающего полное совпадение встречных волеизъявлений сторон.

Посмотрим, как указанные требования законодательства к акцепту применяются при заключении договоров в сети Интернет. Как следует из п. 12 Правил дистанционной продажи товаров, продавец обязан заключить договор с любым лицом, выразившим намерение приобрести товар, предложенный в его описании. Указанные правила оперируют понятием «сообщение покупателя о намерении заключить договор» вместо понятия «акцепт», что, впрочем, не изменяет существа указанного действия.

Правила дистанционной продажи товаров устанавливают определенное содержание таких сообщений. В соответствии с п. 14 Правил в нем должны быть обязательно указаны следующие сведения:

а) полное фирменное наименование (наименование) и адрес (место нахождения) продавца, фамилия, имя, отчество покупателя или указанного им лица (получателя), адрес, по которому следует доставить товар;

б) наименование товара, артикул, марка, разновидность, количество предметов, входящих в комплект приобретаемого товара, цена товара;

в) вид услуги (при предоставлении), время ее исполнения и стоимость;

г) обязательства покупателя.

К сожалению, Правила никак не регламентируют последствия отсутствия в сообщении определенных сведений, указанных выше. На первый взгляд использование формулировки «должны быть обязательно указаны» ориентирует на то, что отсутствие каких-либо данных в сообщении о намерении заключить договор влечет невозможность признания за ним способности породить правовые последствия, а имен-

[1] См.: п. 2 информационного письма Президиума ВАС РФ от 5 мая 1997 г. № 14 «Обзор практики разрешения споров, связанных с заключением, изменением и расторжением договоров». См. также: Практика применения Гражданского кодекса Российской Федерации, части первой / под общ. ред. В.А. Белова. М., 2008. С. 1119.

но повлечь заключение договора. Однако такой подход противоречил бы ГК РФ, нормы об акцепте которого не предписывают необходимости наличия в нем каких-либо сведений, кроме как полного и безоговорочного согласия с условиями, изложенными в оферте. Вышеуказанный пункт Правил, предписывающий достаточно подробное содержание акцепта, фактически искажает его смысл и создает почву для злоупотреблений. Потребитель в ряде случаев может не иметь некоторых сведений по причине того, что контрагент в нарушение своих обязанностей по информированию потребителя не предоставил их. Однако, даже если потребитель имеет такие данные, у него может отсутствовать техническая возможность указать все эти сведения в его ответе (заказе) на сайте, поскольку форма такого ответа (заказа) не позволяет это сделать. Таким образом, придание сведениям, указанным в п. 14, сообщения о намерении заключить договор, статуса своего рода существенных условий акцепта перечеркнуло бы в значительной степени всю защиту потребителя как слабой стороны, возлагая на него не только значительное бремя по обеспечению соответствия такого намерения требованиям закона, но и предоставляя другой стороне, под контролем которой находится возможность реализации такого обеспечения, удобное средство уклонения от специального правового режима, установленного в отношении дистанционных продаж. Как разъяснил Верховный Суд РФ, «положения правил о вступлении договора в силу с момента получения продавцом сообщения о намерении покупателя приобрести товар не противоречат приведенным положениям ГК РФ и направлены на усиление защиты прав и законных интересов потребителей»[1]. Так что введение Правилами понятия «сообщения о намерении покупателя приобрести товар» и специального правового регулирования в отношении него должно толковаться исключительно через призму цели усиления защиты прав потребителя. Поэтому не остается никакого иного разумного толкования, которое бы соответствовало целям и задачам потребительского законодательства, как признать перечень сведений, которые должны быть указаны в сообщении потребителя об акцепте, имеющим характер приблизительного и факультативного. В качестве сообщения о намерении покупателя приобрести товар необходимо рассматривать любое сооб-

[1] Решение Верховного Суда РФ от 4 октября 2011 г. № ГКПИ11-994 «Об отказе в удовлетворении заявления о признании частично недействующими пунктов 5, 20 Правил продажи товаров дистанционным способом, утв. Постановлением Правительства РФ от 27 сентября 2007 г. № 612», оставленное без изменения Определением Верховного Суда РФ от 8 декабря 2011 г. № КАС 11-675.

щение или действие, из которого недвусмысленно усматривается воля потребителя приобрести товар. Судебная практика именно так и толкует данное положение, признавая в качестве акцепта, в частности, направление продавцу копии платежного документа об оплате товара[1]: оплату товара с отсутствием возражений со стороны продавца против действий покупателя[2]; размещение заказа на веб-сайте с присвоением ему определенного номера[3].

Совершение потребителем вышеуказанных действий означает возникновение заключенного договора. Согласно п. 18 Правил договор считается заключенным с момента выдачи продавцом покупателю кассового или товарного чека либо иного документа, подтверждающего оплату товара, *или с момента получения продавцом сообщения о намерении покупателя приобрести товар*. Учитывая, что в электронной коммерции момент получения продавцом сообщения о намерении приобрести товар всегда будет предшествовать выдаче покупателю товарного, кассового чека или иного документа, именно факт получения продавцом сведений о намерении потребителя заключить договор и является тем юридическим фактом, который влечет возникновение договора.

§ 3. Форма договора

Под формой сделки обычно понимается способ, посредством которого участники сделки изъявляют свою волю при ее совершении (устно, письменно, при помощи конклюдентных действий или молчаливо)[4].

---

[1] См., например: кассационное определение Саратовского областного суда от 19 апреля 2011 г. по делу № 33-2062;

[2] Апелляционное определение Московского городского суда от 22 октября 2012 г. по делу № 11-23085/12: «В удовлетворении встречного иска о признании договора об оказании услуг незаключенным в связи с несогласованием его существенных условий отказано, поскольку покупатель принял все условия оферты, уплатил стоимость товара, при этом ответчик не возражал против действий истца».

[3] Постановление Девятнадцатого арбитражного апелляционного суда от 15 февраля 2013 г. по делу № А36-6311/2012: «Арбитражным судом установлено, что 26 июля 2012 г. Новиковой Т.С. на сайте интернет-магазина Позитроника (http://lipetsk.positronica.ru) оформлен заказ на покупку товара – цифрового фотоаппарата 18 *Mpix Canon EOS 600D (kit)* по цене 24 500 руб. Сообщение о намерении приобрести вышеуказанный товара (заказ), поступившее от потребителя, было принято заявителем и ему был присвоен номер *W*0022-03270. Таким образом, 26 июля 2012 г. между ООО «Компьютерные системы» и гражданкой Новиковой Т.С. был заключен договор купли-продажи дистанционным способом, все существенные условия которого (предмет договора) стороны согласовали в соответствии с пунктами 12 и 18 Правил продажи».

[4] Гражданское право: в 4 т. Общая часть: учебник / под ред. Е.А. Суханова. Т. I. М., 2005. *Татаркина К.П.* Форма сделок в гражданском праве России: монография. Томск, 2012.

Российское законодательство предусматривает две формы сделки: устную и письменную. Письменная форма может быть простой и нотариальной (ст. 158 ГК РФ).

Устная форма предполагает выражение воли словами (при встрече, по телефону и т.п.), благодаря чему воля воспринимается другой стороной непосредственно[1] с помощью органов слуха. Формализации волеизъявления каким-либо иным способом в данном случае не происходит. В принципе, не исключено заключение сделок посредством сети Интернет и в устной форме в тех случаях, когда он используется как средство передачи голосовой связи («*Skype*», различного рода видеоконференции). Данные случаи вполне укладываются в классическое регулирование устных сделок, в связи с чем не представляют собой особого исследовательского интереса в контексте проблематики электронной коммерции.

В отличие от устной формы письменная предполагает закрепление волеизъявления на письме, т.е. с использованием специальных графических знаков (знаков письменности). Закон не регламентирует, как должен составляться письменный документ, отражающий содержание сделки, а значит, он может быть написан от руки, напечатан на компьютере или воспроизведен иным способом.

Именно письменная форма является наиболее распространенной в коммерческих отношениях. По общему правилу в простой письменной форме должны совершаться все сделки между гражданами и юридическими лицами, а также между гражданами на сумму свыше 10 МРОТ, а в случаях, указанных законом, – независимо от суммы сделки. Закон или соглашение сторон может предусмотреть необходимость совершения сделки в квалифицированной письменной форме – нотариальной. Однако, как справедливо отмечается в литературе, «через Интернет невозможно совершить сделки, требующие нотариального удостоверения, поскольку удостоверительная надпись может быть совершена только на «бумажном» документе[2]. Это не означает, что нотариальные действия не могут быть в принципе, в силу своего существа, совершены посредством сети Интернет. Например, законодательство США

[1] Гражданское право: в 4 т.: учебник / под ред. Е.А. Суханова. Т. I. Общая часть. С. 462.

[2] *Калятин В.О.* Право в сфере Интернета. С. 329. На это указывает, в частности, толкование ст. 45 Основ законодательства Российской Федерации о нотариате от 11 февраля 1993 г. № 4462-I (далее – Основы законодательства о нотариате), устанавливающей требования к документам, предъявляемым для совершения нотариальных действий. Например: «В документе, объем которого превышает один лист, листы должны быть прошиты, пронумерованы и скреплены печатью».

об электронной подписи допускает совершение нотариальных действий с использованием электронной подписи нотариуса[1]. Просто российское законодательство пока не дошло до такого уровня развития.

Таким образом, методом исключения становится очевидным, что если договоры, заключаемые в сети Интернет, и соответствуют какой-либо из форм, предусмотренных законом, то это может быть только письменная форма. При этом не предполагается подписания традиционных бумажных договоров с проставлением подписей обеих сторон, в противном случае преимущества, предоставляемые сетью Интернет, были бы в значительной степени утрачены. Преимущества, которые предоставляет электронная коммерция, могут быть в полной мере реализованы только в случае признания юридической силы договоров, заключаемых в электронной среде.

За рубежом уже долгое время общепризнанной является принцип недискриминации электронной формы договора по отношению к традиционной бумажной форме. Сам по себе факт того, что информация выражена в электронной форме, не может являться основанием для лишения ее юридической силы. В случае когда при заключении контракта используется электронное сообщение, этот контракт не может быть лишен действительности или исковой силы на том лишь основании, что он совершен в электронной форме[2]. Иными словами, договор не перестает быть договором лишь на том основании, что он заключен при помощи компьютера.

В российском законодательстве, к сожалению, отсутствуют положения, аналогичные вышеизложенным[3].

При этом в отечественной правоприменительной практике и доктрине электронная форма представления информации нередко рассматривается как заведомо ущербная: суды и иные государственные органы неохотно принимают электронные документы, доктрина пестрит выводами о том, что, за очень редким исключением (вроде наличия электронной цифровой подписи), подобные документы имеют

[1] United States Electronic Signatures in Global and National Commerce Act (E-Sign Act) 2000. Sec. 101 (*g*).

[2] Статья 8 Конвенции ООН об использовании электронных сообщений в международных сделках 2005 г.; ст. 11 Типового закона ЮНСИТРАЛ «Об электронной торговле» 1996 г., ст. 7 Единообразного закона США об электронных сделках; ст. 11 Закона об электронных сделках Сингапура 1998 г., ст. 8 Австралийского закона об электронных сделках 1999 г.; ст. 9 Директивы ЕС № 2000/31/ЕС «Об электронной коммерции» и др.

[3] Но могут появиться в случае ратификации Конвенции ООН об использовании электронных сообщений в международных сделках 2005 г., которая была подписана со стороны России 25 апреля 2007 г.

весьма сомнительную юридическую силу[1]. Причем основную роль в формировании подобного рода тональности играет формализм судов и иных правоприменительных органов, поскольку у многих юристов невозможность (или значительная сложность) использования электронных документов в публично-правовых отношениях автоматически предопределяет их гражданско-правовой статус. Хотя в идеале должно было бы быть с точностью наоборот: публично-правовая оценка электронных форм взаимодействия субъектов должна предопределяться их допустимостью с точки зрения гражданского права. А с точки зрения гражданского права последствия несоблюдения письменной формы не являются фатальными: несоблюдение письменной формы влечет недействительность сделки лишь при наличии прямого указания закона. А во всех остальных случаях несоблюдение простой письменной формы сделки лишает стороны права в случае спора ссылаться в подтверждение сделки и ее условий на свидетельские показания, но не лишает их права приводить письменные и другие доказательства (п. 1 ст. 162 ГК РФ). С момента исключения пункта о недействительности внешнеэкономической сделки при несоблюдении ее письменной формы (п. 3 ст. 162 ГК РФ, действовавший до 1 сентября 2013 г.), случаев, применимых к сфере электронной коммерции, при которых закон предусматривал бы такую недействительность, практически не осталось. Но в любом случае вопрос о действительности договоров, заключаемых в электронной среде сети Интернет, является значимым вопросом электронной коммерции, которая имеет в своем основании именно договорные отношения.

Общее регулирование письменной формы договора содержится в положениях ст. 160 и 434 ГК РФ.

Согласно п. 1 и 2 ст. 160 ГК РФ «сделка в письменной форме должна быть совершена путем составления документа, выражающего ее содержание и подписанного лицом или лицами, совершающими сделку или должным образом уполномоченными ими лицами... использование при совершении сделок факсимильного воспроизведения подписи

[1] См., например: Правовые аспекты использования интернет-технологий / под ред. А.С. Кемрадж, Д.В. Головерова. М., 2002. С. 148; *Ткачев А.В.* Правовой статус компьютерных документов: основные характеристики. М., 2000. С. 39; определение Воронежского областного суда от 4 марта 2010 г. по делу № 33-1144/10: «имеющиеся в деле две копии электронного письма не соответствуют требованиям Федерального закона «Об электронной цифровой подписи». Письмо не содержит такой подписи, которая бы позволяла идентифицировать владельца сертификата ключа подписи. В силу ст. 4 указанного Закона только электронный документ с электронной цифровой подписью имеет юридическое значение, и только с помощью ЭЦП возможно проверить место отправки данного письма и установить его отправителя».

либо иного аналога собственноручной подписи допускается в случаях и в порядке, предусмотренных законом, иными актами или соглашением сторон».

Статья 434 ГК РФ конкретизирует способы заключения договора в письменной форме тремя способами: 1) путем составления единого документа, подписанного обеими сторонами; 2) путем обмена документами посредством почтовой, телеграфной, телетайпной, телефонной, электронной или иной связи, позволяющей достоверно установить, что документ исходит от стороны по договору; 3) путем акцепта оферты конклюдентными действиями. В последнем случае письменная форма *считается* соблюденной, т.е. закон вводит фикцию ее наличия.

Как известно, правила о сделках применяются к договорам в субсидиарном порядке, если нормами о договорах не предусмотрено специального регулирования[1]. Таким образом, нормы ст. 434 ГК РФ являются специальными по отношению к положениям ст. 160 ГК РФ и подлежат преимущественному применению. Однако поскольку они не содержат регламентации вопросов, связанных с подписанием документа с использованием аналогов собственноручной подписи, положения ст. 160 ГК РФ подлежат субсидиарному применению в этой части. Данный вывод подтверждается и положениями ч. 4 ст. 11 Закона об информации, который связывает соблюдение письменной формы договора при его заключении путем обмена документами с наличием подписи: «в целях заключения гражданско-правовых договоров или оформления иных правоотношений, в которых участвуют лица, обменивающиеся электронными сообщениями, обмен электронными сообщениями, каждое из которых подписано электронной подписью или иным аналогом собственноручной подписи отправителя такого сообщения, в порядке, установленном федеральными законами, иными нормативными правовыми актами или соглашением сторон, рассматривается как обмен документами».

Таким образом, систематическое толкование положений ГК РФ позволяет сделать вывод, что письменная форма договора считается соблюденной при выполнении двух условий:

1) договор составлен в виде документа или документов, отражающих содержание договоренности сторон (п. 2 ст. 434 ГК РФ), либо

[1] *Витрянский В.В.* Некоторые аспекты учения о гражданско-правовом договоре в условиях реформирования гражданского законодательства // Проблемы развития частного права. Сборник статей к юбилею В.С. Ема / отв. ред. Е.А. Суханов, Н.В. Козлова. М., 2011; Комментарий к Гражданскому кодексу Российской Федерации. Часть первая: учеб.-практич. комментарий (постатейный) / под ред. А.П. Сергеева. М., 2010 (п. 4 комментария к ст. 420).

документа, закрепляющего содержание волеизъявления одной стороны, подкрепленного соответствующим поведением другой стороны (п. 3 ст. 434 ГК РФ);

2) документ(ы) подписан(ы) собственноручной подписью либо ее аналогами.

Особенностью российского законодательства, как, впрочем, и многих иных правопорядков, общие нормы о формах сделок которых «заточены» под традиционные бумажные документы, является тесная взаимосвязь вопроса о наличии письменной формы договора с наличием или отсутствием подписи на документе, в котором выражено волеизъявление стороны на заключение договора. В то же время требование наличия подписи каждой из сторон под документом, выражающим ее волеизъявление, как условие соблюдения письменной формы создает серьезные препятствия для развития электронной коммерции. В отличие от требований к письменной форме, обеспечивающих формализацию содержания договоренностей сторон, подпись выполняет несколько иные функции: идентификацию лица, обеспечение определенности того, что это лицо участвовало в акте подписания, и выражение его согласия с его содержимым.

Вполне можно представить себе письменный документ (или документы), в котором содержатся условия договора, но отсутствуют подписи. Идентификационная и согласительная функции подписи могут компенсироваться поведением стороны, свидетельствующим о том, что именно она является стороной по договору и согласна выполнять его условия (конклюдентные действия). Можно ли говорить о том, что в данном случае письменная форма договора не соблюдена по причине отсутствия надлежащих с точки зрения законодательства подписей? Думается, что такой подход был бы чрезмерно формалистичным и игнорирующим реалии: стороны имеют документ, в котором объективизированы условия договора. Стороны исполняют этот договор, а в случае разногласий разрешают споры со ссылкой на вышеуказанный документ. Основная задача письменной формы договора в данном случае достигнута: стороны имеют объективированный вовне источник его условий, которого нет в случае заключения договора в устной форме. «Ничтожить» договор по причине несоблюдения письменной формы из-за отсутствия подписи в таких случаях было бы явно несправедливо при условии, что речь идет именно о простой письменной форме, а не о квалифицированной нотариальной или требованиях о государственной регистрации. В последних случаях соображения, обусловившие установление законодателем усложненной

формы (защита слабой стороны, участников оборота или публичного интереса), требуют надлежащей формализации волеизъявления сторон. Но в подавляющем большинстве случаев, когда речь идет о простой письменной форме, сторонам должна быть представлена автономия в вопросе выбора способов ее реализации и закон должен защищать сделанный выбор, а не навязывать свои представления о том, каков он должен быть, черпая вдохновение из практики позапрошлых веков.

Примечательно, что Типовой закон ЮНСИТРАЛ об электронной коммерции, а также новейшие акты унификации европейского законодательства дифференцированно подходят к понятиям «письменная форма» и «подпись».

Типовой закон об электронной коммерции исходит из того, что юридические требования, предписывающие использование традиционных бумажных документов, представляют собой основное препятствие для развития современных средств передачи данных. При этом было особо отмечено, что существующие требования о представлении данных в письменной форме зачастую сочетаются с такими не относящимися к «письменной форме» концепциями, как подпись и подлинник[1]. Для разрешения данных препятствий Типовой закон использует так называемый функционально-эквивалентный подход. Суть его заключается в том, что требования к составлению документов на бумаге имеют своей целью обеспечение ряда функций, например: обеспечение того, что документ будет понятен для всех; обеспечение того, что документ не будет со временем изменен; создание возможностей для воспроизведения документа с тем, чтобы каждая сторона имела экземпляр, содержащий одни и те же данные; создание возможности для удостоверения данных посредством подписи; обеспечение того, что документ будет иметь форму, приемлемую для государственных органов и судов.

Поскольку в силу особенностей своей природы электронное сообщение не может рассматриваться в качестве полного эквивалента бумажного документа, Типовой закон об электронной коммерции придерживается гибкого стандарта использования документа в электронной форме: «...требование законодательства предоставить информацию в письменной форме считается выполненным путем предоставления сообщения данных, если содержащаяся в нем информация доступна для последующего использования» (ст. 6). Информация считается

[1] Комментарий к статьям Типового закона «Об электронной торговле» // ЮНСИТРАЛ. Типовой закон об электронной торговле и Руководство по принятию. Нью-Йорк, 1996. С. 36.

доступной для последующего использования, если она является удобочитаемой, разборчивой, и программное обеспечение, необходимое для прочтения такой информации, должно быть доступным[1]. Регламентации вопросов подписания электронного документа в Типовом законе об электронной коммерции посвящена отдельная статья (ст. 7). Как видно, Типовой закон об электронной коммерции четко различает вопросы соблюдения письменной формы договора и наличия подписи.

Также необходимо обратить внимание на решение, которое было выбрано при разработке *DCFR*[2]. Во-первых, данный документ вслед за Типовым законом об электронной коммерции разграничивает вопросы регламентации письменной формы и подписи. Во-вторых, он разграничивает различные виды письменной формы: 1) текстовую форму (*textual form*); 2) текстовую форму на долговечном носителе (*durable medium*); 3) текстовую форму с наличием подписи, соответствующей определенным критериям. В-третьих, в *DCFR* особо отмечается, что письменная форма по общему правилу не предполагает наличия подписи[3]. Вопросы подписи регламентируются *DCFR* отдельной статьей (I-I:106 (3) *DCFR*).

Понятие текстовой формы во многом схоже с тем, как обозначает письменную форму Типовой закон об электронной коммерции. Текстовая форма означает информацию, изложенную с помощью алфавита или иных интеллигибельных символов с использованием средств, обеспечивающих возможность ее прочтения, записи и последующего воспроизведения (ст. I-I:106 (2) *DCFR*)[4]. Информация, изложенная на веб-сайте, подпадает под понятие текстовой формы при условии, что у пользователя имеется возможность ее сохранить на жестком диске.

Текстовая форма на долговечном носителе предполагает помимо выполнения условий обычной текстовой формы изложение информации на носителе, который обеспечивает доступность информации для использования на период, адекватный целям такой информации, а также возможность ее последующего неизменного воспроизведения.

---

[1] Комментарий к статьям Типового закона «Об электронной торговле» // ЮНСИТРАЛ. Типовой закон об электронной торговле и Руководство по принятию. С. 36.

[2] Подробнее о *DCFR* см.: *Клевченкова М.Н.* Кодификация договорного права в Европейском союзе // Законодательство и экономика. 2012. № 7.

[3] Ibid. P. 104.

[4] Весьма широкий подход к пониманию письменной формы, правда, применительно к доказательствам, содержится, например, в ст. 1316 Французского гражданского кодекса, которая предусматривает, что «письменное доказательство вытекает из последовательно расположенных букв, иероглифов, цифр или любых иных знаков или символов, имеющих понятный смысл, независимо от их носителя и от способа их передачи».

Как объясняется в официальном комментарии к *DCFR*, информация будет считаться представленной в текстовой форме на долговечном носителе, если она выражена, к примеру, на бумаге, *CD*- или *DVD*-диске, содержится в отправленном электронном письме. Ключевое отличие от обычной текстовой формы заключается в том, что в данном случае адресат информации получает контроль над содержимым информации и застрахован тем самым от ее одностороннего изменения или уничтожения отправителем. Лицензионные условия, изложенные на диске с программой, охватываются понятием текстовой формы на долговечном носителе. Если условия договора изложены на веб-сайте, то владелец веб-сайта имеет полный контроль над их содержанием. Если те же самые условия были отправлены электронным письмом, то они приобретают «самостоятельную жизнь» и являются более надежным источником договорных условий[1].

Указанные положения *DCFR* не остаются исключительно достоянием доктрины, но находят свое отражение и в общеевропейском законодательстве. Например, понятие текстовой формы на долговечном носителе нашло уже свое отражение в Директиве № 2011/ 83/*EU* «О правах потребителей». Согласно п. 23 преамбулы долговечность носителя определяется возможностью потребителя хранить информацию столько времени, сколько необходимо для защиты его интересов в отношениях с предпринимателем. К долговечным носителям относятся, в частности, бумажный, *USB*-носители, диски *CD*/*DVD*, карты памяти, жесткий диск компьютера, а также сообщения электронной почты.

Представляется, что российское право и доктрина должны также начать проводить разграничение между соблюдением требований к письменной форме и наличием подписи. Простая письменная форма должна считаться соблюденной там, где информация изложена в виде, допускающем ее последующее использование и воспроизведение. Вопросы, связанные с наличием волеизъявления конкретного лица и качеством такого волеизъявления, должны решаться в каждом конкретном случае с учетом всех обстоятельств заключения договора. Иными словами, эти вопросы должны быть не вопросами права, а вопросами факта. Только в таком случае можно обеспечить недискриминационный подход к бумажной и электронной формам договора. И только в тех случаях, когда существо обязательства или иные обстоятельства требуют повышенных требований к волеизъявлению стороны, такие

[1] См. подробнее: Draft Common Frame of Reference (DCFR), Full Edition. Vol. 1 / ed. by Christian von Bar and Eric Clive. Sellier. 2009. P. 106.

требования должны быть отражены в законе в качестве условия признания договора заключенным или действительным.

Рассмотрим теперь способы заключения договора, предусмотренные в п. 2 и 3 ст. 434 ГК РФ подробнее.

3.1. Заключение договора посредством обмена электронными документами (п. 2 ст. 434 ГК РФ)

Данный способ предполагает заключение договора «путем обмена документами посредством почтовой, телеграфной, телетайпной, телефонной, электронной или иной связи, позволяющей достоверно установить, что документ исходит от стороны по договору».

Как следует из данного положения, одним из основных условий действительности заключенного посредством обмена документами договора является возможность достоверно установить, что документ исходит от стороны по договору. Причем, как следует из текста нормы, функция удостоверения факта принадлежности сообщения определенному лицу возлагается не на само содержание документа, а на используемое средство связи[1]. При этом данный пункт сформулирован не самым удачным образом. Как следует из буквального толкования данной нормы, наличие такой возможности презюмируется применительно к обмену документами посредством почтовой, телеграфной, телетайпной, телефонной и электронной средств связи. А вот в отношении иных видов связи наличие такой возможности должно быть прямо доказано заинтересованной стороной. Такое толкование следует из того, что фраза «позволяющей достоверно установить, что документ исходит от стороны по договору» относится с точки зрения правил русского языка к «иной связи», а не ко всем средствам связи, перечисленным в п. 2 ст. 434 ГК РФ. Учитывая, что коммуникации в сети Интернет можно отнести к электронной связи, такое толкование открывает практически неограниченные возможности для заключения договоров в сети Интернет, правда, в совокупности со всевозможными злоупотреблениями, стремление к которым является неотъемлемой частью российского юридического менталитета.

Поэтому более адекватным является толкование, согласно которому использование *любого* из перечисленных в п. 2 ст. 434 ГК РФ средств связи должно позволять установить факт принадлежности документа определенной стороне по договору. В проекте изменений в ГК РФ

[1] *Степанов В.С.* Договоры в сети Интернет: теория и практика // Цивилистические записки. Вып. 2. Екатеринбург, 2002. С. 321.

предполагается уточнить редакцию п. 2 ст. 434 ГК РФ, сместив акцент в вопросе идентификации сторон с используемых средств связи на сами обмениваемые документы. Новая редакция будет предусматривать, что договор может быть заключен путем обмена «письмами, телеграммами, телексами, телефаксами и иными документами, в том числе электронными документами, передаваемыми по каналам связи, позволяющими достоверно установить, что документ исходит от стороны по договору». При этом под электронным документом будет пониматься «информация, подготовленная, отправленная, полученная или хранимая с помощью электронных, магнитных, оптических или аналогичных средств, включая электронный обмен данными и электронную почту».

Обмен электронными документами рассматривается некоторыми авторами в качестве чуть ли не единственно возможного способа заключения договора в сети Интернет[1]. По-видимому, это связано с тем, что любая коммуникация в сети Интернет *с технической точки зрения* осуществляется посредством обмена электронными сообщениями. Вводя определенный адрес в браузер, пользователь отправляет тем самым электронное сообщение, в ответ на которое приходит другое электронное сообщение, реконструируемое средствами браузера в содержимое веб-сайта. Каждый раз, когда пользователь использует какую-либо функциональную возможность веб-сайта или проходит по ссылке, он отправляет определенное электронное сообщение, в ответ на которое на компьютер пользователя приходит электронное сообщение, содержащее «ответ» веб-сайта на его действия. Некоторые авторы при этом прямо заявляют, что при нажатии кнопок ЭВМ происходит обработка и передача информации в виде электрических сигналов, электромагнитных импульсов и т.д., которые следует однозначно толковать как электронный документ[2]. Однако было бы ошибочно *механически* экстраполировать данную особенность функционирования сети Интернет на порядок заключения договора. И уж тем более ошибочно говорить о существовании в сети Интернет некой особой формы договора под названием «конклюдентно-письменная»[3]: во-первых, ГК РФ знает только устную

[1] См., например: *Дмитрик Н.А.* Способы осуществления субъективных гражданских прав и исполнения обязанностей с использованием сети Интернет: автореф. дис. ... канд. юрид. наук. М., 2007. С. 9; *Левашов С.* Виртуальные сделки – реальные права; Правовые аспекты использования интернет-технологий / под ред. А.С. Кемрадж, Д.В. Головерова. С. 148.

[2] *Елин В.М., Жарова А.К.* Указ. соч.

[3] Там же.

и письменную формы договора, а во-вторых, не очень понятно, чего именно «письменного» содержится в электрических сигналах и электромагнитных импульсах.

Обмен электронными документами как способ заключения договора предполагает индивидуализацию электронных сообщений: они адресованы конкретному лицу, а не неопределенному кругу лиц. Иными словами, *заключение договора в порядке п. 2 ст. 434 ГК РФ предполагает адресный характер обмена электронными документами* (посредством электронной почты, *sms*-сообщений и т.п.). Если же коммуникация одной из сторон рассчитана на неопределенный круг лиц и осуществляется с использованием электронных агентов (см. далее), то заключение договора осуществляется посредством акцепта письменной оферты конклюдентными действиями другой стороны (п. 3 ст. 434 ГК РФ). Таким образом, если потребитель размещает заказ на веб-сайте с использованием средств самого сайта, то договор заключается в порядке п. 3 ст. 434 ГК РФ, а если он вступил в переписку с владельцем или менеджером сайта, то условия договора согласовываются в обмениваемых сторонами электронных письмах и договор заключается в порядке п. 2 ст. 434 ГК РФ.

Данное разграничение достаточно четко прослеживается в европейском законодательстве, поскольку с ним связана специфика реализации определенных информационных обязанностей предпринимателя, а также возникновение обязанности по обеспечению возможности исправления ошибок, сделанных при размещении заказа[1]. Российское законодательство хотя и не содержит данного требования в явной форме, но содержит намеки на то, что электронное сообщение, являющееся частью процесса обмена документами при заключении договора, должно позволять достоверно устанавливать, что сообщение исходит от стороны по договору, что предполагает наличие персонализированных коммуникаций между сторонами на стадии заключения договора.

Один из основных вопросов, возникающих при применении п. 2 ст. 434 ГК РФ, заключается в том, какими средствами осуществляется идентификация лица, которое отправило соответствующее сообщение, претендующее на правообразующий статус.

[1] См.: ст. 11 (3) Директивы № 2000/31/ЕС «Об электронной коммерции» (положения о необходимости предоставить подтверждение получения заказа, а также возможность исправления ошибок в заказе неприменимы в случаях заключения договора исключительно посредством обмена электронными сообщениями или иными эквивалентными индивидуальными коммуникациями). См. также: ст. 1369-2, 1369-3 ФГК; ст. II-3:201; Draft Common Frame of Reference (DCFR), Full Edition. Vol. 1 / ed. by Christian von Bar and Eric Clive. Sellier. 2009. P. 241 ff.

Как уже отмечалось ранее, проблема идентификации лица в сети Интернет является одной из основных «болячек», обусловленных ее архитектурой. В условиях, когда потенциальные участники электронной коммерции ранее не имели контактов в реальном физическим мире, а в ряде случаев и не будут их иметь (если договор не только заключается, но и исполняется в сети Интернет), вопрос о доверии к личности контрагента выходит на первый план. Данные получаемые от контрагента посредством сети Интернет, по общему правилу не несут существенных идентификационных характеристик. *IP*-адрес, с которого была осуществлена коммуникация, идентифицирует лишь оконечное устройство, с которого она была сделана, но не само лицо. Администратор доменного имени, определяемый посредством службы *Whois*[1], может не совпадать с оператором интернет-магазина, осуществляющего свою деятельность под таким доменом.

Очевидно, что традиционные способы идентификации лица, принятые в офлайн-мире (собственноручная подпись, печать организации, бумажные документы, выданные государственными органами), даже будучи переведенными в цифровой вид, не будут иметь в электронной среде того же эффекта, что и в обычной жизни, так как отсутствует возможность их верификации путем соотнесения с реальной личностью. Бумажная подпись так или иначе несет в себе отпечаток личности исполнившего ее лица, что обусловливает возможность проведения почерковедческой экспертизы для решения вопроса о ее подлинности[2]. В условиях электронного обмена данными подлинник сообщения неотличим от копии, не имеет собственноручной подписи и не является бумажным документом. Действия, совершаемые в сети Интернет, не имеют столь явно выраженной привязки к конкретной личности и могут быть совершены кем угодно. Как отмечает Л. Лессиг, это связано с тем, что интернет-протоколы не обязывают пользователей идентифицировать себя, а информация о личности пользователя, имеющаяся в локальных точках доступа в Интернет (вроде университетского кампуса или корпоративной сети), ограничена данными

[1] В Рунете данный сервис реализован, в частности, здесь: http://www.ripn.net/nic/whois/index.html

[2] Как отмечают специалисты в области криминалистики, в почерке, проявлением которого является и подпись лица, отражаются индивидуальные особенности личности, совокупность которых является неповторимой и устойчивой. Другими словами, почерк каждого человека имеет свои особенности, которые постоянно проявляются и позволяют при проведении специального исследования идентифицировать личность писавшего даже в том случае, когда лицо умышленно изменяет свой почерк. См.: Криминалистика: учебник для вузов / под ред. Р.С. Белкина. М., 2004. С. 281.

точками и не становится частью самой транзакции, совершаемой в сети Интернет[1].

Однако на определенном этапе развития сети Интернет потребности развития электронной коммерции стали вносить существенные коррективы в первоначальную архитектуру Интернета, направленные в том числе на повышение доверия контрагентов электронных сделок друг к другу. Поскольку проблема идентификации личности в сети Интернет порождена техническими особенностями данной сети, решение данной проблемы также должно иметь преимущественно технический характер. Одними из таких решений стали электронные аналоги собственноручной подписи, которые с той или иной степенью достоверности позволяют сделать вывод о принадлежности сообщения определенному лицу, именуемые в обобщенном виде «электронная подпись» (см. далее).

Для целей вопроса, рассматриваемого сейчас, необходимо отметить, что соблюдение требований п. 2 ст. 434 ГК РФ, а вместе с тем наличие или отсутствие простой письменной формы в договоре, заключенном посредством сети Интернет, будет зависеть от того, имеет ли место какой-либо из видов электронной подписи, предусмотренный действующим законодательством, и если да, то были ли соблюдены требования, предъявляемые к ее использованию. При этом в ряде случаев может получиться парадоксальная ситуация: если письменная форма договора не соблюдена, то это в большинстве случаев влечет лишь невозможность сторон ссылаться на свидетельские показания, но не лишает их возможности приводить письменные и иные доказательства. Распечатки переписки по электронной почте, платежные документы, подписанные акты сдачи-приемки товара и иные письменные доказательства могут служить основанием для признания договора, имевшего место быть, даже несмотря на отсутствие в нем действительной электронной подписи. В результате мы так или иначе (хотя и окольными путями) приходим к тому, что при условии надлежащего сопровождения процесса исполнения договора, заключенного с нарушениями требований к письменной форме, можно тем не менее ссылаться на его наличие. Нормы российского законодательства о последствиях несоблюдения письменной формы являются более либеральными, чем нормы, устанавливающие требования к этой самой письменной форме. Так что бóльшая часть сделок в сфере электронной коммерции, заключаемых посредством обмена документами, являются действительными. Сомнения в соответствии их письменной формы эффективно устраняются

[1] *Lessig Lawrence*. Code: Version 2.0. Basic Books. 2006. P. 35.

наличием документов, относящихся к исполнению договора хотя бы одной стороной.

3.2. Заключение договора посредством совершения конклюдентных действий (п. 3 ст. 434 ГК РФ)

Далеко не все договоры, заключаемые в электронной среде, заключаются посредством обмена электронными документами. Как отмечалось ранее, заключение договора путем обмена документами предполагает индивидуализированный характер документов, которыми обмениваются стороны. Если же договор с интернет-магазином заключается на основании публичной оферты, то в данном случае нет обмена документами для целей п. 2 ст. 434 ГК РФ, а имеет место заключение договора по п. 3 ст. 434 ГК РФ (акцепт оферты путем конклюдентных действий). Получение автоматического подтверждения от магазина о принятии заказа будет доказательством получения оферентом акцепта со стороны потребителя[1].

Заключение договора по п. 3 ст. 434 ГК РФ осуществляется на основании волеизъявления лица, выраженного не в его формальных письменных заявлениях, а в его поведении.

Признание договора заключенным в таких случаях привносит гибкость и оперативность в процесс его заключения, что жизненно необходимо для электронной коммерции. В сфере электронной коммерции договор, заключенный конклюдентными действиями, может принимать форму соглашений, заключаемых путем щелчка мышью (*click-wrap*), и соглашения, заключаемого путем использования вебсайта (*browse-wrap*).

Под *click-wrap*-соглашением понимается договор, заключаемый в электронном виде посредством щелчка мышью одной из сторон по клавише «я согласен», сопровождающей текст такого договора. Данные соглашения впервые возникли в сфере лицензирования программного обеспечения, придя на смену так называемым оберточным лицензиям, при которых условия договора излагались на упаковке материального носителя компьютерной программы. В настоящее время *click-wrap*-соглашения широко используются и в иных сферах, не связанных с лицензированием компьютерных программ, например при предоставлении доступа к контенту или сервисам в сети Интернет.

[1] *Зак А.Ю.* Нарушения прав потребителей при ненадлежащем исполнении договора дистанционной продажи в Интернете и способы их преодоления // Современное право. 2010. № 8.

С учетом достаточно необычного способа заключения договора с точки зрения классической доктрины договорного права и ряда сопряженных с этим правовых проблем не вызывает удивления тот факт, что с момента появления подобных соглашений ведутся споры об их юридической силе.

Впервые вопросы о юридической силе *click-wrap*-соглашений и «оберточных» лицензий, выступающих в качестве их предшественника, были предметом рассмотрения американских судов. Изначально суды отказывались признавать действительность подобных соглашений по причине отсутствия явно выраженного согласия с их условиями со стороны лицензиата и игнорировали положения, содержащиеся в них при рассмотрении споров[1]. Ситуация кардинально изменилась после вынесения Седьмым окружным судом США решения *ProCD, Inc. v. Zeidenberg*[2]. Ключевую роль в аргументации суда сыграл тот факт, что у ответчика имелась возможность ознакомиться с условиями лицензионного соглашения до начала использования продукта, а также право вернуть его в случае несогласия с такими условиями. Поскольку ответчик этого не сделал, то, по мнению суда, это можно рассматривать как согласие с выставленными условиями и, как следствие, возникновение договора.

Указанная логика легла в основу дальнейшей судебной практики, в которой признавались действительными *click-wrap*-соглашения. Как указал один из судов, если суды признают действительными условия «оберточных» лицензий, то условия *click-wrap*-соглашений тем более должны быть признаны таковыми, поскольку согласие пользователя с ними является более явно выраженным[3].

Исторически первым судебным решением, в котором была признана юридическая сила собственно *click-wrap*-соглашения, являлось решение по делу *Hotmail Corp. v. Vans Money Pie, Inc.*, в котором соглашение о порядке пользования почтовым ящиком на сайте *www.hotmail.com* было признано действительным, включая условие о запрете рассылки спама[4].

Другим решением, часто упоминаемым при рассмотрении вопросов, связанных с юридической силой *click-wrap*-соглашений, является решение по делу *Caspi v. Microsoft Network, L.L.C*[5]. В данном деле суд штата

[1] Step-saver Data Systems, Inc. v. Wyse Technology, 939 F.2d 91 (3rd Cir. 1991).
[2] 908 F. Supp. 640, 644 (W.D. Wis. 1996).
[3] i.LAN Systems, Inc. v. NetScout Service Level Corp., 183 F. Supp. 2d 328 (D. Mass. 2002).
[4] No. C-98 JW PVT ENE, C98-20064JV, (N.D. Cal Apr. 1998).
[5] 732 A.2d 528, 529 (N.J. Super. Ct. App. Div. 1999).

Нью-Джерси признал действительным соглашение об оказании сервисов *Microsoft Network (MSN)*, в соответствии с которым все споры должны были рассматриваться в *King County* штата Вашингтон. Поскольку пользователь подал иск не по установленной договором подсудности, иск был отклонен. Суд сослался на решение Верховного суда США, в котором было признано действительным условие о договорной подсудности, изложенное в стандартных условиях перевозчика, к которому делалась отсылка мелким шрифтом на билете[1]. По мнению суда, между данными случаями имеется непосредственное сходство, поскольку существенных различий между условиями на бумажном носителе и на электронном носителе нет. В обоих случаях у потребителей была потенциальная возможность предварительно ознакомиться с условиями договора. Причем соответствующее условие соглашения с *Microsoft Network* не было выполнено мелким шрифтом, равно как не предпринимались попытки скрыть его от взора пользователя иным способом. Все это свидетельствовало, по мнению суда, о действительности соответствующего условия, поэтому интересы гражданского оборота и публичного порядка требовали от суда подтвердить его юридическую силу.

Конечно, нельзя сказать, что американские суды безоговорочно признают юридическую силу оберточных лицензий и *click-wrap*-соглашений. Существуют решения, в которых такие соглашения признавались не имеющими юридической силы. При этом в качестве основания для такого решения выступала недобросовестность условий, содержащихся в таких соглашениях, а не противоречие механизма его заключения каким-либо положениям договорного права[2].

Судебная практика и доктрина европейских стран также высказываются в пользу жизнеспособности конструкции *click-wrap*. Основу для вывода о действительности такого механизма заключения договора заложила ст. 9 Директивы № 2000/31/ЕС «Об электронной коммерции». Она предписывает странам – участницам ЕС обеспечить в их национальном праве возможность заключения договоров в электронном виде, в том числе уделив особое внимание тому, чтобы существующие положения о порядке заключения договоров не препятствовали юридической силе электронных договоров.

---

[1] Carnival Cruise Lines, Inc. v. Shute, 499 U.S. 585 (1991).

[2] См., например: Comb v. PayPal, Inc. 218 F. Supp. 2d 1165 (N.D. Cal. 2002). В данном решении недобросовестными были признаны условия *click-wrap*-соглашения о рассмотрении споров по месту нахождения провайдера услуг, в то время как пользователь находился в другом штате; условие о праве провайдера услуг на одностороннее изменение условий соглашений без уведомления пользователя и некоторые другие.

Договор, заключенный посредством щелчка мышью (*click-wrap*), признается действительным в Англии[1], Италии[2], Франции[3], Германии[4], Канаде[5] и ряде других стран.

Российское право не содержит специальных положений, посвященных соглашениям, заключаемым посредством щелчка мыши. Следовательно, данный механизм заключения договора должен оцениваться через призму общих положений о заключении договора.

В соответствии с п. 3 ст. 434 ГК РФ письменная форма договора считается соблюденной, если письменное предложение заключить договор принято в порядке, предусмотренном п. 3 ст. 438 ГК РФ. Данный пункт в свою очередь предусматривает, что совершение лицом, получившим оферту, в срок, установленный для ее акцепта, действий по выполнению указанных в ней условий договора (отгрузка товаров, предоставление услуг, выполнение работ, уплата соответствующей суммы и т.п.) считается акцептом, если иное не предусмотрено законом, иными правовыми актами или не указано в оферте.

Таким образом, для того чтобы договор считался заключенным по п. 3 ст. 434 ГК РФ, необходимо, чтобы имели место 1) письменная оферта и 2) действие лица по выполнению указанных в ней условий.

При заключении *click-wrap*-соглашения имеет место предложение заключить договор, исходящее от правообладателя (провайдера). Данное предложение изложено в письменной форме, т.е. с использованием алфавита, набора букв и иных письменных символов[6]. Такое предложение можно расценивать как оферту, поскольку оно, как правило, содержит указания на его юридически обязывающий характер и намерение оферента считать себя связанным им в случае его акцепта

---

[1] *Reed C., Angel J.* Op. cit. P. 110. В английской доктрине часто обсуждается дело Beta Computers (Europe) Ltd v. Adobe Systems (Europe) Ltd (1996. S.L.T. 604), где лицензионное соглашение *click-wrap* было признано действительным шотландским судом.

[2] Giudice di pace di Partanna n. 15/2002, case No 206/2001 R.G.A.C. // http://www.riceragiuridica.com/sentenze/index.php?num=868. В данном деле было признано действительным соглашение о подсудности, включенное в соглашение, возникающее при размещении заказа на веб-сайте.

[3] См.: ст. 1369-4, 1369-5 ФГК, посвященные процессу заключения договора в электронной форме (введены в действие Ордонансом № 2005-674 от 16 июня 2005 г.).

[4] BGH, 7.11.2002. NJW 2002, 363. В данном деле суд принял во внимание для целей определения наличия договорных отношений между истцом и ответчиком факт выражения последним согласия со стандартными условиями онлайн-аукциона посредством клика на кнопку «я согласен», без чего товар не мог быть выставлен на продажу, что свидетельствовало, по мнению суда, о совершении ответчиком оферты.

[5] Rudder et al. v. Microsoft Corp. Ontario Supreme Court. 1999, 2 C.P.R. (4th) 474.

[6] *Дмитрик Н.А.* Способы осуществления субъективных гражданских прав и исполнения обязанностей с использованием сети Интернет. С. 18.

пользователем. Также оно обычно содержит необходимые существенные условия соответствующего договора либо непосредственно, либо инкорпорируя их путем отсылки к иным документам.

Поскольку в тексте соглашения имеются указания на то, что, кликая по кнопке «я согласен», пользователь выражает свое согласие с условиями договора, совершение таких действий является действием по выполнению указанных в оферте условий, т.е. акцептом письменной оферты конклюдентными действиями.

Для повышения шансов на признание наличия соглашения целесообразно принимать во внимание те обстоятельства, которые учитывали зарубежные суды при решении вопроса о наличии действительного соглашения между сторонами, заключенного по модели *click-wrap*[1].

Во-первых, пользователю должна быть обеспечена возможность предварительного ознакомления с условиями такого договора до того момента, как договор будет считаться заключенным. При этом желательно, чтобы кнопка «согласен» находилась в конце текста такого соглашения и могла быть активизирована только при условии скроллинга всего текста с начала и до конца. Можно усилить выражение согласия лица с условиями соглашения добавлением фразы «*С условиями договора ознакомился* и согласен».

Во-вторых, пользователь должен иметь возможность отказаться от принятия его условий и от совершения сделки соответственно. Свобода принятия решения о заключении или незаключении договора является важным элементом автономии воли лица, особенно если этот договор относится к категории договоров присоединения. Тот факт, что имея возможность отказаться от заключения договора на условиях, с которыми он мог предварительно ознакомиться, лицо тем не менее продолжило процесс заключения договора, является сильным аргументом в пользу наличия действительного волеизъявления с его стороны на заключение такого договора.

В-третьих, принятие условий соглашения должно являться необходимым *с технической точки зрения* условием получения услуги, доступа к информационному ресурсу, программному продукту. Без выражения пользователем согласия с условиями соглашения невозможен дальнейший процесс заключения договора (размещения заказа) или получения доступа к тем благам, по поводу которых заключается договор.

---

[1] Online Contract Formation. Ed. by Stephan Kinsella and Andrew Simpson. Oceana Publications: N.Y., 2004. P. 421; *Кучер А.Н.* Теория и практика преддоговорного этапа: Юридический аспект. М., 2005. С. 325–326.

В-четвертых, учитывая, что при формировании заказа, сопровождающегося заключением *click-wrap*-соглашения, используются автоматизированные средства, на стадии заключении договора существует повышенная вероятность совершения ошибок при вводе данных. Особенно это касается потребителей, которые заполняют соответствующую форму на веб-сайте. В связи с этим многие законы об электронной коммерции предусматривают специальные положения, направленные на минимизацию возможных ошибок. Директива ЕС № 2000/31/ЕС «Об электронной коммерции» указывает, что национальное законодательство должно предусматривать обязанность обеспечивать наличие специальных средств для исправления ошибок, допущенных при вводе (ст. 11 (2)). Такие специальные механизмы должны быть во всяком случае предусмотрены применительно к договорам с потребителями. В предпринимательских договорах стороны могут своим соглашением исключить их применение. Однако безотносительно к субъектному составу договора данные положения неприменимы при заключении договора путем обмена индивидуализированными сообщениями. Данное положение подкрепляется выделением отдельной обязанности по информированию потребителей о наличии таких средств (ст. 10 (1) (*c*)). Данные предписания были имплементированы в национальное законодательство различными способами. Некоторые страны (например, Италия, Ирландия, Финляндия) установили административную ответственность за их несоблюдение, другие страны предусмотрели наличие такого механизма в качестве условия действительности договора (Франция) или возможного фактора, способного повлечь его недействительность (Голландия) или расторжение (Германия, Великобритания). Несмотря на то что в России в настоящий момент подобные положения отсутствуют, наличие специальных механизмов, обеспечивающих возможность исправления ошибок, может учитываться при определении «качества» волеизъявления потребителя на заключение соответствующего договора.

Наконец, в-пятых, крайне важно обеспечить возможность распечатать и сохранить условия такого соглашения. Необходимость обеспечения такой возможности предписывается европейским[1] и американ-

[1] См.: ст. II-3:105 (2) предусматривает обязанность предпринимателя при заключении договора электронным способом представлять договорные условия в текстовой форме (*textual form*). Текстовая форма означает представление информации с использованием знаков алфавита или иных символов средствами, допускающими ее прочтение, запись и воспроизведение на материальном носителе (I-1:106 (2)). Draft Common Frame of Reference (DCFR), Full Edition. Vol. 1 / ed. by Christian von Bar and Eric Clive. Sellier. 2009. P. 223.

ским правом[1]. Существуют даже отдельные инициативы по стандартизации технических средств, используемых при создании *click-wrap*-соглашений, которые позволили бы сохранять каждое такое соглашение на жесткий диск пользователя при каждом клике по кнопке «согласен»[2], что могло бы быть весьма полезным, учитывая, что такие соглашения имеют тенденцию периодически изменяться предпринимателем в одностороннем порядке.

В Европе вскоре появится еще одно условие для подобного рода соглашений. В соответствии со ст. 8 (2) Директивы № 2011/83/*EU* «О правах потребителей»[3], если договор заключается электронным способом и предполагает наличие на стороне потребителя обязательства по оплате, то согласительная кнопка или иная аналогичная функция, кликая на которую потребитель выражает согласие с условиями заказа, должна быть обозначена как «заказ с обязательством оплаты» или иным аналогичным и достаточно определенным способом. В противном случае такой заказ (договор) не будет обязательным для потребителя. Таким образом, если оформление заказа, предполагающего осуществление оплаты, завершается выражением согласия с условиями *click-wrap*-соглашения, то вместо обычной формулировки «Согласен» или «С условиями ознакомился и согласен» должна быть использована формулировка вроде «С условиями соглашения и порядком оплаты заказа ознакомился и согласен». Положения указанной Директивы должны быть имплементированы и введены в силу до 13 июня 2014 г. Несмотря на то что положения директив и иных актов ЕС не являются обязательными на территории России, представляется, что их добровольная имплементация российскими магазинами весьма желательна, тем более что рано или поздно сходные положения будут введены и в российское потребительское законодательство, как это уже имело место применительно ко многим положениям о дистанционных продажах. Если же российский интернет-магазин допускает возможность заключения договоров с потребителями, проживающими в европейских странах, то следование положениям европейского законодательства превращается из желательного в практически обязательное.

---

[1] Единообразный закон США об электронных сделках в ст. 8 предписывает обеспечить возможность сохранения и последующего использования текста электронного соглашения, в противном случае договор может быть признан судом совершенным с нарушением письменной формы.

[2] *Leff L., Ahmad I. et al.* XML for Click-Through Contracts // International Journal of Law and Information Technology. Vol. 17. No 2. 2008.

[3] Directive 2011/83/EU «On consumer rights» // Official Journal of the European Union. L 304/64. 22.11.2011.

В целом можно сделать вывод, что соглашения *click-wrap* вполне имеют право на существование в рамках российского права[1]. Не только потому, что укладываются в п. 3 ст. 434 и п. 3 ст. 438 ГК РФ, но и потому, что применительно к их предшественникам – «оберточным» лицензиям – отечественные суды и представители доктрины обычно относятся благосклонно во многом благодаря положениям законодательства (п. 3 ст. 1286 ГК РФ[2]), прямо предусматривающим такой особый порядок заключения договора. Если же мы признаем действительность «оберточных» лицензий, где согласие пользователя с ее условиями выражено гораздо менее очевидным образом, то *click-wrap*-соглашения должны признаваться и подавно, так как в них дается возможность предварительно ознакомиться с условиями и согласие с ними является выраженным в явной форме и обеспечивается техническими средствами.

Концепция *browse-wrap*, иногда именуемая также «*web-wrap*» (соглашение, принимаемое путем просмотра веб-сайта), относится к ситуациям, когда условия договора доступны для ознакомления по ссылке на веб-сайте, но пользователь не выражает согласия с его условиями в явной форме[3]. Предполагается, что в качестве акцепта выступает фактическое использование веб-сайта, компьютерной программы, онлайн-сервиса или иного блага. Насколько соответствующие действия могут свидетельствовать об акцепте условий такого соглашения, следует анализировать в каждом конкретном случае. С одной стороны, как отмечалось ранее, судебная практика допускает квалификацию в качестве акцепта действий лица по использованию блага, являющегося предметом оферты[4]. С другой стороны, в таких случаях усложняется доказывание того факта, что пользователь был заранее (т.е. до начала использования) ознакомлен с условиями соглашения.

Типичным примером данных соглашений являются различного рода правила использования веб-сайта, ссылки на которые обычно

---

[1] Действительность *click-wrap*-соглашений признается в отечественной доктрине. См.: *Гаврилов Э.П.* Какие изменения предлагается внести в главу 70 ГК РФ «Авторское право»? // Патенты и лицензии. 2012. № 1; *Кучер А.Н.* Указ. соч. С. 327; *Калятин В.О.* Право в сфере Интернета. С. 336.

[2] Ранее соответствующее положение было предусмотрено в п. 3 ст. 14 Закона РФ от 23сентября 1992 г. № 3523-I «О правовой охране программ для электронных вычислительных машин и баз данных».

[3] *Davidson A.* The Law of Electronic Commerce. Cambridge University Press. 2009. P. 70.

[4] Аналогичный подход имеет место и в зарубежной практике: «В случаях, когда благо предлагается на определенных условиях и другая сторона принимает решение воспользоваться им, будучи осведомленной о таких условиях, такое поведение свидетельствует об акцепте договорных условий, которые становятся обязательными для такой стороны». Register.com Inc. v Verio Inc. 356 F.3d 393 (2nd Cir. N.Y., 2004).

содержатся внизу веб-страницы данного сайта. Эти правила предусматривают, что просмотр или иное использование сайта предполагает выражение согласия с данными условиями. Появление подобных правил связано с опасениями владельцев сайтов, что размещение информации в сети Интернет, доступной бесплатно, может создать иллюзию того, что пользователи вправе ее использовать гораздо шире, чем разрешает закон или предполагает владелец сайта. Подобно тому, как собственник недвижимости может устанавливать правила поведения и ограничения для ее потенциальных посетителей, владельцы веб-сайтов желают установить правила и ограничения для посетителей своих сайтов[1].

Как правило, все условия правил пользования сайтом можно разделить на информационные (содержащие уведомления о правах на интеллектуальную собственность, статусе владельца сайта[2]) и регулятивные (содержащие регламентацию прав и обязанностей пользователей). Так, условия использования сайта *Amazon.com* содержат помимо всего прочего порядок представления заявлений о нарушении авторских прав, порядок рецензирования товаров, запреты на коммерческое использование размещенной на сайте информации, использование роботов для сбора информации на сайте, технологий фрейминга, метатегов или иных скрытых текстов, использующих слова *Amazon.com*[3].

К регулятивным условиям *browse-wrap*-соглашений можно отнести также различного рода сопутствующие условия вроде ограничений ответственности, гарантий, оговорки о применимом праве и порядке рассмотрения споров.

Переходя к вопросу о действительности *browse-wrap*-соглашений, следует отметить, что в России пока данный вопрос не был предметом рассмотрения суда. В связи с этим имеет смысл обратиться к существующей зарубежной практике.

---

[1] *Sandeen S.* The Sense and Nonsense of Web-site terms of Use Agreements // Hamline Law Review. No 26. 2003. P. 525, 528.

[2] Например, условия Пользовательского соглашения веб-сайта «*eBay*» (4 февраля 2013 г.) содержат пояснение о том, что *eBay* не является организатором аукциона «в традиционном понимании этого слова. Наши сайты представляют собой место, позволяющее пользователям предлагать, продавать и покупать практически все, в любое время, из любого места, в различных ценовых форматах и в разных местах, таких как магазины, в формате фиксированной цены или формате аукциона. Мы не участвуем в фактических сделках между покупателями и продавцами» // http://pages.ebay.com/ru/ru-ru/help/policies/user-agreement.html?rt=nc

[3] Amazon.com Conditions of Use (дата обращения 5 декабря 2012 г.) // http://www.amazon.com/gp/help/customer/display.html/ref=footer_cou?ie=UTF8&nodeId=508088

Американские суды, которые одними из первых столкнулись с данной конструкцией, в целом достаточно осторожно подходят к ней, не высказываясь тем не менее однозначно о ее возможной недействительности как таковой.

Одним из наиболее известных зарубежных судебных споров, где рассматривались вопросы действительности подобной конструкции, является дело *Ticketmaster Corp. v. Tickets.com Inc.*[1] Веб-сайт истца представлял собой онлайн-сервис по приобретению билетов. Условия его использования, ссылка на которые содержалась внизу страниц сайта, предусматривали, что любой пользователь, который проходит далее заглавной страницы, соглашается с тем, что информация, размещенная на нем, предназначена для личного пользования и не может быть использована в коммерческих целях, а также с запретом на использование глубоких ссылок[2]. Ответчик также осуществлял деятельность по продаже билетов через Интернет и размещал глубокие ссылки на информацию, содержащуюся на веб-сайте истца. Истец ссылался помимо всего прочего на нарушение подобными действиями условий соглашения об использовании его веб-сайта. Суд не согласился с данным аргументом. Допуская в принципе возможность возникновения договора вследствие использования веб-сайта в случаях, когда лицо было заведомо знакомо с его условиями, суд указал, что сам по себе факт размещения на веб-сайте условий его использования не создает с необходимостью договорные отношения с каждым, кто его использует. Суд при этом исходил из стандартного поведения, характерного для большинства пользователей, которые предпочитают перейти как можно скорее к странице с интересующим их содержимым, нежели чем специально тратить свое время на ознакомление с условиями, на которые сделана ссылка мелким шрифтом где-то внизу сайта. Как видно, основным препятствием признания условий *browse-wrap*-соглашения было отсутствие доказательств наличия согласия ответчика с такими условиями[3].

[1] 54 USPQ 2d 1344 (C.D. Cal. 2000).

[2] Под глубокой ссылкой понимается гиперссылка, которая отсылает на конкретную страницу или ресурс веб-сайта, а не на его заглавную страницу.

[3] Из недавних споров, где суд отказал в признании *browse-wrap*-соглашения заключенным, следует упомянуть дело Hines v. Overstock.com, Inc. 668 E Supp. 2d 362 (E.D.N.Y. 2009). В данном случае гиперссылка на условия договора содержалась внизу страницы веб-сайта и единственное уведомление о юридическом значении данного документа содержалось лишь в нем самом. Суд пришел к выводу, что при таких обстоятельствах условия договора были неочевидны для посетителя сайта и он не мог считаться связанным ими.

Другим известным делом, в котором фигурировала конструкция *browse-wrap*, является дело *Specht v. Netscape Communications Corp.*[1], где стоял вопрос о действительности условий лицензионного соглашения. Компания *Netscape*, выступая в качестве правообладателя программного продукта, предоставляла пользователям возможность загрузить программу, приводя ее лицензионные условия на странице загрузки в виде гиперссылки. Причем данная ссылка вместе с фразой «ознакомьтесь и примите лицензионные условия использования программы *Netscape SmartDownload* до ее загрузки и использования» была расположена существенно ниже, нежели кнопка «загрузить», и требовала пролистывания страницы. Суд признал, что при таких обстоятельствах пользователь не связан условиями такого соглашения, в том числе и арбитражной оговоркой, содержащейся в нем, поскольку он не выразил свое согласие с ними в явной форме, как это имеет место в случае с «оберточными» лицензиями и особенно – *click-wrap*-соглашениями[2]. Данное решение нередко используется в качестве основного аргумента противников признания действительности *browse-wrap*-соглашений, хотя со времен его принятия прошло немало времени и критерии действительности таких соглашений стали более отточенными[3].

В настоящее время одним из наиболее цитируемых дел по вопросам *browse-wrap*-соглашений является *Register.com, Inc. v. Verio, Inc.*[4] Здесь истец осуществлял продажи доменных имен и был обязан в соответствии с требованиями *ICANN* обеспечить наличие сервиса *Whois*, содержащего контактные данные владельцев таких доменных имен. Условия предоставления данного сервиса предусматривали возможность использования полученных данных исключительно в некоммерческих целях. Ответчик осуществлял неоднократную навязчивую рекламу своих услуг клиентам истца, данные о которых были получены с использованием сервиса *Whois*. Проблема заключалась в том, что условия предоставления сервиса появлялись уже после того, как запрос был сделан и данные получены. Однако ответчик многократно использовал данный сервис, несмотря на требования истца прекратить свою рекламную деятельность. По мнению суда, в данном случае можно было говорить о наличии возникновения обязательств в отношении ответчика из *browse-wrap*-

[1] 150 F. Supp. 2d 585 (SD NY 2001).

[2] В настоящее время *browse-wrap* не используются в отношении лицензионных договоров, проприетарного программного обеспечения, будучи полностью вытесненными более удобными и «безопасными» *click-wrap*-соглашениями.

[3] *Moringiello J., Reynolds W.* Survey of the Law of Cyberspace – Electronic Contracting Cases 2007–2008 // The Business Lawyer. No 64. November 2008. P. 204.

[4] 356 F.3d 393 (2nd Cir. 2004).

соглашения, поскольку он *систематически* использовал соответствующий сервис и условия такого соглашения стали ему известны уже после первого же запроса. При этом суд привел интересную аналогию, сравнив действия ответчика с покупателем, который, находясь на рынке у прилавка с яблоками, надкусывает яблоко в расчете попробовать его, а потом замечает ценник: «Яблоки, 50 центов». Суд отметил, что на первый раз возможно и допустимо освободить такого покупателя от оплаты, но было бы крайне несправедливо позволить тому же самому покупателю каждый день приходить к прилавку и надкусывать яблоки без их оплаты, ссылаясь на то, что он не заметил ценника.

Как видно, именно систематический и явно недобросовестный характер действий ответчика послужил основанием для вывода суда о заключенности *browse-wrap*-договора. Данный прецедент дает основания для размышлений о том, что условия *browse-wrap*-соглашений могут иметь юридическую силу как минимум в отношении систематических пользователей веб-сайтов[1]. Учитывая, что современные технологии позволяют отследить статистику посещения веб-сайта с компьютера определенного пользователя, использование данного критерия не должно вызвать больших проблем на практике.

В Канаде *browse-wrap*-соглашение было признано заключенным, правда, в этом деле его сторонами также выступали предприниматели – профессионалы в сфере электронной коммерции. Суд признал ответчика, который осуществлял модификацию и копирование размещенной на веб-сайте информации на своем веб-сайте, нарушившим условия такого соглашения. При этом особую роль сыграл тот факт, что ответчик регламентировал условия использования своего веб-сайта также *browse-wrap*-соглашением на схожих условиях, из чего суд сделал вывод, что «ответчику должно было быть известно о наличии и содержании *browse-wrap*-соглашения истца и его значимости для бизнеса последнего»[2].

---

[1] Указанный подход нашел свое отражение и в других решениях. См.: Southwest Airlines Co. v. BoardFirst, L.L.C. No 3:06-CV-0891-B (N.D. Tex. Sept. 12, 2007) (в данном деле обе компании являлись профессионалами в соответствующей сфере – пассажирских авиаперевозок и обе использовали *browse-wrap*-соглашения в своей деятельности. Это подтолкнуло суд к выводу о наличии заключенного соглашения в данном случае). В другом деле суд пришел к выводу о признании покупателя билета на концерт связанным условиями *browse-wrap*-соглашения, содержащегося на веб-сайте, где был приобретен билет, в том числе и потому, что данный покупатель, с его слов, часто посещал подобные концерты и заказывал билеты онлайн. Druyan v. Jagger 508 F Supp. 2d 228, 232 (S.D.N.Y. 2007).

[2] The Canadian Real Estate Association v. Sutton (Québec) Real Estate Services Inc, Québec Supreme Court. Case No 500-05-074815-026. 10 April 2003.

Имеющаяся практика европейских судов по вопросам действительности *browse-wrap*-соглашений также неоднозначна. Так, немецкий суд подошел достаточно формально к данному вопросу и признал такое соглашение не имеющим юридической силы, поскольку его условия не были надлежащим образом доведены до сведения другой стороны. Суд указал, что «такие условия должны быть либо неотъемлемой частью оферты, либо обозначены таким образом, чтобы пользователь не мог их пропустить. Если же пользователь сам должен предпринимать действия по их поиску, то такие условия не становятся частью договора»[1]. Голландский суд, напротив, признал компанию, использовавшую доступную в сети Интернет базу телефонных номеров истца, связанной условиями использования такой базы данных, доступными по ссылке в левом нижнем углу страницы веб-сайта. Как отметил суд, ответчик в силу специфики своей деятельности является профессионалом в сфере использования интернет-контента и как таковой должен был ожидать, что использование такого контента сопровождается определенными условиями. Факт использования ответчиком контента с сайта означал тем самым, по мнению суда, его согласие с указанными условиями, в том числе с условием об ответственности за рассылку спама с использованием данного веб-сайта[2].

Как видно, конструкция *browse-wrap*-соглашения является весьма спорной. Основная претензия иностранных судов, актуальная и для российского права, заключается в том, что условия таких соглашений не доводятся до сведения другой стороны должным образом[3]. Вероятность того, что такие условия будут иметь юридическую силу в случае, если в качестве другой стороны будет выступать физическое лицо – потребитель, крайне невелика. Гораздо больше шансов на признание юридической силы таких соглашений появляется в отношении контрагентов-предпринимателей, основной вид деятельности которых связан со сферой электронной коммерции. В таких случаях имеется возможность сослаться на сложившиеся обычаи делового оборота, согласно которым использование материалов веб-сайтов регламентируется специальными условиями, разрабатываемыми их владельцами, о чем должно быть известно лицам, которые используют веб-сайты в своей коммерческой деятельности.

В связи с вышеизложенным можно предложить следующую рекомендацию. Если информация на веб-сайте представляет собой высокую

[1] Oberlandesgericht Hamburg. No 3 U 168/00. 13.06.2002.

[2] Netwise v. NTS Computers. 5 December 2002. Computerrecht 2003/02. P. 149.

[3] *Femminella J.* Online Terms and Conditions: Bound by the Web // St. John's Journal of Legal Commentary. No 17. 2003. P. 102.

коммерческую ценность, в связи с чем необходима особая регламентация ее использования (получение предварительного согласия владельца, запрет на глубокие ссылки и пр.), целесообразно использование конструкции *click-wrap*-соглашения в отношении каждого, кто входит на сайт[1]. Отсутствие технической возможности приступить к просмотру сайта без принятия условий соглашения является более надежным способом заключения договора, нежели наличие ссылки на условия договора в отсутствие иных, явно выраженных действий пользователя, свидетельствующих о его согласии с ними. Если же режим использования информации на сайте не является особокритичным для владельца, а ему просто необходимо довести до сведения пользователя ее правовой статус (например, ее распространение на условиях *Creative Commons*) и иметь дополнительные меры защиты от недобросовестных действий конкурентов, то в таком случае может быть достаточно и обычного *browse-wrap*-соглашения. Так или иначе, основные адресаты таких соглашений, конкурирующие веб-сайты, скорее всего, тоже используют подобные соглашения на своих собственных сайтах, что дает дополнительный аргумент в пользу того, что им должно было быть известно о наличии такого соглашения и что подобные соглашения являются сложившимся обыкновением в сети Интернет.

§ 4. Электронная подпись

Положения об электронной подписи являются неотъемлемой частью любого современного законодательства в сфере электронной коммерции.

Одной из основных задач, стоящих перед законодателем при разработке правовых норм в данной области, является выбор между категориями «электронная подпись» (ЭП) и «электронная цифровая подпись» (ЭЦП), поскольку они отражают различные технические и методологические подходы к средствам идентификации лиц в электронной среде. Понятие «электронная подпись» является наиболее широким и включает в себя любое обозначение (буквенное, символьное, звуковое), присоединенное к подписываемому документу и используемое лицом с намерением подписать документ, т.е. идентифицировать себя и выразить свое согласие с его содержимым. Это могут быть как

[1] Еще раз следует подчеркнуть, что это имеет смысл только в том случае, когда цель оправдывает средства, поскольку считается, что использование *click-wrap*-конструкций в качестве условия использования веб-сайта может отпугнуть часть пользователей. См.: *Tracy J.* Browsewrap agreements // B.U.J. Sci & Tech. L. No 11. 2005. P. 165.

самые простые с технической точки зрения методы проставления подписи (вставленная в документ отсканированная собственноручная подпись лица, обычное проставление имени в конце документа), так и технически сложные способы, связанные с использованием средств криптографии.

Термин «электронная цифровая подпись» обозначает разновидность электронной подписи, в которой используются криптографические средства, обеспечивающие не только идентификацию, но и целостность сообщения. Как правило, такая подпись основана на криптографии с использованием публичных ключей[1]. Таким образом, понятие «электронная цифровая подпись» является одним из видов электронной подписи и так или иначе предполагает наличие тесной связи с определенной технологией шифрования, лежащей в ее основе.

В зависимости от того, какой концепции электронной подписи законодатель отдает предпочтение, можно с определенной долей условности выделить три основные модели регулирования электронных подписей[2]:

1) модель, в которой регулирование электронных подписей привязывается к использованию определенной технологии, признаваемой достаточно надежной. Электронные подписи, не использующие такую технологию, не признаются действительными. Иными словами, предметом регулирования в данном случае являются именно электронные *цифровые* подписи. Примером реализации данного подхода являются Германия, Италия, Малайзия и до недавнего времени – Россия;

2) модель, при которой регулирование электронных подписей является максимально технологически нейтральным и направлено на устранение существующих барьеров к использованию электронных документов[3]. Стороны сами определяют степень надежности подписи и технологию, используемую для ее создания. Данный подход свойствен для США, Канады;

3) сочетание вышеуказанных подходов, в котором электронные подписи признаются легитимными в принципе, но существует особый привилегированный вид электронных подписей, отвечающий опреде-

[1] См., например: п. 33 Руководства по принятию Типового закона ЮНСИТРАЛ об электронных подписях // http://www.un.org/ru/documents/decl_conv/conventions/pdf/uncitral.pdf

[2] *Savin A.* Op. cit. Во многом схожая классификация предлагается и Кристиной Спирелли. См.: *Spyrelli C.* Electronic Signatures: A Transatlantic Bridge? An EU and US Legal Approach Towards Electronic Authentication // The Journal of Information, Law and Technology. 2002. No 2.

[3] А не на создание взамен них новых, как это имеет место в первом подходе.

ленным критериям. Данный подход отражен в Директиве ЕС «Об электронных подписях» № 1999/93/ЕС[1] и с недавнего времени – в России.

Исторически одним из первых документов, регламентировавших электронную подпись, является Типовой закон ЮНСИТРАЛ «Об электронной коммерции» 1996 г., который содержит в себе ст. 7 «Подпись». Согласно данной статье, «если законодательство требует наличия подписи лица, это требование считается выполненным в отношении сообщения данных, если:

a) использован какой-либо способ для идентификации этого лица и указания на то, что это лицо согласно с информацией, содержащейся в сообщении данных;

b) этот способ является как надежным, так и соответствующим цели, для которой сообщение данных было подготовлено или передано с учетом всех обстоятельств, включая любые соответствующие договоренности».

Таким образом, предложенное в Типовом законе регулирование близко ко второй модели, описанной выше. Его составители намеренно не стали включать дифференцированное регулирование электронных подписей в зависимости от уровня их надежности, опасаясь, что в таком случае закон станет «привязанным к конкретному этапу технического развития». Вместо этого был использован комплексный подход, при котором анализу подвергается возможность выполнения подписью функций, указанных в ст. 7 (*a*), и то, насколько такая подпись является надежной в контексте конкретных обстоятельств (характера сделки, частоты коммерческих отношений сторон, возможностей средств связи, условий торговых обычаев и практик, ценности подписанной информации, наличия альтернативных средств идентификации и их стоимости и т.д.).

В последующие годы были приняты законы об электронных подписях в США (сначала на уровне отдельных штатов, первыми из которых были Юта[2], Вашингтон[3], Флорида[4], а впоследствии и на уровне федерального закона США[5]) и в Европе (в Германии[6], Италии[7], Испании, Голландии, Финляндии, во Франции, в Швеции и во многих других странах). В 1999 г. Европейским союзом была принята Дирек-

[1] Official Journal. 13/12. 19.01.2000.
[2] Utah Digital Signatures Act of 1996.
[3] Washington Electronic Authentication Act of 1996.
[4] Florida Electronic Signature Act of 1996.
[5] The Electronic Signatures in Global and National Commerce Act (E-Sign Act) of 2000.
[6] Gesetz zur Digitalen Signatur BT-Drs. 13/7934 vom 11.06.1997.
[7] Italian Electronic Document and Digital Signature Act 1997 (Legge Bassanini, 59/1997).

тива № 1999/93/ЕС «Об общих условиях использования электронных подписей в Сообществе» (*Directive on a Community framework for electronic signatures*)[1], которая подобно *E-Sign Act* в США была направлена на обеспечение единообразия в понимании категории «электронная подпись» и обеспечение их взаимного признания европейскими странами.

Указанная Директива разделяет все виды электронных подписей на простые и продвинутые (усиленные). Согласно ст. 2 Директивы первый вид электронных подписей представляет собой данные в электронной форме, которые прилагаются или логически совмещены с другими электронными данными и которые служат в качестве метода для опознавания. Второй вид – продвинутые электронные подписи – должны соответствовать следующим требованиям:

– уникальным образом связаны с определенной стороной, подписавшей документ;

– имеют способность идентифицирования стороны, подписавшей документ;

– могут создаваться с использованием средств, которые сторона, подписавшая документ, в состоянии самостоятельно поддерживать и контролировать;

– должны иметь связь с данными, к которым они имеют непосредственное отношение, таким образом, чтобы последующие изменения, вносимые в данные, могли быть опознаваемыми.

Сферы использования электронных документов и подписей определяются национальным правом. Поэтому именно государства-члены обязаны создавать условия для организации эффективной системы контроля за деятельностью провайдеров сертификационных услуг на своей территории

Таким образом, в период 1996–2001 гг. появился обширный свод законодательных норм разных стран и сформировалась практика использования электронных подписей в коммерческом обороте, на фоне которой стало очевидно, что тех скудных положений Типового закона об электронной торговле, которые содержатся в ст. 7, явно недостаточно для документа, претендующего на статус типового закона. В связи с этим был разработан Типовой закон ЮНСИТРАЛ «Об электронных подписях» 2001 г.[2], который в отличие от своего предшественника построен по «гибридной» (третьей) модели регламентации использования

[1] Official Journal of the European Communities. L 013. 19.01.2000.

[2] Типовой закон об электронных подписях, принятый Комиссией Организации Объединенных Наций по праву международной торговли, утвержден Резолюцией Генеральной Ассамблеи ООН от 24 января 2002 г. № A/56/588.

электронных подписей. В нем предлагаются практические стандарты, на основании которых может быть оценена техническая надежность электронных подписей, а также устанавливается связь между такой технической надежностью и юридической силой конкретной электронной подписи. Наличие таких положений позволяет сторонам заранее оценить юридическую силу используемой подписи, а не дожидаться результатов анализа *post factum*, основанного на учете всех возможных обстоятельств (как это следовало бы при применении ст. 7 Типового закона об электронной торговле).

Так, согласно ч. 1 ст. 6 Типового закона об электронных подписях в тех случаях, когда законодательство требует наличия подписи лица на сообщении данных (информации в электронном виде), это требование считается выполненным, если использована электронная подпись, надежность которой соответствует цели, для которой сообщение данных было подготовлено или передано, с учетом всех обстоятельств и договоренностей. При этом электронная подпись считается надежной для установленной цели и удовлетворяет требованиям, если:

– данные для создания электронной подписи в том контексте, в котором они используются, связаны с подписавшим и ни с каким другим лицом;

– данные для создания электронной подписи в момент подписания находились под контролем подписавшего и никакого другого лица;

– любое изменение, внесенное в электронную подпись после момента подписания, поддается обнаружению;

– в тех случаях, когда одна из целей юридического требования в отношении наличия подписи заключается в гарантировании целостности информации, к которой она относится, любое изменение, внесенное в эту информацию после момента подписания, поддается обнаружению.

Вышеуказанные положения типовых законов ЮНСИТРАЛ и Директивы ЕС № 1999/93/ЕС были приведены не из праздного компаративизма. Они стали основным источником вдохновения для российского законодателя[1]. Правда, на первых этапах это вдохновение принимало весьма своеобразные и избирательные формы.

Первым законом, посвященным регулированию электронных подписей, был Федеральный закон от 10 января 2002 г. № 1-ФЗ «Об электронной цифровой подписи» (далее – Закон об ЭЦП 2002 г.) (утратил силу с 1 июля 2013 г.). Он разрабатывался по поручению Правительства РФ

[1] *Ильиных Е.В., Козлова М.Н.* Комментарий к Федеральному закону от 10 января 2002 г. № 1-ФЗ «Об электронной цифровой подписи» (постатейный). М., 2005.

рядом ведомств: Минсвязью России, ФАПСИ, Гостехкомиссией России, Минюстом России, ФКЦБ России и Госстандартом России с участием Банка России[1]. Участие столь большого количества государственных органов, в буквальном смысле, не побоюсь этого слова, «помешанных» на вопросах безопасности, и отсутствие в числе разработчиков бизнес-сообщества привели к закономерному результату. Закон был посвящен исключительно регулированию электронной цифровой подписи, созданной с использованием технологии асимметричной криптографии с открытым ключом. Под электронной цифровой подписью в соответствии с Законом об ЭЦП 2002 г. понимался «реквизит электронного документа, предназначенный для защиты данного электронного документа от подделки, полученный в результате криптографического преобразования информации с использованием закрытого ключа электронной цифровой подписи и позволяющий идентифицировать владельца сертификата ключа подписи, а также установить отсутствие искажения информации в электронном документе». Все остальные виды электронных подписей остались за рамками Закона, а поскольку какие-либо иные законодательные положения, посвященные им, отсутствовали, они могли быть использованы лишь на основании предварительно заключенного соглашения сторон (ст. 160 ГК РФ).

Учитывая технологическую жесткость Закона и множество административных процедур, связанных с использованием электронной цифровой подписи «в информационных системах общего пользования», к которым относится сеть Интернет, участники гражданского оборота, в особенности иностранные, не торопились применять его к своим отношениям. А если еще учесть установленную данным Законом фактическую невозможность признания на территории России сертификатов электронных подписей, выданных иностранными удостоверяющими центрами (о чем будет сказано далее), ни о каком включении России в международный электронный документооборот не могло быть и речи. Неудивительно, что указанный Закон стал привлекательным объектом для критики. Так, в числе недостатков Закона А.В. Шамраев указывал на неоправданную технологичность и жесткость регулирования, его недостаточную определенность, «встраивание» административных механизмов (сертификации и лицензирования) в рамки юридических последствий использования электронной цифровой подписи, а также высокую степень зависимости указанного Закона от подзаконного ре-

[1] *Леонтьев К.Б.* Комментарий к Федеральному закону «Об электронной цифровой подписи» (постатейный). М., 2003. С. 6.

гулирования[1]. В числе иных недостатков отмечалась невозможность принадлежности ЭЦП юридическим лицам, что ставило вопросы правомерности использования ЭЦП отдельными физическими лицами «от имени компании» после утраты ими полномочий, увольнении и т.д.[2]

Все это привело к тому, что Закон об ЭЦП если и применялся, то преимущественно в отношениях организаций с государственными органами (например, для сдачи налоговой отчетности) либо в отношениях с участием банковских организаций, заинтересованных в обеспечении максимальной надежности при производстве безналичных расчетов. Перспективы использования данного Закона в отношении коммерческих электронных сделок для большинства участников оборота были малопривлекательны. Спустя пять лет после принятия данного Закона процент лиц, использующих ЭЦП, не превысил 0,2%. В то же время, по данным Института Фраунхофера по открытым коммуникационным системам, по состоянию на 2005 г. (т.е. через 5 лет после принятия Директивы № 1999/93/ЕС) в Европе использовали усиленные электронные подписи до 70% населения[3].

Указанные причины обусловили разработку и принятие нового закона, который, как следует уже из названия, охватывает гораздо более широкий спектр электронных подписей. Как указано в пояснительной записке к новому закону, он направлен на устранение недостатков Закона об ЭЦП 2002 г., а также на расширение сферы использования и допустимых видов электронных подписей[4].

Новый Закон вступил в силу 8 апреля 2011 г. При этом старый Закон об ЭЦП 2002 г. не был отменен вплоть до 1 июля 2013 г., что породило достаточно парадоксальную ситуацию параллельного действия двух законов, регулирующих однородные отношения.

Так или иначе, Федеральный закон от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи» (далее – Закон об ЭП 2011 г.) теперь является основным актом, регулирующим использование электронной подписи в России, в связи с чем необходимо рассмотреть подробнее его основные положения.

---

[1] *Шамраев А.В.* Правовое регулирование информационных технологий (анализ проблем и основные документы). Версия 1.0. М., 2003. С. 56.

[2] *Шишаева Е.* Федеральный закон «Об электронной цифровой подписи»: основные положения и проблемы, связанные с применением // Юрист. 2004. № 3.

[3] Данные взяты из пояснительной записки к проекту федерального закона № 305592-5 «Об электронной подписи» // http://asozd2.duma.gov.ru/main.nsf/%28SpravkaNew%29?OpenAgent&RN=305592-5&02

[4] Пояснительная записка к проекту федерального закона № 305592-5 «Об электронной подписи».

В целом новый закон в гораздо большей степени учитывает положения Типового закона ЮНСИТРАЛ об электронных подписях и Директивы ЕС № 1999/93/ЕС, во многом воспроизводя положения последней.

В качестве основных принципов использования электронных подписей в Законе об ЭП 2011 г. указаны:

1) право участников электронного взаимодействия использовать электронную подпись любого вида по своему усмотрению, если требование об использовании конкретного вида электронной подписи в соответствии с целями ее использования не предусмотрено федеральными законами или принимаемыми в соответствии с ними нормативными правовыми актами либо соглашением между участниками электронного взаимодействия;

2) возможность использования участниками электронного взаимодействия по своему усмотрению любой информационной технологии и (или) технических средств, позволяющих выполнить требования настоящего Закона применительно к использованию конкретных видов электронных подписей;

3) недопустимость признания электронной подписи и (или) подписанного ею электронного документа не имеющими юридической силы только на основании того, что такая электронная подпись создана не собственноручно, а с использованием средств электронной подписи для автоматического создания и (или) автоматической проверки электронных подписей в информационной системе.

В соответствии со ст. 2 Закона об ЭП под электронной подписью понимается информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию. Закон предусматривает три вида электронных подписей:

1) простая электронная подпись;

2) усиленная неквалифицированная электронная подпись;

3) усиленная квалифицированная электронная подпись.

1. *Простая электронная подпись* – это электронная подпись, которая создается посредством использования кодов, паролей или иных средств и подтверждает факт формирования электронной подписи определенным лицом. Таким образом, использование логина и пароля к личному кабинету на веб-сайте, использование уникальных паролей, высылаемых на мобильный телефон при совершении конкретной транзакции, использование в качестве идентификатора адреса электронной

почты (для доступа к которой также необходимо знание пароля) – все это подпадает под понятие простой электронной подписи.

Для того чтобы документ считался подписанным простой электронной подписью, необходимо, чтобы такая подпись была проставлена в самом электронном документе либо ключ простой электронной подписи был применен в соответствии с правилами, установленными оператором операционной системы, в рамках которой электронный документ был создан, и в нем имеется указание на лицо, от имени которого был создан и (или) отправлен электронный документ (ст. 9 Закона об ЭП).

Можно привести следующий пример. Для оформления заказа на сайте «*ozon.com*» необходимо пройти процедуру регистрации, предусматривающую формирование логина и пароля для входа в личный кабинет. При регистрации указываются ФИО и иные персональные данные, идентифицирующие потенциального покупателя. Данные логин и пароль выступают в качестве ключа простой электронной подписи (уникальной последовательности символов, предназначенной для создания электронной подписи). При оформлении заказа, сделанного под логином и паролем, формируется электронный документ, в котором средствами информационной системы (веб-сайта «*ozon.ru*») указывается лицо, создавшее (отправившее) заказ. Данное указание и будет выступать в качестве простой электронной подписи, сгенерированной при помощи логина и пароля пользователя. Здесь следует подчеркнуть, что вопреки высказываемому мнению о том, что простой электронной подписью в данном случае является связка «логин – пароль»[1], они выступают лишь в качестве ключа, на основе которого такая подпись генерируется. В противном случае пришлось бы признать, что логин и пароль, будучи конфиденциальными данными (п. 2 ч. 2 ст. 9 Закона об ЭП), должны были бы указываться в тексте подписанного с их помощью электронного документа.

В соответствии с ч. 2 ст. 6 Закона об ЭП электронный документ, подписанный простой электронной подписью, признается равнозначным документу на бумажном носителе, подписанному собственноручной подписью лишь в случае прямого указания закона или иного нормативного правового акта либо соглашения между участниками электронного взаимодействия. В настоящее время отсутствуют нормативные правовые акты, из которых следует признание равной юридической силы электронных документов, подписанных простой элект-

[1] Такое мнение высказывается, в частности, на официальном сайте Минсвязи России. См.: http://minsvyaz.ru/ru/faq/index.php?id_4=14

ронной подписью или усиленной неквалифицированной электронной подписью, и бумажных документов, подписанных собственноручной подписью их составителей. Следовательно, по мнению Ассоциации российских банков равная юридическая сила договоров в электронной форме и на бумажных носителях в рассматриваемых случаях может быть основана только на ранее заключенных сторонами рамочных договорах, которые допускают такой порядок заключения последующих договоров[1]. Существенными условиями такого соглашения являются правила определения лица, подписывающего электронный документ, на основании простой электронной подписи; его обязанность обеспечивать конфиденциальность ключа электронной подписи и порядок проверки подлинности электронной подписи (п. 2 ст. 9, п. 2 ст. 6 Закона об ЭП).

Представляется, что соглашение об использовании средств простой электронной подписи может быть выражено и в иной форме, нежели рамочное, по крайней мере никаких ограничений на сей счет в Законе нет. Отсутствует в законодательстве и требование об оформлении его в письменной форме под страхом недействительности. Главное, чтобы такое соглашение имело место быть и отвечало требованиям гражданского законодательства. Так что в принципе не исключена возможность его заключения и посредством совершения конклюдентных действий. О наличии согласованного волеизъявления по вопросу использования аналога собственноручной подписи может свидетельствовать тот факт, что в ответ на оферту, которая была направлена в электронном виде с использованием такого аналога, акцепт был отправлен с использованием аналогичного вида электронной подписи или в порядке, предписанном полученной офертой. В таком случае можно говорить о том, что участники не возражали против применения такого аналога собственноручной подписи при заключении договора и допускают его применение в дальнейшем. Иной, более формальный подход к определению наличия предварительного соглашения об использовании электронной подписи сводит на нет все возможное положительное влияние Закона об ЭП на развитие электронной коммерции в России.

Следует отметить, что отечественной судебной практике известны случаи гибкого подхода к определению наличия соглашения сторон по определенным вопросам, к определению наличия соглашения о передаче преддоговорных разногласий на рассмотрение суда (ст. 446

[1] См.: п. 2 рекомендаций по заключению договоров в электронной форме, утв. Ассоциацией российских банков 19 декабря 2012 г. // Вестник Ассоциации российских банков. 2013. № 1–2.

ГК РФ). Так, если в суд с разногласиями по договору обратилась одна сторона, а контрагент направил в суд свои предложения по условиям договора, то суды полагают, что спор передан на рассмотрение арбитражного суда по соглашению сторон[1]. Похожий подход используется судами применительно к соглашениям о выборе применимого права. В отсутствие в соглашении сторон условия о применимом праве ссылки обеих сторон в ходе процесса на нормы определенного законодательства могут быть истолкованы как достижение соглашения о выборе применимого права[2]. Поэтому не будет ничего принципиально революционного в том, чтобы обнаружить соглашение об использовании электронной подписи в окружающих ее использование обстоятельствах.

Главной особенностью простой электронной подписи является тот факт, что она хотя и указывает на лицо, подписавшее сообщение, но не позволяет при этом установить неизменность электронного документа после его подписания, главным образом потому, что при ее создании и использовании не используются специальные криптографические средства преобразования информации, неразрывно связанные с ключом электронной подписи, посредством которого создается сама подпись. Логин и пароль к личному кабинету на веб-сайте и итоговый электронный документ (исходящий заказ, подготовленный в рамках такого кабинета) не связаны между собой средствами криптографического преобразования. Однако это ничуть не умаляет их значения в сфере, где они наиболее часто применяются: форма заказа содержит необходимые условия договора, риск недобросовестного изменения которых в большинстве случаев крайне незначителен. Применительно к большинству интернет-магазинов более изощренные виды электронной цифровой подписи малооправданны, поскольку неизбежно связаны с возрастанием сложности совершения покупок в таком магазине, что может отпугнуть немало потенциальных покупателей. Иными словами, риски, связанные с отсутствием более надежного вида электронной подписи, несоизмеримо меньше, нежели риски, связанные с потенциальными потерями от оттока покупателей, обусловленного использованием такой подписи.

---

[1] Комментарий к Гражданскому кодексу Российской Федерации, части первой (постатейный) / под ред. О.Н. Садикова. М., 2006. С. 996.

[2] См., например: постановление ФАС Дальневосточного округа от 1 декабря 2009 г. № Ф03-6794/2009 по делу № А24-5830/2008. В пересмотре дела в порядке надзора отказано Определением ВАС РФ от 14 апреля 2010 г. № ВАС-1375/10; постановление ФАС Московского округа от 5 декабря 2003 г. № КГ-А40/9513-03 по делу № А40-47669/02-69-492.

2. *Усиленная неквалифицированная электронная подпись* предполагает наличие определенных криптографических средств преобразования информации с использованием ключа электронной подписи, которые позволяют не только определить лицо, подписавшее документ, но и обнаружить факт внесения изменений в документ после его подписания. Главное отличие данной подписи от простой электронной заключается в том, что такая подпись выполняет помимо идентифицирующей функции еще и защитную. Никаких особых преимуществ с точки зрения наличия каких-либо дополнительных оснований для признания документа, подписанного ею, равнозначным бумажному по сравнению с простой электронной подписью у усиленной неквалифицированной подписи нет. Для этого все также необходимо указание закона, иного нормативного правового акта или ранее заключенного соглашения между сторонами.

Другое дело, что с технической точки зрения такая подпись является более совершенной и предоставляет больше гарантий по вопросам не только ее принадлежности определенному лицу, но и обеспечения неизменности содержания документа. Это позволяет использовать ее для заключения договоров, которые в ином случае заключались бы «по старинке», в классической бумажной форме: договоров поставки, оказания услуг, подряда, займа, лицензионных договоров и ряда иных. Данный вид электронной цифровой подписи представляется малопригодным для заключения множества стандартизированных соглашений на небольшую сумму, так как размер транзакционных издержек, связанных с ее использованием, значительно выше, чем при использовании простой электронной подписи, поскольку требуется совершение ряда дополнительных действий с обеих сторон по проверке сертификата подписи, что требует привлечения дополнительного ресурса субъектом электронной коммерции и специальных познаний со стороны его контрагента. С другой стороны, никаких дополнительных преимуществ с точки зрения законодательных презумпций данный вид подписи не предоставляет, что может служить хорошим доводом для того, чтобы «поднапрячься» и использовать следующий вид электронной подписи (усиленная квалифицированная), который более выгоден с точки зрения восприятия электронного документа публичными органами и законодательством в целом. Оптимальной сферой применения усиленной неквалифицированной подписи представляется ее использование в закрытых информационных системах между контрагентами с уже сложившимися деловыми отношениями в отношении договоров, содержание отличается информационной

насыщенностью и длительными согласованиями. Здесь может пригодиться защитная функция такой подписи, позволяющая «заморозить» документ по состоянию на определенный момент времени и отследить возможные несанкционированные изменения.

3. *Усиленная квалифицированная электронная подпись*. Данный вид подписи обладает всеми признаками усиленной неквалифицированной подписи (т.е. в ней используются специальные криптографические средства преобразования информации, обеспечивающие идентификацию и аутентификацию сообщения) и дополнительно характеризуется наличием квалифицированного сертификата, содержащего ключ проверки электронной подписи, и использованием для ее создания средств, получивших специальное подтверждение соответствия их требованиям Закона об ЭП.

В качестве примера усиленной квалифицированной электронной подписи можно привести электронную цифровую подпись, о которой шла речь в Законе об ЭЦП. Напомним, что она была основана на технологии асимметричной криптографии, предполагающей использование алгоритмических функций для создания двух разных, но математически соотносящихся ключей. Один такой ключ используется для создания цифровой подписи или преобразования данных в кажущуюся непонятной форму, а другой ключ – для удостоверения подлинности цифровой подписи или возвращения сообщения в его подлинную форму. Взаимодополняющие ключи, используемые для проставления цифровой подписи, состоят из «частного» ключа (*private key*), который используется подписывающим лицом для создания цифровой подписи и держится им в секрете, и «публичного» ключа, который обычно более широко известен и используется получателем для проверки подлинности цифровой подписи отправителя.

С принятием нового Закона данный вид электронной подписи стал не единственно возможным, а одним из возможных видов электронной подписи. Поскольку рассматриваемый вид подписи создается и используется под контролем государства, правовой статус электронного документа, подписанного ею, существенно выше. В отличие от документов, подписанных одним из двух рассмотренных ранее видов электронной подписи, электронный документ, подписанный квалифицированной электронной подписью, является равнозначным бумажному документу, подписанному собственноручной подписью и заверенному печатью. При этом не требуется специального указания на это в специальном законе, ином правовом акте или соглашении сторон. Такая равнозначность юридической силы возникает в силу

прямого указания Закона (п. 1 ч. 3 ст. 6 Закона об ЭП). Исключением являются случаи, когда Закон предусматривает необходимость составления документа исключительно на бумажном носителе. Также законодательство и соглашение сторон могут устанавливать *дополнительные* требования к электронному документу в целях признания его равнозначным документу на бумажном носителе, *заверенному печатью*.

Закон об ЭП закрепляет презумпцию действительности квалифицированной электронной подписи, которая может быть опровергнута лишь в судебном порядке. Действительность данной презумпции зависит от одновременного соблюдения четырех условий:

1) квалифицированный сертификат создан и выдан аккредитованным удостоверяющим центром[1], аккредитация которого действительна на день выдачи указанного сертификата;

2) квалифицированный сертификат действителен на момент подписания электронного документа (при наличии достоверной информации о моменте подписания электронного документа) или на день проверки действительности указанного сертификата, если момент подписания электронного документа не определен;

3) имеется положительный результат проверки принадлежности владельцу квалифицированного сертификата квалифицированной электронной подписи, с помощью которой подписан электронный документ и подтверждено отсутствие изменений, внесенных в этот документ после его подписания;

4) если квалифицированный сертификат содержит определенные ограничения по сфере его действия (например, применительно к характеру договора, его предельной сумме, статусу контрагента), то проставление подписи должно быть осуществлено с учетом таких ограничений (ст. 11 Закона об ЭП).

Для того чтобы система квалифицированных электронных подписей эффективно функционировала, участники оборота должны иметь возможность убедиться в принадлежности «публичного» ключа определенному лицу, а также в надежности используемых для создания электронной подписи технических средств. Причем реализация такой возможности не должна зависеть исключительно от действий или ин-

[1] В соответствии с п. 8 ст. 2 Закона об ЭП аккредитация удостоверяющего центра означает признание уполномоченным федеральным органом соответствия удостоверяющего центра требованиям данного Закона. В настоящее время таким уполномоченным органом является Минкомсвязи России (постановление Правительства РФ от 28 ноября 2011 г. № 976 «О федеральном органе исполнительной власти, уполномоченном в сфере использования электронной подписи»). Перечень аккредитованных удостоверяющих центров размещен на сайте Минкомсвязи России – http://minsvyaz.ru

формации, предоставляемой подписантом, в противном случае не будет никаких гарантий отсутствия возможного подлога и подпись не сможет выполнить доверительную функцию. Тут и приходит на помощь специальный субъект – удостоверяющий центр, который обеспечивает объективную возможность осуществления такой проверки заинтересованными лицами. Именно он устанавливают связь между идентифицированным подписавшим лицом и конкретным «публичным» ключом.

Разумеется, организация, претендующая на осуществление подобных функций, сама должна пользоваться доверием. В связи с этим Закон устанавливает требование об обязательной аккредитации удостоверяющего центра, если речь идет об усиленной квалифицированной электронной подписи. Аккредитация означает подтверждение уполномоченным органом (в настоящее время – Министерство связи и массовых коммуникаций РФ) соответствия центра требованиям Закона об ЭП. Данная аккредитация предполагает выполнение удостоверяющим центром как определенных экономических требований (наличие определенного размера активов и финансового обеспечения ответственности), так и организационно-технических: наличие в штате необходимых специалистов, а также средств электронной подписи и средств удостоверяющего центра, получивших подтверждение соответствия требованиям, установленным ФСТЭК России и ФСБ России[1] (ч. 3 ст. 16 Закона об ЭП).

В отсутствие у удостоверяющего центра такой аккредитации квалифицированная электронная подпись не будет действительной, а электронный документ, подписанный ею, не будет равнозначным бумажному документу, подписанному собственноручной подписью (ч. 1 ст. 6, ч. 1 ст. 11 Закона об ЭП).

Основной задачей удостоверяющего центра является создание сертификатов электронных подписей с выдачей его заявителю, который

[1] Приказ ФСБ России от 30 августа 2012 г. № 440 «Об утверждении Административного регламента Федеральной службы безопасности Российской Федерации по предоставлению государственной услуги по осуществлению лицензирования деятельности по разработке, производству, распространению шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, выполнению работ, оказанию услуг в области шифрования информации, техническому обслуживанию шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств (за исключением случая, если техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя)». Зарегистрирован в Минюсте России 27 сентября 2012 г. № 25563.

приобретает статус владельца такого сертификата. Удостоверяющий центр выполняет ряд других функций, в частности осуществляет по обращениям участников электронного взаимодействия проверку электронных подписей (например, факта включения ее в реестр и действительности ее сертификата на момент обращения с запросом); устанавливает сроки действия сертификатов ключей электронной подписи (как правило, 1 год); досрочно аннулирует сертификаты ключей электронной подписи по заявлению владельца либо в связи с допущенными нарушениями.

Сертификат ключа проверки электронной подписи является важнейшим документом во всей системе отношений по использованию электронной подписи, поскольку от действительности сертификата напрямую зависит действительность такой подписи. Сертификат представляет собой документ в электронной или бумажной форме, в котором содержатся данные, позволяющие сделать вывод о принадлежности электронной подписи определенному лицу. В сертификате содержится так называемый открытый ключ, с помощью которого можно расшифровать переданный документ, подписанный закрытым ключом отправителя, и убедиться, что подпись соответствует заявленному владельцу. Или наоборот – с помощью открытого ключа можно зашифровать отправляемое сообщение, обеспечив его конфиденциальность, поскольку только владелец закрытого ключа (предполагаемый адресат) сможет его открыть и прочитать.

В соответствии со ст. 14 Закона об ЭП сертификат ключа проверки электронной подписи должен содержать следующую информацию:

1) даты начала и окончания срока его действия (с точностью до часов, минут, секунд);

2) фамилию, имя и отчество (если имеется) – для физических лиц, наименование и место нахождения – для юридических лиц или иную информацию, позволяющую идентифицировать владельца сертификата ключа проверки электронной подписи;

3) ключ проверки электронной подписи (открытый ключ);

4) наименование используемого средства электронной подписи и (или) стандарты, требованиям которых соответствуют ключ электронной подписи и ключ проверки электронной подписи;

5) наименование удостоверяющего центра, который выдал сертификат ключа проверки электронной подписи.

Сертификат ключа проверки квалифицированной электронной подписи («квалифицированный сертификат» помимо указанных сведений должен содержать уникальный номер такого сертификата, СНИЛС –

для физических лиц или ИНН для юридических лиц, сведения об аккредитации удостоверяющего центра и его квалифицированный сертификат и иные сведения, подтверждающие соответствие используемых средств электронной подписи жестким требованиям Закона об ЭП 2011 г. и подзаконных актов (ст. 17).

Удостоверяющий центр ведет в порядке, установленном Минкомсвязи России[1], реестр сертификатов, который представляет собой систематизированный свод сведений о сертификатах всех созданных таким центром электронных подписей. Удостоверяющий центр обеспечивает актуальность данных, содержащихся в таком реестре, и возможность безвозмездного ознакомления с ними любого заинтересованного лица. Минкомсвязи России также выполняет функцию главного (корневого) удостоверяющего центра по отношению к аккредитованным удостоверяющим центрам[2].

В отличие от старого Закона об ЭЦП Закон об ЭП позволяет выступать в качестве владельца сертификата электронной подписи не только физическим, но и юридическим лицам. В случае выдачи сертификата ключа проверки электронной подписи юридическому лицу в качестве владельца сертификата ключа проверки электронной подписи наряду с указанием наименования юридического лица указывается физическое лицо, действующее от имени юридического лица на основании учредительных документов юридического лица или доверенности. Правда, Закон об ЭП не дает ответа на вопрос, действительна ли электронная подпись, сделанная иным сотрудником юридического лица, нежели указанная в сертификате. В случае, если она будет все же недействительна (на что намекает необходимость четкого указания в сертификате уполномоченного физического лица), то не очень понятно, в чем состоит принципиальное отличие нового регулирования от подхода ранее действовавшего Закона об ЭЦП, который допускал возможность обладания ЭЦП только физическими лицами. Представляется, что верным является все же первый вариант, а сведения об уполномоченном физическом лице носят информационный харак-

[1] См.: Приказ Минкомсвязи России от 5 октября 2011 г. № 250, утвердивший порядок формирования и ведения реестров квалифицированных сертификатов ключей проверки электронной подписи, а также предоставления информации из таких реестров.

[2] Поскольку информация, предоставляемая аккредитованным удостоверяющим центром в электронной форме, заверяется квалифицированной электронной подписью такого центра, для того чтобы удостовериться в ее действительной принадлежности такому центру, необходимо обратиться к удостоверяющему центру более высокого порядка, который пользовался бы неоспоримым доверием у участников оборота. В России данную функцию и призвано выполнять Минкомсвязи России.

тер, а не правообразующий. В большинстве своем этот вывод основан на специфике механизма функционирования квалифицированной электронной подписи.

Сам по себе факт проставления квалифицированной электронной подписи иным лицом, не указанным в сертификате, не является основанием для оспаривания сделки, подписанной такой электронной подписью, если проверка подписи прошла успешно и выполнены все условия закона (в нашем случае – ст. 11 Закона об ЭП). Вся система функционирования квалифицированных электронных подписей предполагает обязанность ее владельца обеспечить конфиденциальность закрытого ключа, что является основанием для презумпции совершения сделок с использованием этого ключа именно таким лицом. Третьи лица не могут знать, кто фактически подписал документ с использованием закрытого ключа, поскольку не имеют возможности это проверить. Возложение на них рисков, связанных с использованием закрытого ключа неуполномоченным лицом, не только было бы несправедливым, но и поставило бы под сомнение всю систему функционирования квалифицированных электронных подписей, лишая ее какого бы то ни было доверия. Если владелец подписи узнал о том, что закрытый ключ скомпрометирован, он должен незамедлительно обратиться в удостоверяющий центр с заявлением об аннулировании сертификата подписи. И уж тем более он должен нести риски нарушения правил безопасности работы в сети Интернет (неиспользование антивирусных программ, использование нелицензионного программного обеспечения, отсутствие ограничений по принятию документов только с определенного *IP*-адреса и пр.)[1].

Данная логика особенно отчетливо прослеживается в судебных спорах между банками и клиентами в связи с использованием систем удаленного банковского обслуживания, которые на данный момент являются основным источником судебной практики по вопросам использования электронных цифровых подписей (квалифицированных электронных подписей). Обычно клиенты банков оспаривают правомерность совершения банком операций по поручениям, сделанным неуполномоченными лицами с использованием электронной цифровой подписи клиента (квалифицированной электронной подписи). Стандартный ответ суда в таком случае заключается в том, что банк

[1] Данный подход нашел свое отражение в отечественной судебной практике. См.: постановление Семнадцатого арбитражного апелляционного суда от 12 декабря 2011 г. по делу № А60-15360/2011, оставленное в силе постановлением ФАС Уральского округа от 30 марта 2012 г. № Ф09-1458/12.

не несет ответственности за факты использования таких подписей неуполномоченными лицами и *необеспечения клиентом надежного хранения ключей, имен и паролей, используемых при работе с ними*[1]. Те немногие случаи, когда клиентам удавалось обосновать неправомерность списания средств на основании платежных документов, подписанных ЭЦП (квалифицированной электронной подписью), касались ситуаций, в которых суд усматривал отсутствие правовых оснований для использования такой подписи по причинам, зависящим от самого банка, – например, по причине отсутствия актов о подключении системы «Банк-клиент»[2], по причине отсутствия акта передачи новых сертификатов ключей подписи, предусмотренного договором[3].

Однако нельзя говорить о том, что во всем практически всегда оказывается виноватым владелец сертификата электронной подписи. Доверительная функция удостоверяющего центра обеспечивается также возможностью привлечения его не только к ответственности за несоблюдение положений, вытекающих из договора оказания услуг с владельцем сертификата (что и так очевидно в силу общих положений договорного права), но и к ответственности *перед третьими лицами* за неисполнение или ненадлежащее исполнение обязанностей, предусмотренных Закона об ЭП (ч. 3 ст. 13). На обеспечение финансовой возможности несения подобной ответственности направлены специальные условия аккредитации удостоверяющих центров, предъявляющие определенные требования к размеру чистых активов (не менее 1 млн руб.), а также требования финансового обеспечения ответственности в размере не менее 1,5 млн руб., подтверждаемое договором страхования ответственности, банковской гарантией или договором поручительства (п. 1, 2 ч. 3 ст. 16 Закона об ЭП 2011 г.).

Таким образом, если третье лицо понесет, к примеру, убытки вследствие предоставления ему недостоверной информации о сертификатах электронной подписи его потенциального контрагента и если впоследствии подписанный с использованием электронной подписи таким лицом документ будет признан недействительным, соответствующие убытки могут быть возложены на удостоверяющий центр. Разумеется,

[1] См., например, постановления ФАС Московского округа от 13 ноября 2012 г. № Ф05-12672/12 по делу № А40-18115/2012; ФАС Северо-Западного округа от 16 октября 2012 г. № Ф07-5221/12 по делу № А66-9956/2011; ФАС Дальневосточного округа от 23 октября 2012 г. № Ф03-4500/12 по делу № А73-7000/2011.

[2] Постановление Семнадцатого арбитражного апелляционного суда от 18 августа 2011 г. № 17АП-6233/2011-ГК по делу № А50-18570/2010.

[3] Постановление ФАС Северо-Кавказского округа от 27 апреля 2011 г. по делу Т А63-6446/2010.

это не исключает необходимости доказывания размера убытков и причинно-следственной связи в общем порядке. При этом общие условия наступления деликтной ответственности предполагают также наличие вины причинителя вреда, причем безотносительно к возможному предпринимательскому статусу делинквента. Безвиновная деликтная ответственность по общему правилу может быть установлена лишь законом (п. 2 ст. 1064 ГК РФ). Правда, существует судебная практика, которая возлагает ответственность за вред, причиненный в рамках деликтных отношений, на причинителя и в отсутствие его вины, ссылаясь при этом на ст. 401 ГК РФ[1].

Поскольку электронная коммерция функционирует на базе сети Интернет и имеет потенциально трансграничный характер, неизбежно возникает вопрос о статусе на территории России электронных подписей, созданных по законодательству иностранных государств. Ранее действовавший Закон об ЭЦП содержал весьма неоднозначное положение, согласно которому «иностранный сертификат ключа подписи, удостоверенный в соответствии с законодательством иностранного государства, в котором этот сертификат ключа подписи зарегистрирован, признается на территории Российской Федерации в случае выполнения установленных законодательством Российской Федерации процедур признания юридического значения иностранных документов» (ст. 18). Поскольку законодательство не содержало специальных положений, регламентирующих признание иностранных документов в электронной форме (включая сертификаты электронных подписей)[2], это препятствовало применению ЭЦП в трансграничных сделках, превратив ее, по существу, в инструмент электронного документооборота с госорганами Российской Федерации.

В связи с этим особую актуальность приобрел вопрос об изменении регулирования в данной части. Конечно, не следует впадать в другую крайность, при которой осуществлялось бы безоговорочное признание подписей, выданных иностранными удостоверяющими центрами, пос-

[1] Общее правило о безвиновной ответственности лица, осуществляющего предпринимательскую деятельность, в обязательственных отношениях установлено в п. 3 ст. 401 ГК РФ. Несмотря на то что по своей сути оно рассчитано на договорные обязательства, судебная практика расширила применение данного положения и на деликтные отношения, в частности на нарушение исключительного права (см.: постановление Президиума ВАС РФ от 20 ноября 2012 г. № 8953/12; п. 23 постановления Пленума ВС РФ № 5, Пленума ВАС РФ № 29 от 26 марта 2009 г. «О некоторых вопросах, возникших в связи с введением в действие части четвертой Гражданского кодекса Российской Федерации»).

[2] См., например: *Кенсовский П.А.* Легализация и признание документов иностранных государств. СПб., 2003. С. 242; *Карев Я.А.* Указ. соч. С. 129; *Калятин В.О.* Право в сфере Интернета. С. 129.

кольку, по справедливому замечанию В.О. Калятина, «имеет ли смысл устанавливать строгие стандарты по отношению к ЭЦП, заботясь о ее безопасности, если обойти эти стандарты ничего не стоит (достаточно получить сертификат ЭЦП в иностранном удостоверяющем центре)»[1].

Закон об ЭП содержит достаточно сбалансированное решение, в целом соответствующее зарубежному подходу. Статья 7 данного Закона закрепляет, что «электронные подписи, созданные в соответствии с нормами права иностранного государства и международными стандартами, признаются в России электронными подписями того вида, признакам которого они соответствуют на основании данного закона. Электронная подпись и подписанный ею электронный документ не могут считаться не имеющими юридической силы только на том основании, что сертификат ключа проверки электронной подписи выдан в соответствии с нормами иностранного права». Данное положение является отражением того самого функционального подхода, о котором говорится в Типовом законе ЮНСИТРАЛ об электронной подписи: иностранная подпись должна быть признана в стране – получателе электронного документа, если технологии подписания «эквивалентны по существу» (*substantially equivalent*). Таким образом, для признания юридической силы иностранной подписи необходимо убедиться, что при ее создании использовались такие же методы, какие используются при создании подписи в соответствии с российским законодательством. При этом важна именно общность тех принципов, которые использовались при создании данной электронной подписи, а не точное соответствие технологий подписания определенным техническим стандартам.

Во многом аналогичные положения содержатся в Директиве № 1999/93/ЕС. В соответствии с абз. 1 ст. 7 данной Директивы государства – члены ЕС должны гарантировать квалифицированные сертификаты, которые выданы удостоверяющим центром, действующим в третьей стране, и которые будут признаваться юридически эквивалентными сертификатам, выданным удостоверяющими центрами в рамках ЕС, при условии, что: а) иностранный удостоверяющий центр соответствует требованиям, установленным Директивой, и имеет добровольную аккредитацию в одном из государств – членов ЕС, или б) сертифицирующий сервис-провайдер внутри ЕС, соответствующий требованиям Директивы, поручится за иностранный квалифицированный сертификат, или в) квалифицированные сертификат или деятельность иностранного удостоверяющего центра признаны в рамках

[1] *Калятин В.О.* Право в сфере Интернета. С. 130.

заключенного двухстороннего или многостороннего соглашения между ЕС и третьим государством или международной организацией.

Насколько удачными являются положения нового законодательства об электронных подписях покажет время, но тот факт, что по многим вопросам была проведена «работа над ошибками», не может не внушать сдержанный оптимизм.

§ 5. Время и место заключения договора

После положительного решения вопроса о наличии оферты, акцепта, соблюдении требований к форме договора и наличии подписей сторон иногда возникает необходимость определить время и место заключения договора. Место заключения контракта может иметь значение для целей налогообложения, определения юрисдикции и применимого права. Время заключения контракта может иметь значение при определении рыночной цены, действующей на момент заключения договора, момента перехода прав на товар и рисков утраты, момента утраты права на отзыв оферты и решения ряда иных вопросов.

Для определения времени и места заключения договора необходимо установить, когда и где электронные сообщения, составляющие оферту и акцепт, считаются законом полученными адресатом[1]. Вопрос о моменте перфекции оферты и акцепта является частью более общего вопроса о том, когда различного рода уведомления, предназначенные для достижения определенного юридического эффекта, вступают в силу в отношении их адресата[2]. Решение данного вопроса становится особенно актуальным по мере того, как многие уведомления совершаются посредством электронных коммуникаций.

Как известно, сообщения, посланные по электронной почте, могут затеряться и не дойти до адресата, отчасти в силу архитектуры сети

[1] Разумеется, это имеет смысл только при заключении договора между «отсутствующими» (*inter absentes*), поскольку только в таких случаях можно говорить о разрыве во времени между формулированием волеизъявления одним лицом и его восприятием другим.

[2] В некоторых странах проблема распределения рисков при отправке извещений или уведомлений в рамках гражданско-правовых отношений решается путем применения по аналогии правила о моменте заключения договора (получение оферентом акцепта). В качестве примера можно привести австрийское право, в доктрине которого можно встретить мнение о том, что ст. 862 Австрийского гражданского кодекса, устанавливающая, что акцепт считается сделанным при условии и в момент его получения оферентом, должна применяться по аналогии ко всем остальным случаям направления извещений. *Быдлински Ф.* Основные положения учения о юридическом методе. Ч. 2 // Вестник гражданского права. 2006. № 2. Т. 6.

Интернет, не гарантирующей 100%-ной доставки сообщений, а отчасти и потому, что получатель использует различного рода защитные меры вроде фильтров и брандмауэров, которые могут воспрепятствовать получению сообщения пользователем.

В разных странах существуют различные подходы к решению вопроса о том, когда акцепт вступает в силу и договор соответственно считается заключенным.

Так, в странах англо-американского права и некоторых странах континентального права (например, в Испании[1]) действует правило «почтового ящика» (*postal rule*)[2]. Согласно данному правилу договор считается заключенным в момент направления акцепта по почте. Таким образом, юридический эффект акцепта вступает в силу с момента его отправления. При таком подходе юридически безразлично, получил ли адресат извещение в реальности, и если да, то когда. Однако если в процессе заключения договора используются мгновенные (*instantaneous*) способы коммуникации (телефон, телекс и пр.), то сообщение об акцепте должно быть воспринято адресатом для того, чтобы иметь юридический эффект. Вопрос о применимости *postal rule* к электронной почте является предметом дискуссий в англо-американской доктрине, хотя большинство сходятся во мнении, что данное правило не должно переноситься на электронную почту[3].

В большинстве стран континентального права, в том числе и в России, тем не менее действует иное правило, согласно которому юридический эффект уведомления возникает в момент его получения (восприятия) адресатом. Иными словами, все риски, связанные с неполучением адресатом соответствующего уведомления, возлагаются на его отправителя.

Таким образом, с точки зрения законодательства большинства стран юридическая сила уведомлений, в том числе оферты и акцепта, связывается с фактом получения их адресатом. Однако специфика «электронной среды» сразу ставит следующий вопрос: что считать временем получения электронного уведомления адресатом? Необходимо ли фактическое ознакомление адресата с его содержанием или же

[1] Статья 54 Торгового кодекса Испании. Разумеется, как следует из характера акта, закрепившего данное правило, оно касается лишь предпринимательских договоров. Определенные проявления правила «почтового ящика» можно обнаружить даже в России. См. п. 2 ст. 194 ГК РФ: «Письменные заявления и извещения, сданные в организацию связи до двадцати четырех часов последнего дня срока, считаются сделанными в срок».

[2] Adams v. Lindsell [1818] EWHC KB J59; Household Fire Insurance v. Grant [1879] 4 Ex D 216 (Англия); § 63 Restatement Second on Contracts (США).

[3] *McKendrick E.* Contract Law: Cases and Materials. Oxford University Press. 2005. P. 125.

достаточно лишь одного факта наличия возможности ознакомления, возникающего в момент его попадания в электронный почтовый ящик?

В связи с этим особый интерес представляют положения Конвенции ООН об использовании электронных сообщений в международных договорах, которая содержит отдельную статью (ст. 10), посвященную времени и месту, когда электронное сообщение считается полученным. Так, временем получения электронного сообщения является момент, когда создается возможность для его извлечения адресатом по электронному адресу, указанному адресатом. Временем получения электронного сообщения, направленного по иному электронному адресу адресата (принадлежащему ему, но прямо не указанному в качестве адреса для переписки), является момент, когда создается возможность для его извлечения по этому адресу и адресату становится известно о том, что электронное сообщение было направлено именно по этому адресу. При этом возможность извлечения электронного сообщения возникает в тот момент, когда оно поступает на электронный адрес адресата. Дифференцированный подход по отношению к различным электронным адресам вызван тем фактом, что современные компании обычно имеют множество различных электронных адресов, и разумно ожидать, что они будут стараться указывать адрес, предназначенный для получения сообщений определенного характера, и не будут уделять одинаковое внимание всем имеющимся у них адресам. Поэтому если адресат указал определенный адрес для коммуникаций, а уведомление было отправлено вопреки его указаниям на иной адрес, такое уведомление не считается полученным до момента его фактического извлечения адресатом.

Таким образом, по общему правилу электронное сообщение считается полученным в тот момент, когда оно попало в сферу контроля адресата. Фактическое ознакомление с ним не имеет значения для целей решения вопроса о порождении им юридических последствий. Однако невозможность извлечения сообщения по причине государственных праздников или его поступления в нерабочее время может быть принята во внимание[1].

Весьма схожее регулирование содержится и в Единообразном законе США об электронных сделках (*UETA*), согласно ст. 15 (*b*) которого электронное сообщение считается полученным, когда оно поступает в информационную систему, используемую адресатом для обработки электронных сообщений того типа, к которому относится отправ-

[1] Доклад Рабочей группы по электронной торговле о работе ее сорок четвертой сессии (Вена, 11–22 октября 2004 г.). A/CN.9/571, п. 159.

ленное сообщение, и оно представлено в форме, позволяющей ее обработку в такой системе. Такое электронное сообщение признается полученным даже в том случае, если адресат не знал о его получении (ст. 15 (*e*)). Привязка момента получения сообщения к моменту его поступления в информационную систему адресата (например, на его почтовый сервер), а не к моменту его фактического прочтения выделяется в английском праве[1].

Долгое время российское законодательство не содержало специальных положений, регламентирующих момент получения юридически значимых уведомлений. Данный пробел был восполнен включением в ГК РФ ст. 165[1], вступившей в силу 1 сентября 2013 г. Данная статья предусматривает, что заявления, уведомления, извещения, требования или иные юридически значимые сообщения, с которыми закон или сделка связывает гражданско-правовые последствия для другого лица, влекут для этого лица такие последствия с момента доставки соответствующего сообщения ему или его представителю. Сообщение считается доставленным и в тех случаях, если оно поступило лицу, которому оно направлено (адресату), но по обстоятельствам, зависящим от него, не было ему вручено или адресат не ознакомился с ним.

Как видно, российский законодатель пошел по пути формализации общего правила, свойственного континентальной системе права, о необходимости доставки такого уведомления для того, чтобы оно могло породить соответствующие юридические последствия. Фактическое ознакомление адресата с таким уведомлением не имеет юридического значения. Как справедливо отмечает А.Г. Карапетов применительно к моменту вступления в силу уведомления о расторжении договора, «здравый смысл требует исключить необходимость доказывания того факта, что адресат реально ознакомился с сообщением. Учитывая то, что большинство извещений в коммерческой практике высылаются по почте или курьерской службой, никаких возможностей проконтролировать и соответственно доказать факт прочтения полученного сообщения у отправителя нет. Поэтому отправитель должен доказать лишь факт вручения»[2]. Данное соображение в полной мере применимо и к электронным сообщениям.

В целях пресечения недобросовестных действий со стороны получателя закон вводит презумпцию наличия такой доставки в случае обстоятельств, находящихся в сфере контроля адресата, по причине

[1] *Reed C., Angel J.* Op. cit. P. 202.

[2] *Карапетов А.Г.* Расторжение нарушенного договора в российском и зарубежном праве. М., 2007. С. 271.

которых такое уведомление не было фактически доставлено. В контексте электронных коммуникаций данная норма вполне позволяет применять подходы, обозначенные в Конвенции ООН от 23 ноября 2005 г. № 60/21 об использовании электронных сообщений в международных договорах: считать электронное сообщение доставленным в тот момент, когда оно поступает в информационную систему адресата (на его почтовый ящик). И даже более того – считать его доставленным и в тех случаях, когда оно не поступает на почтовый ящик по причине, зависящей от адресата, например по причине неоплаты услуг хостинг-провайдера, который прекратил обслуживание веб-сайта и почтового ящика. Примечательно, что правила ст. 165[1] ГК РФ являются диспозитивными: иное может быть предусмотрено в договоре (что весьма желательно), законе или практике взаимоотношений сторон.

Возникает вопрос: применяется ли данная норма к положениям об оферте и акцепте, которые, как известно, признаются совершенными в момент их получения адресатом (п. 1 ст. 433, ст. 435 ГК РФ)? Если между общим правилом о возникновении юридически значимых последствий уведомления в момент его доставки и положением о том, что оферта и акцепт должны быть получены адресатом для того, чтобы иметь силу, нет противоречий (нельзя считать доставленным то, что не было получено), то положение о презумпции доставки, как представляется, может вступать в противоречие со специальными нормами о порядке заключения договора (ст. 435–442 ГК РФ), поэтому в первую очередь должны применяться последние.

В связи с упомянутым в п. 1 ст. 433 ГК РФ положением о необходимости получения оферентом извещения об акцепте возникает вопрос о том, как быть с теми договорами, механизм которых *a priori* не предусматривает такого извещения, например, с *click-wrap*-соглашениями. В доктрине высказано мнение, что «оберточные» лицензии и *click-wrap*-соглашения, заключаемые путем акцепта оферты конклюдентными действиями (в порядке п. 3 ст. 434 ГК РФ), являются недействительными, поскольку извещение об акцепте до оферента не доходит[1].

Представляется, что такое толкование глубоко неверно. Здесь важно подчеркнуть, что рассматриваемое положение п. 1 ст. 433 ГК РФ направлено исключительно на защиту интересов оферента, ограждая его от риска оказаться связанным сразу несколькими договорами в отношении одного и того же объекта по причине того, что он, не получив ответа от одного контрагента, вступает в договор с другим. В «оберточных»

[1] *Витко В.С.* Гражданско-правовая природа лицензионного договора. М., 2012. С. 283.

лицензиях и *click-wrap*-соглашениях данная ситуация не возникает: они в силу самого своего существа рассчитаны на заключение с множеством контрагентов и сопровождают либо неисчерпаемый товар вроде цифрового контента, либо товар, который имеется в наличии[1]. Иными словами, подобного рода соглашения *всегда исполнимы* для оферента.

К тому же оферент, как хозяин оферты, вправе сам определить то, как может быть осуществлен ее акцепт. Поэтому оферент с учетом характера договора и способа его заключения может либо указать конкретный способ акцепта договора, либо и вовсе отказаться от дополнительных гарантий, предоставляемых данной статьей.

Указанный подход находит свое отражение в Венской конвенции о договорах международной купли-продажи товаров 1980 г.[2], а также воспринят в европейском праве. Так, в соответствии со ст. II-4:205 (3) *DCFR* «если в силу условий оферты, практики, сложившейся между сторонами, или обычая акцептант может принять оферту совершением действия без уведомления оферента, договор считается заключенным в момент начала совершения соответствующего действия». Данное правило отражает подходы, принятые как в романо-германском праве (§ 151 ГГУ, 864 АГУ, 1327 (1) ГК Италии), так и в английском праве[3].

Так что нет никаких оснований, кроме излишне формально-догматического подхода к праву, лишать юридической силы множество договоров, заключаемых в сфере электронной коммерции повседневно, лишь на том основании, что оферент не получил некоего извещения об акцепте, которое ему в принципе и не нужно.

Что же касается места заключения контракта, то в условиях электронной трансграничной среды, при которой *IT*-инфраструктура может быть географически распределенной, необходимы специальные подходы к определению места заключения договора.

Очевидно, что привязка места заключения договора к месту расположения технических средств, посредством которых он был заключен, является слишком произвольной. Во-первых, такие технические

[1] Если товара нет в наличии, то при грамотном подходе к организации веб-сайта разместить заказ будет просто невозможно и подобные соглашения просто не будут заключены.

[2] «Однако, если в силу оферты или в результате практики, которую стороны установили в своих взаимных отношениях, или обычая адресат оферты может, не извещая оферента, выразить согласие путем совершения какого-либо действия, в частности действия, относящегося к отправке товара или уплате цены, акцепт вступает в силу в момент совершения такого действия, при условии, что оно совершено в пределах срока, предусмотренного в предыдущем пункте» (п. 3 ст. 18).

[3] Weatherby v. Banham [1832] 5 C & P 228; *Treitel G.* The Law of Contract. London, 2007. § 2-026, 2-046.

средства могут располагаться за пределами правовой системы, где находятся отправитель и адресат сообщения; во-вторых, одна из сторон (а иногда и обе) могут и не иметь четкого представления о том, в какой географической точке расположена информационная система, посредством которой обрабатываются поступившие на их адрес уведомления. При таких обстоятельствах возникает необходимость в выработке такого правила определения места получения электронного сообщения, при котором существовала бы разумная связь между ним и его адресатом, а также обеспечивалась бы предсказуемость и конкретность в определении такого места другой стороной.

В качестве такого места Конвенция ООН об использовании электронных сообщений в международных договорах указывает местонахождение коммерческого предприятия сторон (п. 3 ст. 10). Под коммерческим предприятием понимается любое место, в котором сторона сохраняет не носящее временного характера предприятие для осуществления иной экономической деятельности, чем временное предоставление товаров или услуг из конкретного места (п. «*h*» ст. 4). Такое местонахождение определяется в соответствии с правилами ст. 6 Конвенции. В первую очередь принимается во внимание указание самой стороны о том, где находится ее коммерческое предприятие. В отсутствие таких указаний и при наличии нескольких коммерческих предприятий у стороны местом получения электронного сообщения будет то коммерческое предприятие, которое наиболее тесно связано с договором, в связи с которым было отправлено такое сообщение.

Следует особо выделить те правила, которые нашли свое отражение в п. 4 и 5 ст. 6 Конвенции об использовании электронных сообщений в международных договорах, поскольку в них отражены принципы, имеющие универсальный характер. Во-первых, какое-либо местонахождение не является коммерческим предприятием лишь в силу того, что в этом месте находится оборудование или технические средства, обслуживающие информационную систему, используемую лицом в связи с заключением договора. Во-вторых, факт использования стороной доменного имени или адреса электронной почты, связанного с какой-либо страной, не создает сам по себе презумпцию, что ее предприятие находится в этой стране.

Таким образом, Конвенция ООН об использовании электронных сообщений в международных договорах прямо закрепляет принцип юридического безразличия по отношению к местонахождению серверов и иных технических средств, используемых в процессе заключения и исполнения договоров в электронной форме. Как отмечается разработ-

чиками, «в Конвенции об электронных сообщениях применен осторожный подход к периферийной информации, связанной с электронными сообщениями, такой как *IP*-адреса, доменные имена или географическое расположение информационных систем, которая при всем своем на первый взгляд объективном характере практически не дает возможности однозначно установить физическое местонахождение сторон»[1].

Российское законодательство придерживается схожих принципов. В соответствии со ст. 444 ГК РФ, если в договоре не указано место его заключения, договор признается заключенным в месте жительства гражданина или месте нахождения юридического лица, направившего оферту. Таким образом, то место, где была фактически получена оферта или извещение об акцепте (при его наличии), а равно местонахождение технических средств и оборудования, с использованием которого был заключен договор, являются иррелевантными при решении вопроса о месте заключения договора с российским правом в качестве применимого.

§ 6. Правосубъектность сторон договора. Электронные агенты

Как известно, под правоспособностью понимается способность иметь гражданские права и нести обязанности (ст. 17 ГК РФ), под дееспособностью – способность гражданина своими действиями приобретать и осуществлять гражданские права, создавать для себя гражданские обязанности и исполнять их (п. 1 ст. 21 ГК РФ). Единство правоспособности и дееспособности нередко определяется в цивилистической науке как правосубъектность, т.е. как социально-правовая возможность лица быть участником гражданских правоотношений. В рамках данной работы нет возможности приводить все положения, связанные с понятием правосубъектности и содержанием соответствующих норм ГК РФ о право- и дееспособности, тем более что данный вопрос уже являлся предметом исследования многих ученых[2].

---

[1] См.: Пояснительная записка Секретариата ЮНСИТРАЛ к Конвенции ООН об использовании электронных сообщений в международных договорах. С. 15. Представляется, что указанные соображения, высказанные уважаемой организацией, позволяют в полной мере оценить практическую пригодность высказываемых в отечественной доктрине предложений по использованию местонахождения оборудования в качестве универсального критерия установления юрисдикции по рассмотрению интернет-споров (см., например: *Зажигалкин А.В.* Указ. соч. С. 10).

[2] См., например: *Козлова Н.В.* Правосубъектность юридического лица. М., 2005; *Тарасова А.Е.* Правосубъектность граждан. Особенности правосубъектности несовершеннолетних, их проявления в гражданских правоотношениях. М., 2008. Обе работы доступны в СПС «КонсультантПлюс» и содержат множество ссылок и цитат иных работ по данной тематике.

Для целей рассмотрения договорных аспектов в сфере электронной коммерции необходимо сказать следующее.

1. ГК РФ предусматривает, что полная дееспособность граждан наступает с 18 лет. Соответственно граждане, не достигшие указанного возраста, по общему правилу могут заключать договоры лишь с согласия своих законных представителей. Исключение составляют отдельные виды сделок, прямо указанные в законе. Данные виды сделок дифференцируются в зависимости от возраста несовершеннолетнего лица. Применительно к лицам, не достигшим возраста 14 лет, такие сделки включают: 1) мелкие бытовые сделки; 2) сделки, направленные на безвозмездное получение выгоды, не требующие нотариального удостоверения либо государственной регистрации; 3) сделки по распоряжению средствами, предоставленными законным представителем или с согласия последнего третьим лицом для определенной цели или для свободного распоряжения (п. 2 ст. 28 ГК РФ). Лица в возрасте от 14 до 18 лет помимо вышеуказанных сделок вправе самостоятельно распоряжаться своим заработком, стипендией и иными доходами (подп. 1 п. 2 ст. 26 ГК РФ). Как видно, российское законодательство предусматривает достаточно детальное и императивное регулирование, касающееся договоров, заключаемых несовершеннолетними лицами. В то же время именно данные лица составляют одну из наиболее многочисленных групп пользователей сети Интернет, а значит, они неизбежно становятся участниками отношений, возникающих в данной сети, в том числе и коммерческого характера. В условиях, когда архитектура сети Интернет не позволяет в большинстве случаев убедиться в личности контрагента и его возрасте, вышеуказанные положения формально создают немалые риски для ведения предпринимательской деятельности в сети Интернет, ведь многие сделки, совершенные с несовершеннолетними, формально могут быть признаны недействительными (ст. 172, 175 ГК РФ).

К слову сказать, подобные риски существуют и в зарубежных правопорядках, и там тоже подходят весьма гибко к решению данного вопроса. Например, в одном споре стороной был высказан аргумент о том, что контрагент являлся несовершеннолетним и не мог быть связанным условиями *click-wrap*-соглашения, на что суд, установив тот факт, что лицо получило определенную выгоду от продукта, распространяемого на условиях данного соглашения, пришел к выводу о недопустимости извлечения выгоды из договора без одновременного несения соответствующего бремени, содержащегося в его условиях[1].

[1] A. V. v. iParadigms, LLC, 544 E Supp. 2d 473, 480-81 (E.D. Va. 2008).

Представляется, что российское гражданское законодательство допускает не меньшую гибкость при решении вопросов о действительности сделок, заключенных несовершеннолетними в сети Интернет. Так, понятие «мелкая бытовая сделка» отсутствует в законодательстве, толкуется в зависимости от конкретных обстоятельств и может охватывать различного рода сделки, подпадающие под законодательство о защите прав потребителей[1]. Достаточно много сделок розничной купли-продажи может быть отнесено к категории мелких бытовых. Помимо мелких бытовых сделок ГК РФ допускает самостоятельное совершение несовершеннолетними сделок по распоряжению собственными средствами, причем их размер не ограничен какими-либо твердыми суммами: все зависит от щедрости законных представителей, предоставивших эти средства, либо от размеров собственных доходов несовершеннолетнего. Большинство договоров, заключаемых в сети Интернет, которые могут и не подпасть под категорию мелких бытовых сделок, все же могут подпасть под подобное исключение в виде распоряжения несовершеннолетним собственными средствами (которое исходя из общей презумпции добросовестности участников гражданского оборота должно предполагаться, пока не доказан факт их кражи). К тому же не следует забывать про соображения чисто практического порядка: если «цена вопроса» невелика, то риски оспаривания сделки в суде являются лишь гипотетическими. В тех же случаях, когда сумма сделки является высокой (приобретение дорогой бытовой или вычислительной техники), дополнительная идентификация пользователя может оказаться нелишней: оплата крупных заказов только банковской картой[2]; установление контакта с клиентом по телефону; заполнение данных на сайте с указанием возраста и иных сведений, которые могут свидетельствовать о нем, и пр. Совокупность данных мер будет свидетельствовать о проявленной добросовестности субъекта электронной коммерции и минимизировать риски, связанные с последующим оспариванием сделок, совершенных несовершеннолетними. Однако целиком устранить данные риски без одновременной утраты преимуществ электронной коммерции все же невозможно.

2. Риски, связанные с заключением договора лицом, формально не имеющим права на его заключение, встречаются не только в отношениях с физическими лицами. Подобные вопросы нередко возникают и в предпринимательских договорах. Речь идет главным образом о достаточно типичной ситуации, когда работник компа-

[1] См.: *Тарасова А.Е.* Указ. соч.

[2] Данный подход реализован, в частности, в российском *Apple Store*.

нии устанавливает программное обеспечение на рабочий компьютер, присоединяясь к условиям *click-wrap*-соглашения, а компания-работодатель отрицает факт наличия договорных отношений, утверждая об отсутствии у такого работника необходимых полномочий на заключение договора. Данная проблема уже была предметом детального рассмотрения в другой работе[1]. Там был сделан вывод о возможности признания организации работодателя связанной условиями *click-wrap*, заключенного ее сотрудником в тех случаях, когда обстоятельства, сопутствующие заключению такого договора, свидетельствовали о его одобрении со стороны компании[2]. К таким действиям в контексте *click-wrap*-соглашений и электронной коммерции в целом может быть отнесена произведенная по такому договору оплата; переписка уполномоченных лиц с контрагентом, из которой следует их готовность приобрести соответствующий продукт; содержание должностных инструкций лица, фактически заключившего договор, фактическое использование блага, выступавшего предметом спорного договора, в интересах компании и т.д. Помимо аргументов о последующем одобрении сделки можно также ссылаться на сложившиеся в *IT*-индустрии практики заключения договоров и обычаи делового оборота. Именно на них чаще всего ссылаются американские суды при рассмотрении подобных споров. В частности, один из судов указал, что «заключение *click-wrap*-соглашения является неотъемлемой частью процесса установки программного обеспечения, поэтому оно не должно являться сюрпризом для компании, деятельность которой носит международный характер». Далее суд сделал вывод о том, что «компании не могло не быть известно о возможности заключения такого соглашения ее сотрудниками, поскольку в противном случае это означало бы, что программное обеспечение было установлено сотрудником сторонней организации на рабочий компьютер организации без какого-либо надзора со стороны ее сотрудников, что немыслимо для современной компании»[3].

---

[1] *Савельев А.И.* Лицензирование программного обеспечения в России: Законодательство и практика. М., 2012. § 2, гл. 2.

[2] Информационное письмо от 23 октября 2000 г. № 57 «О некоторых вопросах практики применения статьи 183 Гражданского кодекса Российской Федерации».

[3] Via Viente Taiwan, L.P. v. United Parcel Service, Inc. No. 4:08-cv-301, 2009 U.S. Dist. LEXIS 12408 (E.D. Tex. Feb. 17, 2009). См. также: Appliance Zone, LLC v. NexTag, Inc. 2009 U.S. Dist. LEXIS 120049: «...заключение договора рассматриваемым способом и отображение его условий является типичным для сферы онлайн-ритейла». В данном деле суд также отверг аргумент истца о том, что его сотрудник не имел полномочий на заключение договора, поскольку выполнение им функций системного администратора компании создавало для третьих лиц видимость наличия у него полномочий (*apparent*

Как представляется, данные аргументы *mutatis mutandis* являются актуальными не только для случаев заключения лицензионного договора на программное обеспечение в форме *click-wrap*-соглашения, но и для любых *click-wrap*- и *browse-wrap*-соглашений, которые заключаются работниками организации в процессе осуществления ими своих должностных обязанностей.

Однако далеко не всегда соглашения в сети Интернет заключаются посредством взаимодействия физических лиц.

В настоящее время значительная часть электронных сделок заключается без непосредственного участия человека, т.е. при помощи автоматизированных информационных систем, которые именуют обычно «электронными агентами» (*electronic agents*) или, как их иногда еще называют, программами-роботами. Подобно тому, как стандартизация договорных условий в свое время ознаменовала переход к эпохе индустриализации и массовому производству, адаптировав процесс заключения договора к новым реалиям, использование электронных агентов и иных средств автоматизации договорного процесса является неизбежным следствием перехода к информационному обществу и адаптации бизнес-процессов к новым требованиям. Технические средства начинают использоваться не только как средство коммуникации между людьми, но и в качестве заменителя человека при принятии решений, что не может не ставить вопрос о действительности волеизъявления сторон при заключении договора подобным, пока еще необычным способом[1].

В связи с тем, что использование электронных агентов является в некоторой степени неотъемлемой частью электронной коммерции и в перспективе следует ожидать все бóльшую степень автоматизации процесса контрактования, имеет смысл остановиться на правовом статусе электронных агентов подробнее.

Следует выделить две группы отношений, возникающих в связи с использованием электронных агентов при заключении и исполнении договоров[2]:

1) «человек – электронный агент»;

2) «электронный агент – электронный агент».

---

authority), достаточную для того, чтобы связать компанию-работодателя соответствущими договорными обязательствами. Здесь представляет собой интерес доктрина доверия к внешним фактам, которая освещается далее применительно к электронным агентам.

[1] *Tom Allen, Robin Widdison*. Can Computers Make Contracts? // Harvard Journal of Law Technology. No 9. 1996.

[2] Данная классификация проводится в ст. 14 Единообразного закона США об электронных сделках.

Примером первого типа отношений являются многочисленные случаи заключения договоров с интернет-магазинами, где специальная программа обрабатывает поступивший заказ и отправляет подтверждение о его принятии. Обычно именно эта ситуация и является предметом рассмотрения в отечественной доктрине при анализе вопросов, связанных с использованием электронных агентов. Как правило, анализ сводится к проведению аналогий с заключением договоров с использованием автоматов и последующим выводом о том, что «воля, выраженная в договоре, – воля владельца программы-робота»[1]. Как отмечает В.О. Калятин, «программа же не принимает решение, а только перенаправляет клиенту заранее определенное на данный случай решение владельца сайта»[2].

Соглашаясь в целом со сделанным выводом, хотелось бы добавить, что в таких достаточно простых по современным меркам случаях действительно можно говорить о наличии заранее выраженного согласия владельца сайта с теми действиями, которые совершит электронный агент в рамках того «задания», которое ему было дано. Российская доктрина и судебная практика признают действительность данной категории в различных контекстах договорного права[3], что можно рассматривать в качестве проявления общего принципа осуществления гражданских прав по усмотрению участников оборота (ст. 9 ГК РФ).

Однако при этом может возникнуть вопрос о том, как следует расценивать различного рода программные сбои, вызванные внутренними причинами (например, ошибками при вводе данных сотрудниками интернет-магазина) или внешними причинами (скажем, хакерскими атаками). В обоих случаях результат функционирования электронного агента, может, мягко говоря, отличаться от запланированного его владельцем изначально. Ранее уже приводился пример того, как

[1] См., например: *Дмитрик Н.А.* Осуществление субъективных гражданских прав с использованием сети Интернет. С. 89; *Ананько А.* Заключение договоров путем электронного обмена данными // www.russianlaw.net/law/doc/a123.htm; *Карев Я.А.* Указ. соч. С. 216. К аналогичным выводам приходят и в зарубежной доктрине: См.: Online Contract Formation. Ed. by Stephan Kinsella and Andrew Simpson. Oceana Publications. N.Y., 2004. P. 49–50.

[2] *Калятин В.О.* Право в сфере Интернета. С. 337.

[3] Например: заранее выраженное согласие поручителя на последующее изменение основного обязательства (п. 16 постановления Пленума ВАС РФ от 12 июля 2012 г. № 42 «О некоторых вопросах разрешения споров, связанных с поручительством»); заранее выраженное согласие на заключение сублицензионных договоров (п. 17 постановления Пленума Верховного Суда РФ № 5, Пленума ВАС РФ от 26 марта 2009 г. № 29 «О некоторых вопросах, возникших в связи с введением в действие части четвертой Гражданского кодекса Российской Федерации»).

вследствие допущенных технических ошибок при указании цены стоимость телевизора была указана на веб-сайте как 3 ф. ст. вместо 300[1], а фотокамеры – 98 ф. ст. вместо 600[2]. В.О. Калятин приводит еще один пример, в котором на сайте фирмы «Кодак» было размещено предложение купить одну из моделей цифровых камер этой фирмы по специальной цене в 100 ф. ст. в канун Нового года (при обычной стоимости такой камеры в 329 ф. ст.). Электронный агент добросовестно известил всех покупателей о принятии их заказа. Ошибка вскрылась уже потом, и компания заявила об отсутствии какого-либо соглашения с покупателями. И лишь под давлением общественности компания была вынуждена выполнить все размещенные заказы[3].

В иностранной литературе предлагается решать такие вопросы по правилам оспаривания договора по причине допущенной ошибки. Общий принцип сводится к следующему: если характер допущенной ошибки является явно очевидным для любого разумного лица (например, продажная стоимость установлена в виде 40 долл. при обычной стоимости в 4000 долл., то акцептант не должен иметь возможности «ухватиться» (*snap*) за такое предложение)[4]. В приведенном выше примере нельзя говорить об очевидности ошибки – 100 фунтов не является бросовой ценой, да и распродажи в канун Нового года являются обычным делом.

По российскому праву с учетом недавно произошедших изменений такая ситуация могла бы рассматриваться по правилам ст. 178 ГК РФ (недействительность сделки, совершенной под влиянием существенного заблуждения). Данная статья предусматривает возможность признания сделки, совершенной под влиянием заблуждения, недействительной по иску стороны, действовавшей под влиянием заблуждения, если заблуждение было настолько существенным, что эта сторона, разумно и объективно оценивая ситуацию, не совершила бы сделку, если бы знала о действительном положении дел.

Новая редакция ст. 178 ГК РФ существенно расширила перечень ситуаций, квалифицируемых в качестве существенного заблуждения, включив в него помимо всего прочего *очевидные* оговорки, описки и опечатки. Правда, применение положений ст. 178 ГК РФ к предпринимательским отношениям, скорее всего, будет носить нечастый

[1] *Stone R.* Op. cit. P. 55.

[2] *Arthur C.* Op. cit.

[3] *Калятин В.О.* Право в сфере Интернета. С. 337.

[4] *Lerouge J.* The Use of Electronic Agents Questions under Contractual Law: Suggested Solutions on a European and American Level // Marshall Journal of Computer & Information Law. No 18. 2000. P. 427.

и исключительный характер по причине того, что подобного рода ошибки по общему правилу должны охватываться понятием предпринимательского риска. К тому же в соответствии с общими принципами договорного права должник несет ответственность за действия как своих работников, так и третьих лиц, привлеченных к исполнению обязательства (ст. 402, 403 ГК РФ). Из этого следует, что он должен тем более нести ответственность за действие подконтрольных ему электронных агентов, решение об использовании которых он принимал сам.

Что же касается возможных искажений «волеизъявления» электронного агента вследствие хакерской атаки, то в данном случае гораздо больше оснований говорить о том, что воля владельца и его электронного агента не совпадают, а следовательно, оснований для квалификации возникших отношений в качестве договорных становится меньше. По мнению Н.А. Дмитрика, подобного рода «сделку просто нельзя считать совершенной, так как лицо, перенастроившее программу-робота, заранее знало об истинной воле лица и знало, что обладатель программы-робота не давал своего согласия заключить сделку на таких условиях. Аналогично нельзя считать состоявшейся «покупку» товара в автомате, если такой товар был «выбит» из автомата либо вместо полагающейся монеты в автомат был вставлен простой металлический кружок»[1].

Приведенная аналогия не может не вызывать сомнений в своей универсальности. Безусловно, когда в качестве покупателя выступает то же самое лицо, которое и совершило недобросовестные действия по взлому электронного агента, есть все основания говорить не только об отсутствии договора, но и о наличии деликтных и даже уголовных отношений. Но в том случае, когда в качестве покупателя выступает третье лицо, не совершавшее противоправных действий и полагающееся на информацию, предоставляемую ему электронным агентом, подход должен быть иным. В данном случае мы опять имеем дело с распределением между сторонами рисков совершения третьими лицами противоправных действий. В случае если одной из сторон является лицо, осуществляющее предпринимательскую деятельность, подлежат применению положения п. 3 ст. 401 ГК РФ: такое лицо несет ответственность за неисполнение или ненадлежащее исполнение своих обязательств, если только не докажет, что надлежащее исполнение обязательства стало невозможным вследствие обстоятельств непреодолимой силы, если иное не установлено законом или договором.

[1] *Дмитрик Н.А.* Осуществление субъективных гражданских прав с использованием сети Интернет. С. 90.

Хакерские атаки в сети Интернет не отвечают признакам обстоятельств непреодолимой силы, так как не имеют 1) чрезвычайного характера, выступая одной из «классических» угроз безопасности интернет-сайта, а также 2) качества непредотвратимости, так как многие атаки могут быть предотвращены использованием специальных технических средств. Таким образом, риски, связанные с несанкционированным изменением заложенной в электронных агентах программы, по общему правилу должен нести их владелец в случае наличия у него предпринимательского статуса.

Только такой подход является справедливым и отвечающим требованиям оборота: ведь участники оборота судят о воле контрагентов по тому, как она проявляется вовне, т.е. по «волеизъявлению», которое в данном случае исходит от электронного агента. К тому же у владельца сайта больше возможностей по предотвращению негативных последствий подобного рода казусов и именно от его усилий в значительной степени зависит сама возможность их наступления. Примечательно, что судебная практика возлагает риски, связанные с наступлением убытков, вызванных несанкционированным использованием программ-роботов для установления международных соединений, на владельца участка сети, к которой было осуществлено несанкционированное подключение, а не на его контрагента[1], главным образом потому, что ответственность за принятие мер по предотвращению подобных убытков лежит именно на таких лицах, поскольку соответствующий сегмент сети находится под их контролем.

Наиболее ярко вопросы о соотношении воли и волеизъявления при использовании электронных агентов и распределении рисков между сторонами проявляются в схеме «электронный агент – электронный агент». Многие договоры заключаются между компьютерами

[1] См., например: постановление Восьмого арбитражного апелляционного суда от 25 ноября 2011 г. № А70-3415/2011 («Согласно выводам эксперта исходящие международные соединения... инициировались посредством использования программы-робота. При существующей схеме организации предоставления услуги связи (когда сервер авторизации находится на стороне провайдера) такая атака с целью взлома аккаунта могла быть проведена только на аппаратуру оператора связи... Оператор связи должен принимать организационные и технические меры, направленные на предотвращение несанкционированного доступа к линиям связи, сооружениям связи (находящимся как внутри, так и вне сооружений связи) и передаваемой по сетям информации»); постановление Восьмого арбитражного апелляционного суда от 4 февраля 2013 г. № 08АП-10404/12 (ответственность за ненадлежащую эксплуатацию абонентской линии или пользовательского (оконечного) оборудования несет сам абонент, что влечет возложение несения бремени негативных последствий несанкционированного доступа к сетям связи лиц, не имеющих на это права).

безо всякого человеческого участия. Примером могут служить случаи, когда по факту возникновения необходимости в определенном товаре автоматически генерируется запрос, передаваемый электронному агенту, который осуществляет поиск в Интернете наиболее выгодных предложений по различным параметрам и размещает заказ, который также обрабатывается в автоматическом режиме. Или другой пример. Между организациями, которые вовлечены в единый технологический процесса создания продукта (например, предприятие по сборке автомобилей и предприятия, производящие запчасти), нередко существуют соглашения об электронном обмене данными *EDI*, в рамках которых заказ на недостающие запчасти размещается и принимается в автоматическом режиме.

Приведенные примеры демонстрируют, что электронный агент может быть автономным. Еще в 1996 г. американские исследователи писали о возможности компьютеров действовать не только «автоматически», но и «автономно». Автономные машины могут учитывать предыдущий опыт, модифицировать свои инструкции в соответствии с ним и даже самостоятельно создавать их[1]. Они могут делать выбор, принимать решения, давать или не давать согласие на совершение определенных действий[2]. В связи с этим вряд ли уместно проведение аналогий между такими интеллектуальными электронными агентами и автоматами, о которых идет речь в ст. 498 ГК РФ. Сложность алгоритмов электронных агентов, предопределяющая высокую степень имеющегося у них усмотрения при решении различных вопросов договорно-правового характера, мало коррелирует с такими пассивными техническими инструментами, как автоматы. При использовании таких электронных агентов договоры могут заключаться в отсутствие знания их владельцев о факте заключения договора и его условиях. Подобные случаи могут поставить стороны в тупик при попытке применения классических канонов договорного права[3].

В качестве примера такой ситуации можно привести достаточно любопытное дело, рассмотренное судом штата Колорадо в 2007 г.[4] Ответчиком по данному спору выступал известный интернет-архив *Wayback Machine*, который осуществляет копирование содержания вебстраниц различных сайтов сети Интернет с определенным временны́м

[1] Пояснительная записка Секретариата ЮНСИТРАЛ к Конвенции ООН об использовании электронных сообщений в международных договорах. Нью-Йорк, 2007. С. 69.

[2] *Tom Allen & Robin Widdison*. Op. cit. P. 26–27.

[3] *Lerouge J.* Op. cit. P. 406.

[4] Internet Archive v. Shell. Civil Action. No 06-cv-01726-LTB-CBS, 2007 U.S. Dist. LEXIS 10239 (D. Colo. Feb. 13, 2007).

промежутком посредством специальных программ – ботов (схожих с теми, которые используются поисковыми системами). Истец разместил на своем сайте уведомление, что «любое копирование или распространение информации с данного сайта означает заключение договора», условия договора предусматривали обязанность выплаты 5000 долл. за каждую скопированную страницу. Поскольку данные страницы были скопированы по результатам «посещения» их ботом интернет-архива, истец предъявил к нему требования об оплате. Интернет-архив ссылался на то, что поскольку ни одному его сотруднику не было известно о факте заключения договора и его условиях, а все происходило исключительно в автоматическом режиме, никакого договора не было. К сожалению, узнать позицию суда по данному вопросу не удастся, поскольку дело было завершено мировым соглашением, но само по себе данное дело заставляет задуматься.

В зарубежной доктрине предлагались различные подходы к решению подобных ситуаций.

1. Признание наличия отношений представительства (агентирования) между владельцем программы-робота (принципалом) и электронным агентом (теперь в буквальном смысле слова)[1]. Однако данная теория вызвала шквал критики, главным образом потому, что отношения представительства предполагают наличие правосубъектности на стороне представителя, с которой у компьютера явные проблемы. По мнению ЮНСИТРАЛ, хотя использование выражения «электронный агент» и допустимо с точки зрения удобства, аналогия между автоматизированной системой сообщений и сбытовым агентом неправомернаы. К функционированию таких систем не могут применяться общие принципы агентского права (например, принципы, предусматривающие ограничение ответственности при наличии вины агента)[2].

2. Признание электронного агента с элементами искусственного интеллекта правосубъектным лицом[3]. Основным аргументом сторонников данного подхода выступает наличие у таких «субъектов» возможности принимать автономные решения, что является свойством субъекта права. Некоторые авторы идут еще дальше, предлагая допус-

[1] *Fisher J.* Computers as Agents: A Proposed Approach to Revised U.C.C. Article 2 // Indiana Law Journal. No 72. 1997. P. 545, 570.

[2] Пояснительная записка Секретариата ЮНСИТРАЛ к Конвенции ООН об использовании электронных сообщений в международных договорах. С. 69.

[3] *Solum L.* Legal Personhood for Artificial Intelligences // North Carolina Law Review. No 70. 1992. P. 1231.

тить возможность предъявления иска (!) к такому «субъекту»[1]. В ответ на вполне резонный вопрос о том, каким имуществом будет отвечать такой «субъект», они предлагают использовать механизм страхования ответственности[2]. Подобно тому, как это имеет место в отношении юридических лиц, сторонниками данного подхода допускается возможность регистрации электронных агентов, правда, сразу делается оговорка о том, что издержки такой регистрации превысят всю возможную пользу от предоставления электронным агентам статуса субъекта права[3].

Оценивая данный подход с позиций российского права и современного развития уровня техники, испытываешь смешанные чувства. С одной стороны, сложно избавиться от чувства некоторой бредовости всех эти рассуждений: признать то, что традиционно считается объектом права, в качестве субъекта права весьма непросто. С другой стороны, когда-то и рабы рассматривались в качестве объектов прав, а юридические лица и вовсе являются фикцией, что не препятствует признанию их правосубъектности. А главное, развитие технологий происходит такими темпами, что мысли об искусственном интеллекте не выглядят такими уж искусственными, о чем свидетельствует и факт появления специальных юридических исследований на сей счет[4]. Так что нельзя исключать возможность возникновения через некоторое время реальной необходимости определения правового статуса устройств, оснащенных искусственным интеллектом. Однако в таком случае все равно придется решать вопрос об имущественной обособленности таких субъектов, без которой гражданско-правовой статус субъекта утрачивает какой-либо смысл.

3. Наибольший интерес представляет собой третий подход, заключающийся в применении к отношениям, связанным с использованием электронных агентов, теории доверия к внешним фактам[5]. Ее суть можно свести к следующему. Участники оборота не могут всегда видеть истинные права и полномочия, особенно когда оборот приобрел уже безличные формы. Участники оборота находятся в опасности, поскольку,

---

[1] *Wein L.* The Responsibility of Intelligent Artifacts: Toward an Automated Jurisprudence // Harvard Journal of Law & Technology. No 6. 1992. P. 103 and ff.

[2] Правда, на вопросы о том, кто именно должен страховать ответственность, готовы ли страховые компании ее страховать и что делать в отсутствие такой страховки, ответа ими не дается.

[3] *Tom Allen, Robin Widdison*. Op. cit. P. 42.

[4] См., например: *Pagallo U.* The Laws of Robots: Crimes, Contracts and Torts. Springer-Verlag. Berlin, 2013.

[5] *Yves Poullet*. Conclude a Contract Through Electronic Agents? 1999.

поверив видимому положению, проявленному во внешней, фактической ситуации, могут ошибиться относительно действительных прав, по своей природе невидимых, равно как и недоступных иным органам чувств. Для третьих лиц недостаток права часто бывает нераспознаваем, в связи с чем безопасность оборота требует доверия к внешним проявлениям наличия права. Как отмечал Рене Демог, «тот, кто заключил договор с лицом, имеющим полную видимость права, не должен быть обманут. Разумная видимость права должна в отношениях с третьими лицами производить тот же эффект, что и само право»[1]. И.А. Покровский еще в начале XX в. писал, что «при современных условиях на участников делового оборота не может быть возложена обязанность проверять наличность всех необходимых условий юридической сделки»[2].

Теория доверия к внешним фактам имеет много различных проявлений[3]. В контексте обязательственного права она означает, что лицо может оказаться связанным обязательством даже в отсутствие своей воли на то, если другое лицо добросовестно полагало, что такая воля имеет место быть. Данный подход находит свое отражение, например, во французском[4], голландском[5], английском[6], американском договорном праве[7]. Наиболее универсальным примером является подход к инкорпорированию стандартных условий в договор, при котором факта подписи другой стороны достаточно для того, чтобы они стали частью договора, даже если фактического ознакомления с текстом таких условий не происходило[8].

В контексте электронных сделок она будет применяться приблизительно следующим образом. В случае, если интернет-магазин исполь-

---

[1] *Demogue R.* Notions fondamentales du droit prive. Paris, 1911. P. 67.

[2] *Покровский И.А.* Основные проблемы гражданского права. М., 2003. С. 201.

[3] Одним из наиболее известных ее проявлений является объяснение концепции добросовестного приобретения права собственности от неуполномоченного лица. См., подробнее: *Черепахин Б.Б.* Юридическая природа и обоснование приобретения права собственности от неуполномоченного отчуждателя. М., 2001.

[4] *Nicholas B.* The French Law of Contract, Clarendon Press Oxford. 2ed. 1992. P. 178.

[5] *Harkamp A., Tillema M,* Contract Law in the Netherlands. Kluwer Law International, 1995. P. 35, 61 and 76.

[6] *McKendrick E.* Op. cit. P. 23–50.

[7] Farnsworth on Contracts. 4th ed. Aspen Publishers. N.Y. P. 115.

[8] О регулировании стандартных условий договора и защите слабой стороны см. подробнее: *Клочков А.А.* Стандартные (общие) условия договоров в коммерческом обороте: правовое регулирование в России и зарубежных странах: дис. ... канд. юрид. наук. М., 2002; *Савельев А.И.* Договор присоединения в российском гражданском праве // Вестник гражданского права. 2010. № 5; *Карапетов А.Г., Савельев А.И.* Свобода договора и ее пределы: в 2 т. М., 2012. Т. 2: Пределы свободы определения условий договора в зарубежном и российском праве.

зует электронных агентов, которые осуществляют оформление заказа и такой заказ был принят, то договор должен быть признан заключенным безотносительно к тому, что в программе-роботе имели место ошибки, которые могли повлиять на факт заключения договора или его условия (например, указание старой цены на товар либо принятие заказа в отсутствие его на складе). В данном случае интернет-магазин несет полную ответственность за ту *видимость факта* заключения договора, которая возникла в результате его деятельности.

Данная теория удобна тем, что она предоставляет суду определенное пространство для маневра, позволяя учитывать обстоятельства процесса заключения договора при решении вопроса о наличии последнего. Однако вряд ли данная теория способна стать универсальным средством для решения вопросов о влиянии деятельности электронных агентов на права и обязанности их сторон. Непонятно, как ее применять в случае контрактования по схеме «электронный агент – электронный агент». В таких случаях обе стороны находятся в равном положении, в равной степени создав видимость права друг для друга. Как разрешать возникшие конфликты в таких случаях – не ясно. Но так или иначе, такая теория может стать неплохим вариантом на переходный период, пока использование электронных агентов и уровень развития искусственного интеллекта не обусловили необходимость выработки полноценного регулирования *sui generis* в отношении них.

В российских условиях теория доверия к внешним фактам в контексте договорного права может быть рассмотрена через призму долгих споров о том, что имеет приоритет: воля или волеизъявление. Любое решение законодателя в пользу или воли, или волеизъявления по самой сущности своей представляет способ защиты соответствующей стороны в договоре – либо той, чья воля порочна, либо ее контрагента и тем самым оборота[1]. Российскому праву известны случаи приоритета волеизъявления над волей. Так, например, согласно ст. 173 ГК РФ сделка, совершенная за пределами правоспособности юридического лица, может быть признана недействительной, только если другая сторона знала или должна была знать о таких ограничениях. Налицо классический пример действия доверия к внешним фактам: одно лицо действовало, как если бы оно имело право (подписало договор), другое лицо добросовестно (т.е. при извинительном незнании о наличии порока в реализации права) положилось на действия такого лица. Примеров, в том числе и из сферы вещного права (например, правила

[1] *Брагинский М.И., Витрянский В.В.* Договорное право. Общие положения. М., 2003. С. 172.

о виндикационном иске, ст. 302 ГК РФ), можно приводить много. Главное в другом: использование применительно к ошибкам электронных агентов теории доверия к внешним фактам не деформирует российскую правовую систему, не трансплантирует в нее инородные элементы, а позволяет оценить ситуацию «по существу», с учетом всех обстоятельств (наличия или отсутствия предпринимательского или потребительского статуса у сторон, характер очевидности ошибки для разумного участника оборота и т.д.) и вынести решение в отсутствие специальных норм об электронных агентах в российском праве, без привлечения при этом конструкций вроде электронного представительства.

В перспективе имеет смысл внести ясность в правовой статус электронных агентов и рассмотреть возможность заимствования зарубежного и международного опыта в данной области.

§ 7. Динамика заключенного договора: особенности одностороннего изменения и прекращения договора в сфере электронной коммерции

Электронной коммерции, как и иным процессам, происходящим в сети Интернет, присущ динамический характер. Появление новых технологий, бизнес-моделей, правовых норм и прочих обстоятельств, влияющих на осуществление предпринимательской деятельности в сети Интернет, обусловливает необходимость оперативного внесения изменений в договоры, заключаемые в сфере электронной коммерции.

Само по себе изменение договора не является экстраординарным явлением: существуют специальные положения, посвященные порядку изменения договора (ст. 450–453 ГК РФ). Другое дело, что данные положения были выработаны еще в «доисторические» времена и не учитывают современные реалии и динамическую природу электронной коммерции. В связи с этим следование данным положениям нередко делает процесс изменения договора сложнее, чем его заключение.

Типичный пример. Пользователь заключает *click-wrap*-соглашение, по которому предоставляется право на использование компьютерной программы или информационного сервиса, которое носит длящийся характер. Как правило, правообладатель (сервис-провайдер) не несет каких-либо специфических затрат на заключение такого рода договоров с контрагентами: весь процесс является автоматизированным, последующее получение доступа к благу или его использование невозможно без выражения согласия с такими условиями. В случае же с последующим изменением условий такого договора не так все просто.

Поскольку изменение договора представляет собой отдельный договор, обе стороны должны выразить свое согласие по поводу него[1]. Инициатор изменений должен предпринять усилия по доведению условий таких изменений до сведения контрагента. В контексте электронной коммерции это означает, что необходимо обеспечить учет всех лиц, которые вступили в договорные отношения (заключили *click-wrap*-соглашения), получить их контактные данные, обеспечить возможность поддержания их в актуальном состоянии, осуществить впоследствии адресную рассылку изменений, вносимых в договор, и надеяться, что соответствующее уведомление успешно дошло до адресата. Очевидно, что это уже совсем иные транзакционные издержки со стороны владельца электронного бизнеса, особенно при большом количестве пользователей (клиентов). Отсюда предпринимаемые попытки сделать одностороннее изменение договора столь же простым, как и заключение первоначального договора: соответствующие изменения публикуются на веб-сайте, а инициативу по ознакомлению с ними должен проявлять пользователь, подобно тому, как это происходит при заключении им первоначального договора.

Подобная практика одностороннего изменения условий договоров, заключенных в сети Интернет, стала весьма распространенной. Однако распространенность не означает легитимность: идея о том, что в договор могут быть внесены изменения без ведома другой стороны, является достаточно «дикой» с точки зрения классического договорного права. В связи с этим хотелось бы остановиться на вопросе о том, как регламентируется вопрос об одностороннем изменении договора по российскому праву, и оценить легитимность сложившихся в сети Интернет бизнес-практик изменения договора.

Общее регулирование вопросов оснований и пределов допустимости одностороннего изменения условий договора содержится в ст. 310 и 450 ГК РФ. В соответствии со ст. 310 ГК РФ «Односторонний отказ от исполнения обязательства и одностороннее изменение его условий не допускаются, за исключением случаев, предусмотренных законом. Односторонний отказ от исполнения обязательства, связанного с осуществлением его сторонами предпринимательской деятельности, и одностороннее изменение условий такого обязательства допускаются также в случаях, предусмотренных договором, если иное не вытекает из закона или существа обязательства». Положения п. 3 ст. 450 ГК РФ предусматривают, что «в случае одностороннего отказа от исполнения

[1] См.: п. 1 ст. 420 ГК РФ: «Договором признается соглашение двух или нескольких лиц об установлении, изменении или прекращении гражданских прав и обязанностей».

договора полностью или частично, когда такой отказ допускается законом или соглашением сторон, договор считается соответственно расторгнутым или измененным».

Как видно, указанные положения находятся в некотором противоречии между собой: ст. 310 ГК РФ допускает установление в договоре оснований для его одностороннего изменения лишь в предпринимательских договорах, в то время как п. 3 ст. 450 ГК РФ не делает такой оговорки, формально допуская указание оснований для его одностороннего изменения в любом договоре, в том числе и потребительском.

Вопрос о соотношении данных норм является одним из наиболее обсуждаемых в дискуссии об основаниях и пределах допустимости одностороннего изменения договоров с участием потребителей, поэтому на нем имеет смысл остановиться в первую очередь.

Существуют различные подходы к разрешению данной коллизии.

1. Отдать приоритет положениям п. 3 ст. 450 ГК РФ как специальной норме, посвященной договорным обязательствам, по сравнению с общей нормой ст. 310, посвященной обязательствам в целом (п. 3 ст. 420 ГК РФ). Данный подход разделяется некоторыми судами[1]. Несмотря на всю кажущуюся простоту данного толкования, оно является уязвимым с формальной точки зрения. В соответствии с п. 3 ст. 420 ГК РФ «к обязательствам, возникшим из договора, применяются общие положения об обязательствах (статьи 307–419), если иное не предусмотрено правилами *настоящей главы* и правилами об отдельных видах договоров, содержащимися в настоящем Кодексе». Данное положение содержится в гл. 27 ГК РФ, а ст. 450 ГК РФ входит в гл. 29 ГК РФ, поэтому п. 3 ст. 420 ГК РФ может быть использован в качестве обоснования приоритета положений ст. 450 ГК РФ над ст. 310 ГК РФ[2].

2. Признать п. 3 ст. 450 ГК РФ тем самым «законом», о котором говорится в ст. 310 ГК РФ, в качестве основания для легитимизации од-

[1] Постановление ФАС Северо-Кавказского округа от 15 февраля 2000 г. по делу № Ф08-204/2000: «Применительно к договорным обязательствам в пункте 3 статьи 450 Гражданского кодекса не содержится ограничения, предусмотренного статьей 310 Гражданского кодекса, из чего следует, что закон допускает включение условия о праве на односторонний отказ и в договоры, не связанные с предпринимательской деятельностью»; постановление ФАС Волго-Вятского округа от 23 мая 2008 г. № А29-3799/2007: «условие о праве абонента на одностороннее изменение объема потребляемой энергии включено в договор, и, соответственно, п. 3 ст. 450 ГК РФ применяется приоритетно по отношению к общим положениям об обязательствах (к числу которых относится и статья 310 ГК РФ)».

[2] См.: *Соменков С.А.* Расторжение договора в гражданском обороте: теория и практика. М., 2005. С. 95.

ностороннего изменения условий потребительского договора. При всей кажущейся изящности данного подхода нетрудно заметить, что подобное толкование, как, впрочем и предыдущее, практически полностью перечеркивает значение ст. 310 ГК РФ, поскольку она окажется неприменимой к самой многочисленной разновидности обязательств – договорам. В то же время, по утверждениям разработчиков ГК РФ, именно договоры имелись в виду при включении данной нормы. Как отмечает А.Л. Маковский, хотя ст. 310 ГК РФ и находится в подразделе, посвященном общим положениям об обязательствах, но прямо говорит о том, что соответствующее условие не может быть включено именно в договор[1].

Об ошибочности рассматриваемого подхода свидетельствует и правовая позиция Конституционного Суда РФ, высказанная им в одном из постановлений, где предметом рассмотрения было схожее толкование положений закона[2]. Данное постановление примечательно тем, что оно напрямую касается вопросов толкования понятия «в случаях, предусмотренных законом» для целей конкретизации положений, касающихся правомерности одностороннего изменения условий договора с гражданином экономически более сильной стороной. Суд указал, что «только федеральным законом, а не договором должно определяться, возможно ли (а если возможно – то в каких случаях) снижение банками в одностороннем порядке процентных ставок, с тем чтобы исключалось произвольное ухудшение условий договора для гражданина – вкладчика в отсутствие каких-либо объективных предпосылок. Таким образом, *без дополнительного правового регулирования, конкретизирующего основания и пределы необходимых ограничений*, по существу *отсылочное положение* ч. 2 ст. 29 Федерального закона «О банках и банковской деятельности»[3] (далее – Закон о банках и бан-

[1] *Маковский А.Л.* Общие правила об обязательствах в Гражданском кодексе // Вестник ВАС РФ. 1995. № 9. С. 96.

[2] См.: постановление Конституционного Суда РФ от 23 февраля 1999 г. № 4-П «По делу о проверке конституционности положения части второй статьи 29 Федерального закона от 3 февраля 1996 г. «О банках и банковской деятельности» в связи с жалобами граждан О.Ю. Веселяшкиной, А.Ю. Веселяшкина и Н.П. Лазоренко» // Вестник Конституционного Суда РФ. 1999. № 3.

[3] Согласно ч. 2 ст. 29 Закона о банках и банковской деятельности кредитная организация не имеет права в одностороннем порядке изменять процентные ставки по кредитам, вкладам (депозитам), комиссионное вознаграждение и сроки действия этих договоров с клиентами, за исключением случаев, предусмотренных федеральным законом или договором с клиентом. В ст. 838 ГК РФ прямо установлено, что размер процентной ставки по договору срочного банковского вклада с гражданином не может быть односторонне уменьшен банком, если иное не предусмотрено законом. Таким

ковской деятельности) *применяться не может*. Иное его истолкование правоприменителем не согласуется с Конституцией РФ».

Изложенная позиция может иметь непосредственно значение с точки зрения толкования гражданско-правовых норм. Как отмечается, правовые позиции, высказанные в решениях Конституционного Суда РФ, носят общеобязательный характер: «императивность правовых позиций предопределяется тем, что в силу ст. 6 Закона о Конституционном Суде общеобязательным является решение Конституционного Суда РФ в целом, а не только его резолютивная часть. Закрепление правовых позиций как нормативно-интерпретационных установлений в решениях Конституционного Суда РФ в единстве с нормативными предписаниями резолютивной части и придает этим решениям качество не индивидуального, правоприменительного, а нормативно-интерпретационного акта»[1].

Формальное толкование положений ст. 310 ГК РФ с учетом разъяснений Конституционного Суда РФ и экономического неравенства, существующего в потребительских договорах, приводит к выводу о том, что наиболее корректным является следующий вариант.

3. Отдать приоритет положениям ст. 310 ГК РФ и признать недопустимым одностороннее изменение условий договора с участием потребителя в отсутствие оснований, указанных в законе[2]. Данный подход в большинстве своем и разделяется отечественной судебной практикой. В одном из решений прямо указано, что «только законом, а не договором определяется возможность изменения банками в одностороннем порядке условий договора для гражданина-потребителя... одностороннее изменение условий договора возможно

образом, ГК РФ в отличие от ч. 2 ст. 29 Закона о банках и банковской деятельности не допускает включения в договор срочного банковского вклада с гражданином условия о возможности одностороннего изменения банком процентных ставок в случаях, когда это предусмотрено только договором. Между тем на практике при наличии указанной коллизии норм продолжалось применение оспариваемого положения ч. 2 ст. 29 Закона о банках и банковской деятельности, которое толковалось банками в качестве закона, который устанавливает «иное» по сравнению с положениями ст. 838 ГК РФ. Данный случай аналогичен рассматриваемой нами коллизии между ст. 310 и п. 3 ст. 450 ГК РФ.

[1] *Лазарев Л.В.* Правовые позиции Конституционного Суда России. М., 2003. С. 75; *Гаджиев Г.А.* Ratio decidendi в постановлениях Конституционного Суда России // Конституционное правосудие. Вестник конференции органов конституционного контроля стран молодой демократии. Вып. 2(4). Ереван, 1999. С. 7.

[2] Постановления ФАС Поволжского округа от 6 декабря 2010 г. по делу № А12-10892/2010; Пятнадцатого арбитражного апелляционного суда от 22 июля 2013 г. № 15АП-8131/2013 по делу № А53-36813/2012; Первого арбитражного апелляционного суда от 22 июля 2013 г. по делу № А43-5251/2013.

только в случае заключения между банком и гражданином, не являющимся предпринимателем, соответствующего дополнительного соглашения»[1].

Таким образом, указание в договоре с потребителем права коммерческой организации в одностороннем порядке об изменении его условия будет противоречить ст. 310 ГК РФ и являться ничтожным условием в соответствии с п. 1 ст. 16 Закона РФ о защите прав потребителей, запрещающим ухудшение положения потребителя по сравнению с правилами, установленными законами или иными правовыми актами Российской Федерации. В связи с этим вопрос о допустимости одностороннего изменения условий договора путем публикации таких изменений на веб-сайте без уведомления о таких изменениях потребителя в большинстве случаев отпадает сам собой: такие изменения не будут иметь юридической силы, если только сам закон не санкционирует такое изменение.

Данный вывод был поддержан судами в ряде споров с участием операторов связи, которые нередко используют практику одностороннего изменения тарифов и иных условий договора на оказание услуг связи абоненту-потребителю.

В одном из решений уведомление потребителя об изменениях путем размещения их на официальном сайте оператора связи было прямо признано не соответствующим законодательству[2]. Размещение информации в сети Интернет на официальном сайте компании не позволяет, по мнению судов, «безусловным образом довести до абонента информацию, отвечающую требованиям необходимости, достоверности, наглядности, доступности и, следовательно, обеспечить надлежащее волеизъявление абонента в отношении адресованного ему оператором предложения (изменений)»[3]. Молчание потребителя (отсутствие поступивших возражений или отказа от договора с его стороны в течение определенного периода времени) не может приравниваться к согласию с изменениями, так как молчание не является конклюдентным действием[4].

---

[1] Постановление Седьмого арбитражного апелляционного суда от 23 января 2013 г. по делу № А27-13416/2012. См. также: постановление Четырнадцатого арбитражного апелляционного суда от 14 мая 2013 г. по делу № А13-12661/2012.

[2] Постановление ФАС Волго-Вятского округа от 8 февраля 2011 г. по делу № А28-14037/2009.

[3] Постановления: ФАС Волго-Вятского округа от 8 февраля 2011 г. по делу № А28-14037/2009; ФАС Дальневосточного округа от 7 февраля 2012 г. № Ф03-6661/2011.

[4] Постановление ФАС Волго-Вятского округа от 8 февраля 2011 г. по делу № А28-14037/2009.

Таким образом, с точки зрения российского права одностороннее изменение договора с участием потребителя возможно при соблюдении следующих условий:

1) наличие в законе или подзаконном акте, принятие которого санкционировано законом, права коммерческой организации (индивидуального предпринимателя) на изменение определенного условия договора в одностороннем порядке;

2) надлежащее доведение произведенных изменений до сведения потребителя. Простое размещение их на официальном веб-сайте компании является недостаточным. Необходимо *адресное* уведомление о таком изменении.

Указанные положения российского законодательства нельзя обойти путем выбора в качестве применимого иностранного права, которое более гибко подходит к вопросам допустимости одностороннего изменения условий договора. Как отмечалось ранее, ст. 1212 ГК РФ хотя и допускает возможность выбора применимого права к потребительскому договору, осложненному иностранным элементом, но такой выбор «не может повлечь за собой лишение такого физического лица (потребителя) защиты его прав, предоставляемой императивными нормами права страны места жительства потребителя», если заключению договора предшествовала оферта или реклама, доступные в России, и действия потребителя по заключению договора были совершены также в России. Несмотря на то что интерпретация существующих формулировок ст. 1212 ГК РФ в контексте электронной коммерции может столкнуться с затруднениями, о которых уже говорилось ранее, есть основания полагать, что среднестатистический российский суд не будет вдаваться в доктринальные дебри и применит данные положения к онлайн-договорам с участием потребителя. Поэтому применение иностранного права к договору не может предоставить надежную защиту от нежелательных положений российского потребительского законодательства.

Как видно, российское законодательство является достаточно жестким в вопросах одностороннего изменения условий договора с потребителем, причем суды достаточно последовательно приводят его в жизнь. Тем не менее многие типовые договоры на оказание услуг связи, банковские договоры и иные договоры, которые фактически заключаются по модели договора присоединения, все же содержат подобные условия. В чем причина данного парадокса? Представляется, что основной причиной является тот факт, что в существующих условиях включение таких условий в договор не несет в себе рисков,

которые превышают возможную выгоду от их включения. В подавляющем большинстве случаев потребитель не пойдет в суд оспаривать произведенное в одностороннем порядке изменение договора в силу различных причин (незнание своих прав, нежелание связываться с российскими судами общей юрисдикции, незначительная «цена вопроса» по сравнению с возможными временны́ми и материальными затратами на такое оспаривание, нежелание ссориться с контрагентом и пр.). Таким образом, в большинстве случаев такие условия будут восприняты потребителями как своего рода «неизбежное зло», и тем самым их реализация коммерческой организацией сможет привести к желаемому правовому эффекту: взаимоотношения сторон будут регулироваться по-новому. Существующие же публично-правовые механизмы, которые по идее и должны выполнять основную превентивную роль, стимулируя экономически более сильную сторону к добросовестности при формулировании условий договора, не работают. Основным публично-правовым последствием включения в договор условий, ущемляющих права потребителя, является ч. 2 ст. 14.8 КоАП РФ, санкция которой предусматривает штраф в отношении юридических лиц в размере от 10 000 до 20 000 руб. Как видно, это далеко не самая большая «плата» за те преимущества, которые такие условия представляют собой для коммерческих организаций. В итоге получается ситуация, при которой одностороннее изменение условий договора с потребителем является формально запрещенным, но вполне реализуемым на практике с незначительными издержками.

Справедливости ради надо отметить, что нередко возможно достигнуть того же результата, что и посредством одностороннего изменения договора, и без нарушения закона. Просто необходимо несколько изменить структуру возникающих в связи с этим отношений и их квалификацию. Одностороннее изменение характеризуется возможностью изменения условий ранее заключенного договора без согласия другой стороны. В связи с этим оно может быть охарактеризовано как односторонняя сделка. В то же время зачастую ничто не мешает заключить новое соглашение, на новых условиях. В таком случае будет иметь место уже изменение договора по соглашению сторон, а к данным случаям рассмотренные ранее ограничения ст. 310 ГК РФ и законодательства о защите прав потребителей не применяются. В связи с этим в случаях, когда речь идет о предоставлении некоего онлайн-сервиса, условия которого регламентируются предварительно принятым *click-wrap*-соглашением, ничто не препятствует «попросить» пользователя принять такое соглашение еще раз, когда в нем появятся изменения.

Данный подход позволяет уйти от скользких вопросов, связанных с допустимостью односторонних изменений условий договора и порядком доведения таких изменений до сведения другой стороны. Однако сфера возможного применения данного подхода ограничена онлайн-сервисами длящегося характера.

В остальных случаях можно предусмотреть в договоре с потребителем положения приблизительно следующего содержания: «Изменение договора оформляется путем заключения дополнительного соглашения в письменной форме либо путем совершения абонентом конклюдентных действий в виде [*указать перечень таких действий, например производство оплаты услуги, продолжение пользования сервисом и пр.*]». В таком случае речь идет не об одностороннем изменении условия договора, а об изменении договора по обоюдному согласию, которое выражается со стороны потребителя в виде определенных действий, указанных в договоре, что вполне укладывается в положения п. 3 ст. 434 и п. 3 ст. 438 ГК РФ. Единственное ограничение, которое отличает данный подход от механизма одностороннего изменения условий договора, заключается в том, что в данном случае необходимо совершение определенного действия со стороны потребителя, выражающего его волю. Одного только уведомления о произведенных изменениях недостаточно для того, чтобы они приобрели силу[1]. Молчание потребителя в виде отсутствия каких-либо возражений на изменения не может расцениваться как такое действие, необходимо совершение положительных действий с его стороны, которые могли бы быть квалифицированы в качестве выполнения условий договора на новых условиях.

Таким образом, существует два варианта легитимного изменения условий договора с потребителем:

наличие основания для изменения такого условия в законодательстве → уведомление потребителя о таком изменении в порядке, предусмотренном в соответствующем нормативном правовом акте и договоре;

указание в первоначальном договоре возможности его изменения и порядка выражения согласия потребителем с такими изменениями (конкретизация возможных конклюдентных действий) → направление потребителю уведомления-оферты на изменение условий договора (по сути – на заключение нового договора) → совершение потребителем действий, свидетельствующих об акцепте оферты.

[1] Постановление Второго арбитражного апелляционного суда от 31 января 2012 г. по делу № А28-8512/2011.

Как видно, существуют способы достижения бизнес-цели (внесение изменений в ранее заключенные договоры) и без формального нарушения законодательства. Правда, для полноты картины необходимо отметить, что в последнем варианте существует риск возможного признания подобного рода схемы обходом закона (ст. 10 ГК РФ). В таком случае в защите права коммерческой организации на инициирование изменений условий договора будет отказано, а к отношениям сторон будут применяться нормы законодательства «по умолчанию». Насколько данный риск является серьезным, следует анализировать в каждом конкретном случае отдельно, в том числе с учетом возможных последствий привлечения к административной ответственности, о которых говорилось выше.

Посмотрим, как решается вопрос о допустимости и об условиях одностороннего изменения договора, заключенного между предпринимателями. Здесь у сторон гораздо больше гибкости по сравнению с потребительскими договорами. Во-первых, ст. 310 и п. 3 ст. 450 ГК РФ прямо допускают возможность установления оснований для одностороннего изменения условий предпринимательского договора не только в законе, но и в договоре. Во-вторых, здесь отсутствуют специальные ограничения, подобные ст. 1212 ГК РФ и связанные с выбором применимого права к договору, осложненному иностранным элементом.

С другой стороны, возникает другая проблема: содержит ли российское право какие-либо ограничения, касающиеся пределов реализации управомоченным лицом, своего права на одностороннее изменение договора[1]. Нетрудно представить себе ситуацию, при которой в результате реализации такого права первоначальный договор может видоизмениться до степени полной неузнаваемости.

К сожалению, российское право не содержит детального регулирования вопросов, связанных с использованием стандартных условий и обеспечением их добросовестности и справедливости, как это имеет место быть в некоторых странах[2]. В связи с этим возможные меры защиты от недобросовестного изменения условий в одностороннем порядке носят фрагментарный характер.

Так, поскольку большинство договоров, заключаемых в сети Интернет, могут быть квалифицированы в качестве договора присоеди-

[1] Разумеется, здесь речь идет именно о специальных ограничениях, а не об общих – вроде императивных норм законодательства, которые уже в силу своего характера не допускают изменения определенных положений, составляющих правовой режим договора.

[2] Например, в Германии (см.: Gesetz zur Regelung des Rechts der Allgemeinen Geschaftsbedingungen 1976 г. (в настоящее время данный закон инкорпорирован в ГГУ в § 305–310)), Голландии (Гражданский кодекс Нидерландов 6:231–6:243) и т.п.

нения (*click-wrap-* и *browse-wrap-*соглашения относятся к ним в силу используемого характера механизма заключения договора), существует потенциальная возможность применения механизма ст. 428 ГК РФ. Данная статья предусматривает возможность изменения или расторжения договора в случае, если его условия являются чрезмерно обременительными для другой стороны и она не приняла бы их, если бы имела возможность влиять на условия договора. Правда, существенным недостатком данного механизма является то, что он не предусматривает возможность признания такого условия недействительным. Как следствие, сложно «отменить» действие обременительного условия задним числом. Относительно такого условия, как право на одностороннее изменение договора, применять ст. 428 ГК РФ для противодействия недобросовестному его использованию проблематично в том числе и потому, что чрезмерно обременительным является не столько это условие само по себе, сколько его реализация, выразившаяся в новых условиях. При этом такие новые условия могут и не быть сами по себе чрезмерно обременительными: такая обременительность возникает из совокупности факторов – наличия в договоре права на одностороннее его изменение, не ограниченное какими-либо пределами; последующая реализация данного права, которая вылилась в существенное изменение его условий; новые условия не отражают ожиданий присоединившейся стороны, которые имели место на момент заключения договора. При таких обстоятельствах, которые не укладываются в полной мере в диспозицию п. 2 ст. 428 ГК РФ, применять ее в качестве средства противодействия недобросовестным изменениям договорных условий достаточно проблематично, даже несмотря на то, что ее использование в рамках предпринимательских отношений было санкционировано ВАС РФ[1].

[1] ВАС РФ указал, что поскольку у предпринимателя отсутствовала фактическая возможность влиять на содержание условий договора, поэтому он принял его условия путем присоединения к предложенному договору в целом, в том числе с учетом оспариваемых условий. Следовательно, к спорному договору могут быть по аналогии закона (ст. 6 ГК РФ) применены положения п. 2 ст. 428 ГК РФ. При этом тот факт, что в договоре имелись и условия, согласованные сторонами индивидуально, не препятствует применению п. 2 ст. 428 ГК РФ к тем положениям договора, в отношении которых заемщик был вынужден принимать навязанные ему условия. См.: п. 2 информационного письма Президиума ВАС РФ от 13 сентября 2011 г. № 147 «Обзор судебной практики разрешения споров, связанных с применением положений Гражданского кодекса Российской Федерации о кредитном договоре». Таким образом, ВАС РФ фактически лишил силы положение п. 3 ст. 428 ГК РФ, которое долгое время сдерживало возможность применения положений о договоре присоединения к предпринимательским договорам.

Более эффективной может оказаться ст. 10 ГК РФ, содержащая общий принцип недопустимости злоупотребления правом. В том случае, когда сторона договора, обладающая формально неограниченным правом на его одностороннее изменение, изменяет его без каких-либо обоснованных причин в ущерб своему контрагенту, можно говорить о злоупотреблении правом. В качестве общего последствия признания какого-либо действия злоупотреблением правом закон предусматривает отказ в защите такого права. К примеру, если провайдер какого-либо сервиса в сети Интернет, воспользовавшись своим правом на одностороннее изменение условий договора в любой момент, впоследствии обратится в суд со ссылкой на измененные условия, суд может отказать такому провайдеру в защите права. Долгое время ни закон, ни судебная практика не признавали иных последствий злоупотребления права. Однако с некоторых пор у участников оборота появилась возможность выступить в качестве активной стороны при пресечении злоупотреблений правом. По мнению ВАС РФ, злоупотребление правом может являться основанием для признание договора или его части недействительным, как противоречащего закону (ст. 10, 168 ГК РФ)[1]. Данное разъяснение открывает возможность для признания условия о неограниченном праве на одностороннее изменение договора недействительным, а вместе с ним – и все произведенные на его основе изменения.

Представляется, что положения ст. 10 ГК РФ могут рассматриваться в качестве сверхимперативной нормы, которая может быть применена российским судом безотносительно к положениям применимого права. Напротив, ст. 428 ГК РФ является составной частью договорного статута и может применяться, лишь если в качестве применимого права выступает российское. Если применимым выступает иностранное право, то механизмы контроля над справедливостью и добросовестностью договорных условий должны определяться в соответствии с ним.

Определив, что российское законодательство содержит определенные ограничители свободы реализации одной из сторон договора своего права на его одностороннее изменение, необходимо коснуться вопроса реализации данного права. А именно: насколько включение в предпринимательский договор условия о том, что контрагент извещается о произведенных изменениях на официальном веб-сайте организации, соответствует канонам договорного права.

[1] См.: п. 9 информационного письма Президиума ВАС РФ от 25 ноября 2008 г. № 127 «Обзор практики применения арбитражными судами статьи 10 Гражданского кодекса Российской Федерации».

В зарубежной практике суды также, как правило, признают действительными изменения, сделанные путем размещения их на веб-сайте при возложении договором на другую сторону обязанности периодического посещения веб-сайта для проверки наличия таких изменений, если оба участника являются профессионалами в соответствующей сфере[1].

Представляется, и в рамках российской правовой системы нет веских оснований считать недействительными подобные условия. Как известно, одним из принципов договорного права, в том числе и российского, является принцип свободы договора, допускающий возможность сторон определить условия договора по своему усмотрению, за исключением случаев, предусмотренных законом или иным правовым актом. ГК РФ не содержит запрета на включение условия об уведомлении контрагента о произведенных изменениях в условиях договора путем публикации их на веб-сайте, а равно как и его обязанности периодически проверять сайт на предмет наличия изменений. Таким образом, вроде бы формальные препятствия к реализации подобного рода механизма внесения изменений в предпринимательский договор отсутствуют. Анализ отдельных судебных решений позволяет сделать вывод о том, что суды в целом лояльно относятся не только к факту изложения отдельных договорных документов на веб-сайте, но и к возможности его изменения в одностороннем порядке с размещением на том же веб-сайте обновленной версии[2].

Таким образом, договоры между предпринимателями допускают достаточно много свободы в плане определения оснований для их одностороннего изменения, а также порядка реализации данного права, что позволяет легитимировать многие существующие в сфере электронной коммерции бизнес-практики. Другое дело, что подобного рода свобода должна быть компенсирована эффективным механизмом, направленным на предотвращение возможных злоупотреблений со стороны экономически более сильных контрагентов. Пока такие механизмы в России представлены преимущественно в виде норм о договоре присоединения (ст. 428 ГК РФ) и о злоупотреблении правом (ст. 10 ГК РФ) и находятся в относительно зачаточном состоянии,

[1] См., например: Margae, Inc. v. Clear Link Technologies, LLC. No. 2:07-CV-00916-TC, 2008 (D. Utah June 16, 2008); *Moringiello J., Reynolds W.* Electronic contracting Cases 2008-2009 // The Business Lawyer. No 65. 2009. P. 318–320. В отношениях с участием потребителей американские суды пока демонстрируют нежелание признавать действительность подобного рода условий. Douglas v. United States District Court for the Central District of California, 495 F3d 1062 (9th Cir. 2007).

[2] Постановление ФАС Московского округа от 31 декабря 2009 г. № КГ-А40/13774-09.

однако есть все основания полагать, что в ближайшем будущем эмпирическая нагрузка на них существенно возрастет во многом благодаря электронной коммерции.

Все, что было ранее сказано относительно одностороннего изменения условий договора *mutatis mutandis*, применимо и к определению оснований для одностороннего расторжения договора. Статья 310 и п. 3 ст. 450 ГК РФ в равной степени применимы и к одностороннему отказу от договора со всеми вытекающими ограничениями для потребительских договоров, а также свободой договора для предпринимательских договоров. Здесь хотелось бы коснуться одного вопроса, связанного с практикой прекращения договора, нередко встречающейся в сфере электронной коммерции. Речь идет об условиях *click-wrap-* и *browse-wrap*-соглашений, которые предусматривают его автоматическое прекращение в случае нарушения его условий пользователем. Подобного рода условия являются типичными для многих лицензионных соглашений на программное обеспечение, а также онлайн-сервисов. Насколько такие условия являются легитимными с точки зрения положений договорного права?

Закон (п. 3 ст. 450 ГК РФ) лишь указывает на возможность одностороннего отказа от исполнения договора, но не предусматривает процедуру осуществления такого способа расторжения. В большинстве стран мира такой отказ осуществляется путем направления должнику уведомления о расторжении, получение которого должником приводит к прекращению договорных обязательств[1].

На практике данный подход используется и в России. В качестве обоснования применяется ряд положений. Во-первых, применение по аналогии закона нормы из положений о договоре поставки, предусматривающих, что односторонний отказ от исполнения договора поставки приобретает юридическую силу с момента получения соответствующего уведомления должником, если иной срок расторжения не предусмотрен в уведомлении либо не определен в договоре (п. 4 ст. 523 ГК РФ). Во-вторых, применение к отношениям по одностороннему расторжению договора по аналогии положений ст. 452 ГК РФ, согласно которой оформление соглашения о расторжении договора должно производиться в той же форме, что и основной договор. Из этого делается вывод о том, что если договор был заключен в письменной форме, то и отказ от него должен совершаться в письменной форме и доводиться соответствующим образом до должника. Отечественная

[1] Подробный обзор см.: *Карапетов А.Г.* Расторжение нарушенного договора в российском и зарубежном праве.

судебная практика также исходит из того, что односторонний отказ от договора представляет собой сделку, требующую восприятия другой стороной для порождения правового эффекта[1]. В доктрине данный подход разделяется практически единодушно[2]. Более того, проект изменений в ГК РФ содержит ряд положений, конкретизирующих порядок реализации права на односторонний отказ от договора, одно из которых прямо предусматривает необходимость доведения до сведения контрагента уведомления об одностороннем отказе от договора. Таким образом, реализация права на одностороннее расторжение договора при применимом российском праве (п. 5 ст. 1215 ГК РФ) должна осуществляться посредством уведомления другой стороны о таком расторжении, в отсутствие которого договор будет считаться действующим.

Возникает вопрос, можно ли использовать какие-либо альтернативные конструкции, позволяющие обеспечить возможность прекращения договора в случае его нарушения другой стороной, без уведомления такой стороны? Представляется, что в качестве таковой мог бы быть использован п. 2 ст. 157 ГК РФ о сделках, совершенных под отлагательным условием. В соответствии с данными положениями сделка считается совершенной под отменительным условием, стороны могут поставить прекращение прав и обязанностей в зависимость от обстоятельства, относительно которого неизвестно, наступит оно или не наступит. По существу, именно это и имеется в виду в рассматриваемой ситуации: договор считается прекратившим свое действие при его нарушении одной из сторон. Проблема в применении п. 2 ст. 157 ГК РФ заключается в существующем в российской доктрине и судебной практике представлении о недопустимости использования в условных сделках так называемых потестативных условий, т.е. условий, наступление которых зависит от действий или бездействия одной из сторон[3]. Вместе с тем из ст. 157 ГК РФ этот запрет прямо не вытекает. Данная статья устанавливает, что отлагательное или отменительное

[1] Постановление Президиума ВАС РФ от 11 июня 2002 г. № 6746/01.

[2] См.: *Витрянский В.В.* Указ. соч.; *Карапетов А.Г.* Расторжение нарушенного договора в российском и зарубежном праве; *Егорова М.А.* Односторонний отказ от исполнения гражданско-правового договора. 2-е изд., перераб. и доп. М., 2010; *Соменков С.А.* Указ. соч. С. 43.

[3] Подробнее о данной проблеме см.: *Карапетов А.Г.* Зависимость условия от воли сторон условной сделки в контексте реформы гражданского права // Вестник ВАС РФ. 2009. № 7. С. 28–94. Обзор судебной практики по этому вопросу см.: *Бабаев А.Б., Бевзенко Р.С., Белов В.А., Тарасенко Ю.А.* Практика применения Гражданского кодекса Российской Федерации, части первой / под общ. ред. В.А. Белова. М., 2008. С. 254–261.

условие в условной сделке должно касаться события, которое не должно наступить неизбежно. Но эта статья ничего не говорит о возможности или невозможности указывать в качестве условия обстоятельства, наступление которых зависит от одной из сторон договора. При буквальном прочтении закона никаких оснований вывести из требования о неизвестности факта наступления условия в будущем жесткий запрет на условия, зависящие от действий одной из сторон, не усматривается. Когда заключается условная сделка с потестативным условием, никто не может точно знать, что соответствующее условие наступит, и даже если точно знает, то вряд ли можно признать нормальной ситуацию, при которой лицо заключает договор заведомо с намерением его нарушить. Допуская возможность существования подобных ситуаций на практике, следует признать, что право не должно предоставлять таким лицам преимуществ в виде признания соответствующих механизмов, направленных на защиту интересов кредитора, недействительными по причине несоответствия их догматическим конструкциям, выработанным в тиши профессорских кабинетов.

Примечательно, что отечественные суды нередко отказываются следовать навязанной доктриной подмене понятия «отсутствие неизбежности» независимостью от воли одной из сторон. На практике встречается немало споров, в которых суды допускали прекращение договора на основании наступления отменительного условия, предусмотренного в таком договоре, в том числе когда в качестве такового фигурировал факт неисполнения должником своих обязательств по такому договору[1]. В одном из решений прямо указано, что «из содержания ст. 157 ГК РФ не усматривается, что отменительным условием может быть только обстоятельство, которое не зависит от воли

[1] См., например: постановление Одиннадцатого арбитражного апелляционного суда от 18 февраля 2013 г. по делу № А65-24014/2012 («Согласно представленному соглашению был определен другой порядок погашения задолженности, однако при однократном нарушении должником графика погашения задолженности в силу п. 2 ст. 157 ГК РФ отменяется действие указанного соглашения в части непогашенной суммы долга, при этом кредитор имеет право на взыскание неоплаченной части задолженности и санкций за несвоевременное исполнение обязательств на основании действующих договоров на условиях, существовавших до заключения соглашения»); постановление Десятого арбитражного апелляционного суда от 4 апреля 2013 г. по делу № А41-53037/12 («неосуществление платежа в сумме и сроки, указанные в ст. 3, представляет собой отменительное условие... Наступление такого условия влечет прекращение прав и обязанностей сторон, возникших из договора, а именно: договор считается расторгнутым, все обязательства сторон прекращаются, и продавец освобождается от исполнения своих обязательств по передаче объекта»). См. также постановления ФАС Московского округа от 28 мая 2007 г., 4 июня 2007 г. № КГ-А40/4055-07-П; Седьмого арбитражного апелляционного суда от 15 марта 2010 г. № 07АП-516/2010 по делу № А45-24348/2009.

сторон», и признано допустимым включение в договор отменительного условия в виде несоблюдения предусмотренного договором графика выполнения работ[1].

Таким образом, российское право и отдельные суды допускают возможность автоматического прекращения договора при наступлении определенных в нем обстоятельств без уведомления должника о таком прекращении. Подобные условия должны толковаться по правилам ст. 431 ГК РФ как отменительное условие. Конечно, существует немалый риск признания установленного в договоре отменительного условия в виде нарушения договора другой стороной в качестве потестативного и недействительного. И хотя в настоящее время имеется судебная практика, которая более разумно подходит к данному вопросу, данный риск может быть в значительной степени минимизирован лишь подчинением договора иностранному праву, более адекватно подходящему к вопросам прекращения действия договора.

[1] Постановление ФАС Восточно-Сибирского округа от 13 ноября 2010 г. по делу № А10-132/2010 (Определением ВАС РФ от 25 апреля 2011 г. № ВАС-2293/11 отказано в передаче дела № А10-132/2010 в Президиум ВАС РФ для пересмотра в порядке надзора). См. также: постановление ФАС Восточно-Сибирского округа от 29 ноября 2010 г. по делу № А10-140/2010.

Глава 4. Процессуальные аспекты электронной коммерции

§ 1. Общие замечания

Ранее уже отмечалось подозрительное отношение отечественных государственных органов к электронным документам, которое бросает самою большую тень на развитие электронной коммерции. В значительной степени такой подход предопределяется распространенным убеждением о том, что электронные доказательства легче подделать, нежели классические бумажные документы, и уж тем более вещественные доказательства[1]. Другой причиной подобного подхода, неразрывно связанной с первой, является сложность идентификации субъекта, от которого исходит тот или иной документ. В ряде случаев возможно определить техническое устройство, с которого оно было отправлено, но персонифицировать источник достаточно проблематично. Наконец, далеко не все государственные органы оборудованы необходимыми техническими средствами, а их сотрудники – необходимыми техническими навыками для эффективной работы с электронными документами. Государственные органы переполнены людьми, компьютерная грамотность которых находится на уровне ниже «прожиточного минимума», в связи с чем неудивительно, что бумага с подписью и печатью воспринимается как полноценное доказательство, а все остальное – с повышенным подозрением.

В защиту отечественных судов следует сказать, что даже либеральным американским судам были близки аналогичные воззрения. Одним из наиболее показательных является дело *St. Clair v. Johnny's Oyster & Shrimp*, *Inc.*, в котором судья заявил буквально следующее: «В то время как некоторые смотрят на Интернет как на инновационный способ коммуникаций, Суд продолжает рассматривать его как один большой источник слухов, инсинуаций и дезинформации... Любое лицо может выложить в Интернет все что угодно. Ни один веб-сайт не мониторится на предмет достоверности информации, и ничто содержащееся там

[1] *Smith G.* Internet Law & Regulation. Sweet & Maxwell. London. 4th ed. 2007. P. 872.

не выкладывается под присягой или подлежит независимой верификации. Кроме того, суд не имеет иллюзий относительно того, что хакеры не способны изменить содержимое веб-сайта из любой точки мира в любое время. В силу этих причин любое доказательство, полученное из сети Интернет, равнозначно ничему стоящему... Вместо того чтобы опираться на шаманскую информацию (в оригинале: *«voodoo information». – А.С.*) из Интернета, истец должен был охотиться на доказательства в бумажной форме, отвечающей требованиям допустимости».

В целом недоверие судов к доказательствам, основанным на новых технологиях, является достаточно типичным явлением. В тех же США сначала отказывались принимать в качестве доказательств фотографии[1], впоследствии – звукозаписи[2] и видеозаписи[3]. По мере того как бывшие когда-то новыми технологии становились привычными, суды становились более лояльными к основанным на них доказательствам и ослабляли первоначально жесткие требования к их допустимости[4].

Так или иначе, вышеуказанные проблемы приводят к тому, что некоторые договоры, которые с материально-правовой точки зрения можно рассматривать как заключенные и действительные, воспринимаются правоприменительными органами «в штыки» и оставляются без исковой защиты. Если воспользоваться замечанием Р. Иеринга о том, что право, не обеспеченное исковой силой, есть «свет, который не светит»[5], то подавляющее большинство участников оборота, находящихся под властью российского права и судебной юрисдикции, бродят

[1] Cunningham v. Fair Haven & Westvill R. Co., 43 A. 1047, 1049 (Conn. 1899). В качестве обоснования суд высказал опасение, что «либо в силу недостатка навыков фотографа, либо ненадлежащих инструментов или материалов, либо в силу намеренной и искусной манипуляции фотография может быть не только неточной, но и вводящей в заблуждение».

[2] State v. Simon, 174 A. 867, 872 (N.J. Sup. Ct. 1934). Суд подошел к вопросу допустимости звукозаписи достаточно формально и указал, что ему «не известно ни одного решения, ни одного авторитетного комментария, в которых бы звукозапись предполагаемого разговора была бы признана судом в качестве допустимого доказательства».

[3] *Gruber J.* Electronic Evidence. West Group: A Thomson Company. 1995. § 8.1 «Видеозаписи первоначально были достаточно враждебно восприняты судом, поскольку, по мнению судов, они предоставляли большой простор для искажений, фабрикаций и фальсификаций».

[4] Так, в момент, когда электронные доказательства только-только появились, суды США требовали помимо обеспечения их соответствия общим требованиям к доказательствам указание первоначального источника компьютерной программы, с использованием которой они были получены, процедур, в соответствии с которыми информация вводилась, а также результаты тестов, подтверждающих точность и надежность электронных устройств. См.: *Goode S.* The Admissibility of Electronic Evidences // Review of Litigation. No 29. 2010. P. 5.

[5] *Иеринг Р.* Цель в праве // Избранные труды. СПб., 2006. Т. I. С. 292.

в потемках. Так или иначе, электронная коммерция развивается, в том числе и в России, что свидетельствует о том, что между процессуальными и материально-правовыми проблемами электронных договоров нет неизбежной корреляции. В ряде случаев стороны просто не пойдут в суд, но для эффективного взаимодействия им необходимо наличие уверенности в том, что они состоят в договорных отношениях. В отношениях, регулируемых гражданским правом, стороны могут широко использовать для защиты своих прав и средства негосударственного принуждения (технические средства защиты, внесение в «черный список», придание огласке недобросовестного поведения другой стороны, что может иметь гораздо более сильное дисциплинирующее воздействие, чем судебное преследование, особенно на рынках с небольшим количеством игроков). Поэтому нельзя согласиться с позицией многих ортодоксальных юристов, согласно которой невозможность использования электронного документа в качестве доказательства в российском суде влечет недействительность заключенных с использованием таких документов договоров. В конце концов, помимо российских судов существуют зарубежные суды, чья юрисдикция в отношении отношений, возникающих в сети Интернет, имеет тенденцию к расширению. Существует еще и арбитраж, который весьма либерально подходит к вопросам допустимости доказательств.

Тем не менее, поскольку некоторые договоры, заключаемые в электронной форме, все же придется отстаивать в российских судах, необходимо рассмотреть существующие процессуальные правила, регламентирующие вопросы допустимости доказательств, а также сложившуюся практику их применения.

Доказательствами в арбитражном процессе являются полученные в установленном АПК РФ и другими федеральными законами порядке сведения о фактах, на основании которых арбитражный суд устанавливает наличие или отсутствие обстоятельств, обосновывающих требования или возражения сторон, а также иные обстоятельства, имеющие значение для правильного разрешения спора (ст. 64 АПК РФ). В качестве доказательств допускаются письменные и вещественные доказательства, объяснения лиц, участвующих в деле, заключения экспертов, показания свидетелей, аудио-, видеозаписи, иные документы и материалы.

Буквальное содержание текста ст. 64 АПК РФ свидетельствует о том, что законодатель весьма свободно трактует понятие процессуальный формы и оставляет перечень средств доказывания, которые можно использовать для установления фактических обстоятельств дела, от-

крытым, допуская возможность привлечения в процесс доказывания «иных документов и материалов». Следовательно, формально возможно использование любых источников, в отношении которых законом не устанавливается процессуальный порядок получения информации, т.е. не определяется механизм обеспечения достоверности получаемой информации[1].

Несмотря на то что ст. 55 ГПК РФ содержит сходное с АПК РФ определение доказательства, подход к возможным средствам доказывания несколько иной: абз. 2 ст. 55 ГПК РФ содержит закрытый перечень средств доказывания: соответствующие сведения могут быть получены из объяснений сторон и третьих лиц, показаний свидетелей, письменных и вещественных доказательств, аудио- и видеозаписей, заключений экспертов. Указание на иные документы и материалы отсутствует. Неудовлетворительность данного подхода отмечалась в литературе[2].

Возникает вопрос: к какой категории доказательств относятся электронные сообщения, обмен которыми был осуществлен посредством сети Интернет, а также различного рода сведения, которые содержатся на веб-сайтах?

Как следует из положений п. 1 ст. 71 ГПК РФ и п. 3 ст. 75 АПК РФ документы и материалы в цифровой форме, полученные посредством электронной связи, относятся к категории письменных доказательств. Как известно, характерной чертой письменных доказательств, отличающей их от вещественных доказательств, является тот факт, что в первом случае доказательственное значение имеют сведения, воспринимаемые из содержания письменных знаков, а во втором – доказательственное значение имеют свойства, внешний вид или иные признаки предмета. Как отмечается, единственным требованием к письменным знакам любого вида является наличие у них в совокупности определенной мысли, составляющей содержание документа. Это могут быть не только средства письменной речи, но и цифры, нотные знаки и любые другие условные знаки[3]. Электронные документы и сведения с веб-сайтов вполне подпадают под понятие письменного доказательства, поскольку их основная ценность заключается в их содержании.

---

[1] См.: Арбитражный процесс: учебник для студентов юридических вузов и факультетов / под ред. М.К. Треушникова. 3-е изд., испр. и доп. М., 2007.

[2] *Исаенкова О.В.* Некоторые проблемы доказательств и формы их представления в гражданском судопроизводстве // Налоги. 2009. № 17.

[3] См.: *Боннер А.Т.* Традиционные и нетрадиционные средства доказывания в гражданском и арбитражном процессе. М., 2013. С. 113.

Правда, наличие у таких цифровых доказательств специфических черт приводит к выводам о том, что они являются письменными доказательствами особого рода[1].

В соответствии с нормами процессуального права основными признаками или свойствами судебных доказательств являются их относимость (ст. 67 АПК РФ, ст. 59 ГПК РФ) и допустимость (ст. 68 АПК РФ, ст. 60 ГПК РФ). Относимость доказательств – это органическая связь между содержанием фактических данных и обстоятельствами, подлежащими доказыванию по делу. Как определить, какое доказательство относимо? Для этого следует сначала определить, имеют ли значение для дела факты, для установления которых предлагается доказательство, а затем – может ли доказательство подтвердить или опровергнуть относимый к делу факт. При положительном ответе доказательство может считаться относимым[2].

Допустимость доказательств означает, что в предусмотренных законом случаях могут быть использованы только предписанные законом виды доказательств или, напротив, установлены запреты на использование в качестве доказательств определенных средств доказывания[3].

Применительно к письменным документам в электронной форме ГПК РФ и АПК РФ также предъявляются требования об их выполнении способом, позволяющим установить их достоверность (п. 1 ст. 71 ГПК РФ и п. 1 ст. 75 АПК РФ). Как известно, под достоверностью понимается такое качество доказательства, которое характеризует точность, правильность отражения обстоятельств, входящих в предмет доказывания. Достоверно то доказательство, которое содержит правдивую информацию о действительности. Впрочем, достоверность является общим требованием к любым доказательствам, а не только к электронным (п. 3 ст. 67 ГПК РФ, п. 2 ст. 71 АПК РФ). Достоверность доказательства проверяется при оценке всей совокупности доказательств, имеющихся по делу[4].

Рассмотрим, какие требования предъявляются к различным доказательствам в электронной форме, которые могут иметь значение в контексте электронной коммерции.

---

[1] Справочник по доказыванию в гражданском судопроизводстве / под ред. И.В. Решетниковой. 5-е изд., доп. и перераб. М., 2011. С. 45.

[2] Там же. С. 24.

[3] Практика применения Арбитражного процессуального кодекса Российской Федерации / отв. ред. И.В. Решетникова. 2-е изд., перераб. и доп. М., 2012.

[4] Гражданский процесс / под ред. В.В. Яркова. М., 2012. С. 223.

§ 2. Сообщения электронной почты (e-mail messages) как доказательства в гражданском и арбитражном процессе

Основными вопросами, которые могут возникнуть при использовании подобных сообщений в гражданском и арбитражном процессе, являются формальные условия допустимости такого сообщения как доказательства, факт отправки (получения) такого сообщения другой стороной, неизменность содержания такого сообщения.

АПК РФ содержит дополнительное требование к допустимости электронных доказательств: наличие специального санкционирующего их использование положения либо в нормах законодательства, либо в договоре, заключенном между сторонами. В соответствии с п. 3 ст. 75 АПК РФ документы, полученные посредством факсимильной, электронной или иной связи, в том числе с использованием информационно-телекоммуникационной сети Интернет, а также документы, подписанные электронной подписью или иным аналогом собственноручной подписи, допускаются в качестве письменных доказательств в случаях и в порядке, которые установлены АПК РФ, другими федеральными законами, иными нормативными правовыми актами или договором либо определены в пределах своих полномочий ВАС РФ.

Данная норма во многом повторяет материально-правовую норму ст. 160 ГК РФ об условиях допустимости электронной цифровой подписи и других аналогов собственноручной подписи: «Использование при совершении сделок факсимильного воспроизведения подписи с помощью средств механического или иного копирования, электронной подписи либо иного аналога собственноручной подписи допускается в случаях и в порядке, предусмотренных законом, иными правовыми актами или соглашением сторон».

В случаях, когда электронное сообщение, а точнее документ, отправленный средствами электронной почты контрагенту, подписан электронной цифровой подписью[1], такой документ представляется в суд в электронном виде на материальном носителе (например, на *CD*-, *DVD*-диске) и в распечатанном виде для приобщения к материалам дела.

Поскольку электронная цифровая подпись признается равнозначной собственноручной подписи лишь при определенных условиях[2],

[1] Под электронной цифровой подписью в данном случае имеется в виду электронная цифровая подпись по Закону об ЭЦП 2002 г. и усиленная квалифицированная подпись по Закону об ЭП 2011 г.

[2] См.: ст. 11 Закона об ЭП 2011 г.; ст. 4 Закона об ЭЦП 2002 г.

помимо собственно электронного документа необходимо предоставить доказательства, подтверждающие соблюдение таких условий.

Так, поскольку одним из таких условий является действительность сертификата подписи на момент подписания документа, то должен быть предоставлен сертификат ключа проверки электронной подписи[1]. Он также необходим для определения наличия каких-либо ограничений по сфере его действия и установления соответствия подписанного электронного документа таким ограничениям.

Другим условием юридической силы электронной цифровой подписи является положительный результат проверки действительности электронной цифровой подписи. Для подтверждения подлинности ЭЦП необходимо обратиться в удостоверяющий центр с заявлением, выдавший соответствующий сертификат, о представлении заключения о подлинности ЭЦП, в котором необходимо указать сведения о подписанте и сертификате ключа подписи, времени подписания документа, а также приложить сам документ, который подлежит проверке.

Наконец, поскольку закон предъявляет определенные требования к удостоверяющим центрам и используемым средствам электронной подписи, для подтверждения равнозначности электронной подписи собственноручной подписи необходимо, чтобы удостоверяющий центр также предоставил документы, подтверждающие его аккредитацию в установленном порядке, а также сертификаты соответствия используемых криптографических средств установленным требованиям.

Таким образом, в материалы дела, в котором фигурирует документ, подписанный электронной цифровой подписью, включается: 1) электронный документ на материальном носителе; 2) распечатка электронного документа, заверенная стороной; 3) заключение удостоверяющего центра о подтверждении подлинности ЭЦП в данном документе; 4) документы, подтверждающие аккредитацию удостоверяющего центра и сертификацию используемых им криптографических средств.

В случае возникновения сомнений в верности выводов удостоверяющего центра относительно подлинности ЭЦП на спорном документе по данному вопросу может быть назначена экспертиза.

В случае, когда договор был заключен в электронной форме с подписанием электронной цифровой подписью, но стороны не представляют его в процесс в электронной форме (например, по причине его

[1] См., например: постановление ФАС Волго-Вятского округа от 11 августа 2010 г. по делу № А43-5226/2010.

утраты), бумажная копия такого договора должна содержать сведения о проверке и подтверждении подлинности такой подписи[1].

Следует оговориться, что принятие законов об ЭЦП 2002 г. и об электронной подписи 2011 г. фактически отменило разъяснения ВАС РФ о порядке использования электронной цифровой подписи, принятые задолго до вступления в силу данных законов. Речь идет об информационном письме от 19 апреля 1994 г. № С1-7/ОП-587 «Об отдельных рекомендациях, принятых на совещаниях по судебно-арбитражной практике», в котором было указано, что суд не должен принимать в качестве доказательства документы с ЭЦП в случае, если в договоре между сторонами отсутствовала процедура согласования разногласий и одна из сторон оспаривала наличие документа с ЭЦП. В Информационном письме ВАС РФ от 7 июня 1995 г. № С1-7/03-316 разъяснялось, что юридическая сила ЭЦП может признаваться при наличии в автоматизированной информационной системе программно-технических средств, обеспечивающих идентификацию.

Однако далеко не все сообщения, отправляемые посредством электронной почты, подписаны с использованием средств электронной цифровой подписи (усиленной квалифицированной подписи), в связи с чем вопрос об их допустимости в контексте п. 3 ст. 75 АПК РФ представляет особый интерес.

Как известно, Закон об ЭЦП 2002 г. содержал прямое указание на то, что он не распространяется на иные аналоги собственноручной подписи. В то же время специальных законов или иных правовых актов, регламентировавших порядок использования иных, помимо электронной цифровой подписи, аналогов собственноручной подписи, не было. Основная нагрузка по регламентации условий использования таких аналогов в договорных отношениях, а вместе с тем и на определение процессуального статуса соответствующих документов ложилась на договор. В условиях электронной коммерции наличие предварительно согласованного и подписанного бумажного договора между сторонами, регламентирующего различные аспекты будущего электронного документооборота, является скорее исключением, нежели общим правилом. В большинстве случаев стороны заключают договор посредством сети Интернет, не имея каких-либо организационных бумажных договоров с контрагентом. Процессуальный статус электронных договоров, не скрепленных электронной цифровой подписью, в итоге является неопределенным с высокой степенью вероятности

[1] Постановление ФАС Московского округа от 10 апреля 2012 г. по делу № А40-74288/11-141-615.

признания их недопустимыми доказательствами. В отсутствие иных письменных доказательств факта заключения договора и содержания его условия (актов сдачи-приемки, документов об оплате) доказать наличие договорных отношений между сторонами весьма проблематично.

В связи с этим можно привести в качестве примера следующее дело. Истец – организатор международного экономического форума – отправил другой стороне (Минздравсоцразвития России) по электронной почте приглашение принять в нем участие. Электронный адрес был взят с официального бланка Минздравсоцразвития России. Ответчик заполнил регистрационный лист с указанием двух сотрудников, а также направил просьбу забронировать отель для указанных сотрудников на период проведения мероприятия. В ответ истец отправил по электронной почте документы, подтверждающие бронирование. После получения гарантийного письма от ответчика, которым он подтверждал готовность оплатить услуги в соответствии с выставленными счетами, ему была выслана по электронной почте программа форума и пригласительные билеты. Факт участия представителей ответчика на форуме подтверждался регистрационным листом и фотоотчетом. Суд отказал в иске о взыскании стоимости оказанных услуг, сославшись на то, что представленных доказательств не достаточно для вывода о наличии между сторонами договора возмездного оказания услуг. Электронная переписка не была признана допустимым доказательством со ссылкой на п. 3 ст. 75 АПК РФ. Копия гарантийного письма ответчика не была принята во внимание, так как не был предоставлен оригинал, а копия не содержит «необходимых реквизитов документа (даты, номера), предусмотренных Государственным стандартом ГОСТ Р 51141–98»[1].

Если оставить в стороне сомнительные аргументы о недопустимости гарантийного письма в качестве доказательства, достаточно показательной является позиция о неприемлемости электронной переписки, которой самой по себе достаточно для решения вопроса о наличии или отсутствии договорных отношений между сторонами.

Определенные надежды возлагались на новый Закон об ЭП 2011 г., который должен был способствовать развитию электронной коммерции и преодолению недостатков Закона об ЭЦП. И действительно, в отличие от Закона 2002 г. он предусматривает уже три типа электронной подписи: простая электронная подпись, усиленная неквалифицированная электронная подпись и усиленная квалифицированная

[1] Постановление Девятого арбитражного апелляционного суда от 15 марта 2012 г. № 09АП-4617/2012-ГК по делу № А40-62542/11-87-479.

электронная подпись (аналог электронной цифровой подписи, предусмотренной Законом 2002 г.). Казалось бы, появился закон, о котором идет речь в п. 3 ст. 75 АПК РФ и который должен обеспечить допустимость электронных документов в качестве доказательств в гораздо большем количестве случаев, нежели в случае наличия электронной цифровой подписи. Особенно это касается документов, подписанных простой электронной подписью (т.е. сформированных с использованием паролей, кодов и иных средств, подтверждающих факт формирования документа определенным лицом), коих большинство в сфере электронной коммерции. Однако в соответствии с ч. 2 ст. 6 Закона об ЭП «информация в электронной форме, подписанная простой электронной подписью или неквалифицированной электронной подписью, признается электронным документом, равнозначным документу на бумажном носителе, подписанному собственноручной подписью, в случаях, установленных федеральными законами, принимаемыми в соответствии с ними нормативными правовыми актами или соглашением между участниками электронного взаимодействия». Иными словами, условия эквивалентности электронного и бумажного документов, а по существу – действительности электронных документов и возможности их использования в качестве доказательств по делу, ставятся опять в зависимость от наличия указания на то в законе, ином правовом акте или соглашении сторон. Круг замкнулся.

Существует устойчивая судебная практика, согласно которой распечатки электронных сообщений, не подписанных электронной цифровой подписью, рассматриваются в качестве допустимых доказательств лишь в случаях, когда соглашение сторон предусматривает возможность обмена сообщениями по электронной почте с указанием адресов, с которых такой обмен может производиться. В качестве примера можно привести следующую цитату из судебного решения: «Стороны ни в договоре, ни в приложении к нему не предусмотрели ни саму возможность обмена письмами посредством электронной почты (в том числе получение каких-либо документов посредством электронной почты), ни определили адреса электронной почты для осуществления переписки или обмена документами, в связи с чем электронная переписка истца и ответчика не может считаться надлежащим доказательством по делу»[1].

[1] Постановление Девятого арбитражного апелляционного суда от 24 февраля 2012 г. по делу № А40-93546/11-1-548. См. также: постановления Третьего арбитражного апелляционного суда от 25 июля 2012 г. по делу № А33-543/2012; Девятого арбитражного апелляционного суда от 26 января 2011 г. № 09АП-33426/2010-ГК

Очевидно, что ограничения, предусмотренные в п. 3 ст. 75 АПК РФ в отношении случаев использования электронных документов, создают необоснованные препятствия для развития гражданского оборота, так как формальное его применение предполагает, что, прежде чем заключать договор посредством обмена электронными сообщениями, скрепленными ЭЦП, необходимо предусмотреть целый ряд положений в договоре на бумажном носителе[1].

Не менее очевидна и благодатная почва для злоупотреблений со стороны недобросовестных контрагентов, которые охотно использовали высокие технологии на стадии заключения или исполнения договора, а потом «вдруг» вспомнили в нужный момент о недопустимости использования электронной переписки в качестве доказательства в отсутствие специальных договорных положений.

Неудивительно, что в некоторых случаях суды начали расширительно толковать положения п. 3 ст. 75 АПК РФ, допуская электронные сообщения в качестве доказательств не только в случае наличия прямых указаний на то в письменном договоре, но и при наличии иных обстоятельств, которые могли бы быть интерпретированы в качестве соглашения сторон об использовании электронных сообщений в своих взаимоотношениях.

Так, в некоторых случаях суд находит признаки такого соглашения в том, что инициатива вести переговоры в электронной форме исходила от ответчика (т.е. лица, делающего заявление о недопустимости электронной переписки). Так, суд указал, что «из материалов дела следует, что и проект договора на оказание услуг обсуждался сторонами посредством электронной почты, и инициатива работать посредством электронной почты исходила от представителя ответчика. Поэтому суд кассационной инстанции не может согласиться с выводом апелляционного суда о том, что полученные ответчиком по электронной почте документы нельзя считать доказательствами»[2]. Иногда суды принимают электронную переписку в качестве доказательств и в отсутствие специальных положений в договоре, если другая сторона не сделала

по делу № А40-53184/10-158-452, оставленное без изменения постановлением ФАС Московского округа от 17 мая 2011 г. № КГ-А40/4041-11; ФАС Центрального округа от 18 марта 2010 г. № Ф10-561/10 по делу № А35-3401/2009.

[1] *Ворожбит С.П.* Проблемы представления и исследования электронных почтовых сообщений в арбитражном процессе // Арбитражный и гражданский процесс. 2010. № 1.

[2] Постановление ФАС Центрального округа от 21 января 2010 г. № Ф10-5994/09 по делу № А14-3050/2009/122/15. Определением ВАС РФ от 15 марта 2010 г. № ВАС-2621/10 отказано в передаче дела № А14-3050/2009/122/15 в Президиум ВАС РФ для пересмотра в порядке надзора данного постановления.

заявление о фальсификации доказательств[1] либо не привела конкретных доводов об установлении при рассмотрении дела каких-либо обстоятельств, свидетельствовавших о невозможности идентифицировать электронное письмо общества либо об искажениях в нем[2].

В других случаях факт наличия соглашения сторон об использовании электронных сообщений, подписанных аналогом собственноручной подписи, суды усматривают в конклюдентных действиях, совершенных одной из сторон. Например, в виде оплаты, произведенной на основании документов, полученных по электронной почте[3].

Как видно, суды нередко признают неадекватность формального подхода к условиям допустимости электронных сообщений в качестве доказательств, особенно если другая сторона не приводит каких-либо конкретных доводов о недостоверности информации, содержащейся в них, а ссылается *лишь* на формальное нарушение требований п. 3 ст. 75 АПК РФ.

Однако в отсутствие единообразия судебной практики и разъяснений ВАС РФ по данному вопросу целесообразно включать в договоры условие о придании юридической силы электронным письмам, полученным с определенных адресов электронной почты. Даже если эти договоры сами заключаются в электронной форме. Поскольку суды в целом признают разумность использования электронной почты в современном договорном процессе[4], наличие таких положений в договоре, пусть и заключенном в электронной среде, более предпочтительно, нежели их полное отсутствие.

В качестве примера возможных для включения в договор можно привести следующие положения:

«Стороны договорились, что все соглашения, заключаемые в рамках настоящего Договора, а также коммуникации, возникающие в связи

---

[1] Постановление ФАС Дальневосточного округа от 16 марта 2010 г. № Ф03-1209/2010 по делу № А59-3597/2009.

[2] Определение ВАС РФ от 15 марта 2010 г. № ВАС-2621/10 по делу № А14-3050/2009-122/15. См. также постановления ФАС Северо-Западного округа от 1 июня 2010 г. по делу № А56-13328/2009; Девятого арбитражного апелляционного суда от 5 октября 2009 г. № 09АП-15486/2009-ГК по делу № А40-48586/09-48-349.

[3] Постановление ФАС Северо-Кавказского округа от 8 августа 2012 г. по делу № А53-11601/2011: «своими конклюдентными действиями (оплатой на основании полученных по электронной почте актов транспортно-экспедиционных услуг, оказанных в декабре 2010 года и январе 2011 года) ответчик подтвердил возможность обмена документами посредством электронной почты».

[4] Постановление ФАС Московского округа от 28 декабря 2011 г. по делу № А41-15927/08: «суд признал также, что обмен документами по электронной почте отвечает обычаям делового оборота, широко используется в сфере бизнеса и не противоречит нормам права, в том числе законодательству Российской Федерации».

с их исполнением, могут заключаться в том числе посредством обмена сообщениями по электронной почте.

Указанные сообщения признаются отправленными Стороной по договору, если они исходят со следующих электронных адресов _____.

Датой получения соответствующего электронного сообщения является дата его отправления другой Стороной.

Ответственность за получение сообщений и уведомлений вышеуказанным способом лежит на получающей Стороне, за исключением случаев, когда неполучение сообщения вызвано результатом неисправности систем связи вне сферы контроля такой Стороны, действия (бездействия) интернет-провайдеров или форс-мажорных обстоятельств».

В случае отказа суда в приобщении электронного письма в качестве доказательства вследствие формального подхода к прочтению п. 3 ст. 73 АПК РФ можно попробовать представить электронное сообщение как иной документ или материал в соответствии со ст. 64, 89 АПК РФ[1]. Наличие в АПК РФ неисчерпывающего перечня средств доказывания как раз и дает больше возможностей для использования в современном процессе современных средств информации[2].

В АПК РФ отсутствуют требования относительно формы представления электронных документов в качестве доказательств. Однако на основании ст. 64, 75 АПК РФ можно предположить, что в связи с необходимостью приобщения доказательств к материалам дела следует представлять электронную переписку распечатанной на бумажном носителе[3]. Данные документы должны быть надлежащим образом заверены. В большинстве случаев достаточно заверения их стороной по делу. Однако если есть основания полагать, что другая сторона будет опровергать содержимое такой переписки или сам факт ее наличия, то имеет смысл предоставить их в нотариально-заверенной форме (т.е. в виде протокола осмотра нотариусом информации на мониторе компьютера).

Рассмотренные выше положения и практика относились преимущественно к вопросу о формально-юридических условиях допустимости электронных сообщений в качестве доказательств. Однако это далеко не единственный вопрос, который может возникнуть при их

---

[1] *Малинина Е.С.* Электронное сообщение как доказательство по делу в арбитражном судопроизводстве // Администратор суда. 2009. № 2.

[2] *Боннер А.Т.* Указ. соч. С. 512.

[3] См., например: Определение ВАС РФ от 23 апреля 2010 г. № ВАС-4481/10; постановления ФАС Московского округа от 20 мая 2010 г. № КГ-А40/4455-10, ФАС Северо-Западного округа от 1 июня 2010 г. по делу № А56-13328/2009, ФАС Центрального округа от 21 января 2010 г. № Ф10-5994/09.

использовании в процессе. Нередко другая сторона делает заявление о том, что не получала такого сообщения. Тогда возникает вопрос о доказывании факта получения спорного сообщения такой стороной.

В таких случаях необходимо доказать факт принадлежности адреса электронной почты, оспаривающей факт получения сообщения стороне, факт отправки сообщения на данный адрес и в идеале – факт его получения другой стороной.

Суды исходят из того, что бремя доказывания факта принадлежности электронного адреса стороне – получателю сообщения лежит на его отправителе[1]. Наилучшим доказательством данного факта является ссылка на наличие такого электронного адреса в заключенном между сторонами контракте. В качестве иного возможного доказательства данного факта может быть сделана ссылка на контактную информацию, размещенную на веб-сайте контрагента, которая обычно расположена по ссылке «Контакты». Так, суды признают ссылки на публично доступную информацию об электронном адресе, размещенную на официальных сайтах государственных органов, в качестве достаточного доказательства принадлежности такого адреса такому органу[2].

В отсутствие специальных договорных положений с указанием «авторизованных» электронных адресов и общедоступной контактной информации на веб-сайте доказывание факта принадлежности электронного адреса определенному лицу становится весьма нелегким делом. Вряд ли российские суды возьмут на вооружение подход своих американских коллег, при котором доказывание принадлежности лицу определенного электронного адреса возможно с помощью свидетельских показаний[3].

Нередко определенные намеки на принадлежность электронного адреса определенному лицу могут содержаться уже в самом наименовании такого адреса. Например, адрес *alexandersavelyev@rambler.ru* содержит в себе достаточно определенные сведения о возможном имени

---

[1] См., например: постановление ФАС Московского округа от 30 ноября 2009 г. № КГ-А40/11226-09. В данном деле истец отрицал факт получения по электронной почте проектной документации. В связи с тем, что ответчик не смог представить доказательств принадлежности истцу электронного адреса, на который такая документация была направлена, суд признал расторгнутый истцом в одностороннем порядке договор неисполненным и взыскал сумму предоплаты в качестве неосновательного обогащения.

[2] Постановление ФАС Западно-Сибирского округа от 23 марта 2011 г. по делу № А-75-6285/2010.

[3] См., например: State v. Bohlman (Minn. Ct. App. 2006). В данном деле свидетель показал, что он неоднократно получал от ответчика электронные письма с указанного адреса почтового ящика.

его владельца[1]. Как известно, именно под своим именем обычно гражданин приобретает гражданские права и обязанности (ст. 19 ГК РФ). Другое дело, что при создании почтового ящика на общедоступных почтовых серверах вроде *yandex*, *gmail*, *yahoo* и т.п. пользователь может указать любую контактную информацию, в том числе и недостоверную, поэтому идентификационная ценность данных, содержащихся в наименовании электронного адреса, зарегистрированного на общедоступных почтовых сервисах, а равно информации, указанной при его регистрации, является достаточно невысокой. Однако в совокупности с иными доказательствами такие идентификационные данные могут приобрести доказательственную силу. К таким иным доказательствам можно отнести:

– наличие на компьютере предполагаемого отправителя следов электронного сообщения, отправленного с определенного почтового ящика. Для установления данного факта может быть истребован такой компьютер и назначена компьютерно-техническая экспертиза;

– сопоставление спорного электронного сообщения с иными сообщениями, принадлежность которых ответчику не оспаривается. В таких случаях может быть назначена автороведческая экспертиза[2];

– при наличии у предполагаемого владельца почтового ящика зарегистрированного доменного имени можно сопоставить сведения, указанные при регистрации доменного имени (в том числе адреса электронной почты), с адресами электронной почты, имеющимися в материалах дела.

В качестве примера можно привести следующее дело. Истец просил признать договор на разработку веб-сайта незаключенным в связи с отсутствием согласованного технического задания и сроков начала и окончания работ и взыскать сумму предоплаты в качестве неосновательного обогащения. Представленные ответчиком электронные письма истца с материалами для информационного наполнения сайта, по утверждению истца, на самом деле им не направлялись, указанный в предоставленных письмах электронный почтовый ящик (*mailsvb@mail.ru*) ему не принадлежит.

Суд подчеркнул, что эти утверждения истца опровергаются имеющимися в материалах дела доказательствами, которые подтверждают, что администратором домена *mircrossoft.ru* с 5 декабря 2010 г.

[1] Данный электронный адрес не принадлежит автору и приведен лишь в качестве примера того факта, что под ним может скрываться кто угодно.

[2] См. подробнее: *Галяшина Е.И.* Речеведческие экспертизы в судопроизводстве // Законы России: опыт, анализ, практика. 2011. № 12.

по настоящее время является истец, имеющий адрес электронной почты *mailsvb@mail.ru*. Сомнений в принадлежности предпринимателю адреса электронный почты *mailsvb@mail.ru* у суда не возникло, поскольку в ответе ЗАО «Региональный сетевой Информационный центр» содержались ссылки на паспортные данные и сведения об адресе администратора домена – владельца электронной почты, соответствующие паспортным и адресным данным истца по данному делу.

Кроме того, в процессе судебного заседания по рассмотрению апелляционной жалобы судом было удовлетворено ходатайство ответчика об исследовании его электронной почты с целью установления идентичности переписки сторон, представленной в материалах дела на бумажном носителе в виде распечатки файлов электронной почты с перепиской в электронном виде, находящейся в электронном почтовом ящике общества. Обществом был предоставлен суду логин и пароль для входа в электронный почтовый ящик. Суд изучил электронную переписку, осуществленную с почтового ящика *mailsvb@mails.ru* на принадлежащий ответчику почтовый ящик *liccilip@gmail.com,* и признал имеющиеся в материалах дела документы идентичными с их электронными версиями.

В итоге суд пришел к выводу о том, что общество привело надлежащие доказательства, свидетельствующие о ведении между сторонами электронной переписки по вопросу согласования характеристик сайта, предоставлению необходимых материалов для наполнения сайта и исполнения договора, а предприниматель не доказал обратное в соответствии со ст. 65 АПК РФ.

Суд также подчеркнул, что предприниматель отказался от предоставления доказательств, в том числе от помощи суда по истребованию их от интернет-провайдера (о том, какой электронный почтовый ящик зарегистрирован за истцом), от владельцев электронных ресурсов *mail.ru* и *gmail.ru* (относительно подтверждения или опровержения ведения переписки, предоставленной ответчиком в вышеуказанные даты, соответствующего содержания между сторонами)[1].

Данное дело представляет особый интерес не только в связи с тем, что речь шла о почтовых ящиках, зарегистрированных на общедоступных почтовых сервисах, но и в связи с тем, что суд достаточно подробно изложил свое мнение по вопросам возможных доказательств принадлежности этого ящика определенному лицу. Следует максимально

[1] Постановление Первого арбитражного апелляционного суда от 23 декабря 2011 г. по делу № А43-9577/2011, оставленное без изменения постановлением ФАС Волго-Вятского округа от 18 апреля 2012 г.

использовать данные, которыми располагают регистраторы доменных имен и интернет-провайдеры, у которых можно затребовать сведения относительно подтверждения или опровержения факта ведения переписки между сторонами в конкретные даты.

Данные, предоставленные интернет-провайдерами, активно используются и зарубежными судами при анализе вопросов о принадлежности электронного почтового ящика определенному лицу. Так, в одном из дел, рассмотренных китайским судом, истец представил доказательства использования данного почтового адреса ответчиком в общении с другими лицами, использования офисного телефона ответчика для дозвона интернет-провайдеру (дело было во времена широкого распространения *dial-up*) и отправления сообщения под определенным *IP*-адресом в определенное время и привел свидетеля, который подтвердил факт присутствия ответчика в офисе в это время[1]. Правда, как видно, немалую роль здесь сыграли и свидетельские показания, которые пока неохотно принимаются отечественными арбитражными судами.

Идентификационные данные, содержащиеся в электронном письме, отправленном с корпоративной почты, должны иметь иной статус, нежели данные с общедоступных почтовых сервисов. Во-первых, получить электронный адрес на сервере корпоративной почты может не любое заинтересованное лицо, а только сотрудники компании или в порядке исключения иные заранее определенные категории лиц. Во-вторых, пользование такой почтой предполагает наличие строгих процедур идентификации, обеспечивающих «привязку» почтового ящика к конкретной личности, а также повышенных требований к паролям, порядку их регулярного изменения и обеспечения их конфиденциальности. В-третьих, наличие в электронном адресе указания на наименование организации в доменном имени почтового сервера также указывает на связь определенного физического лица с данной организацией[2]. В связи с этим имеет смысл несколько уточнить высказывание А.Т. Боннера, который хотя и признает наличие в электрон-

[1] Shao Dali vs. Zhang Ershen Beijing First Intermediate People's Court, January 2001. См.: *Wang M.* Electronic Evidence in China // Digital Evidence and Electronic Signature Law Review. No 5. 2008. P. 48.

[2] Поскольку электронное письмо, отправленное с корпоративной почты, содержит в себе информацию о его происхождении и принадлежности к определенной компании, в США идентификационные данные, содержащиеся в таком письме, считаются обычно достаточными для его аутентификации в целях решения вопроса об их допустимости в процессе (правило 902 (7) Федеральных правил о доказательствах) (см.: *Goode S.* Op. cit. P. 41).

ном адресе реквизитов, идентифицирующих электронный документ, но отмечает, что «такого рода реквизиты не позволяют с достоверностью установить отправителя электронного документа»[1]. Это справедливо в отношении бесплатных почтовых сервисов, но не электронных адресов корпоративной электронной почты, которые содержат в наименовании достаточно персонализирующих их обладателя сведений (*alexander.savelyev@ru.ibm.com*).

В некоторых случаях, когда невозможно отрицать факт принадлежности электронного сообщения сотруднику ответчика, им может быть сделано заявление о том, что такое лицо не является уполномоченным. Поскольку в данном случае речь идет о материально-правовой трактовке отношений, мы не будем останавливаться на подробном его анализе, отметив, что имеет место судебная практика, согласно которой факт активного участия в согласовании условий договора по электронной почте может являться основанием для вывода о наличии представительства в силу обстановки[2].

Установив факт принадлежности определенного электронного почтового ящика, на которое было отправлено электронное письмо, необходимо доказать факт такого отправления. С этой целью могут представляться различные доказательства.

Во-первых, протокол осмотра почтового ящика, произведенного нотариусом. В процессе совершения действий по обеспечению доказательств нотариус осматривает компьютер, с которого велась электронная переписка, удостоверяет факт ее наличия и составляет протокол с подробным описанием своих действий[3]. Сами электронные письма распечатываются и подшиваются к протоколу. Нотариально заверенный протокол будет доказательством того, что на определенную дату в данных осмотренного компьютера действительно имелись электронные сообщения с конкретной информацией. Подробнее о порядке нотариального обеспечения доказательств, полученных из сети Интернет, будет сказано далее. Забегая немного вперед, необходимо отметить, что такое обеспечение должно иметь место до возбуждения дела в суде. В рамках действующего процесса возможно заявление

[1] *Боннер А.Т.* Указ. соч. С. 510.

[2] Постановление ФАС Восточно-Сибирского округа от 18 февраля 2011 г. № А33-3344/2010. Поскольку стороны регулярно согласовывали план и объем размещения рекламы, довод о том, что менеджер не обладал полномочиями по согласованию условий договора, был отклонен судом, поскольку полномочия явствовали из обстановки (абз. 2 п. 1 ст. 182 ГК РФ).

[3] См. подробнее: *Бегичев А.В.* Обеспечение доказательств нотариусами: Теория и практика. М., 2013. С. 197.

ходатайства об осмотре содержимого почтового ящика в порядке ст. 78 АПК РФ, ст. 58 ГПК РФ. К такому осмотру для оказания консультаций, непосредственной технической помощи при осмотре целесообразно привлечь специалиста, поскольку он обладает специальными знаниями в области информационных технологий.

В качестве примера можно привести дело, рассмотренное арбитражным судом г. Хабаровска, где суд непосредственно в зале заседания произвел осмотр содержимого почтового ящика общества на почтовом сервере «*Mail.ru*», в ходе которого было установлено, что в папке «Отправленные» имеется письмо с приложенной котировочной заявкой, в в папке «Входящие» имеется полученное 9 декабря 2011 г. письмо с указанием адреса и имени отправителя: *ofimz@mail.ru*, Волошин Владимир, что соответствует реквизитам почтового ящика отдела, указанного в извещении о запросе котировок. Данных сведений было достаточно суду для того, чтобы признать факт получения заявки отделом, даже несмотря на тот факт, что он удалил всю переписку со своего сервера[1].

Во-вторых, для подтверждения факта отправки (получения) электронного сообщения целесообразно привлечение в процесс данных, находящихся у интернет-провайдеров. В частности, их лог-файлы могут содержать системную информацию о работе сервера и информацию о действиях пользователей, включающую дату и время визита пользователя, *IP*-адрес компьютера пользователя, факт отправки сообщения с *IP*-адреса пользователя, факт получения сообщения с определенного *IP*-адреса с указанием времени[2]. Существуют прецеденты, в которых суды достаточно лояльно подходили к принятию распечаток лог-файлов провайдера.

Для получения указанных сведений может быть заявлено ходатайство об истребовании доказательства (ст. 66 АПК РФ, ст. 57 ГПК РФ).

Таким образом, факт отправки сообщения и его получения другой стороной может быть подтвержден данными лог-файлов интернет-

[1] Решение арбитражного суда Хабаровского края от 2 апреля 2012 г. по делу № А73-1608/2012, оставленное без изменения постановлением Шестого арбитражного апелляционного суда от 27 июня 2012 г. № 06АП-2252/2012.

[2] Постановление ФАС Московского округа от 6 февраля 2013 г. по делу № А40-68757/11-42-562: «Проанализировав данные лог-файла от 29.10.2010, суды установили, что электронное платежное поручение поступило 29.10.2010 в 15 час 50 мин с *IP*-адреса 178.177.143.22. (Распечатка лог-файлов, которые содержат сведения о соединениях между *IP*-адресами 212.17.3.23 и 62.105.142.132 за период с 01.01.2008 по 31.12.2008 с указанием следующих реквизитов: год, месяц, день, время, *IP*-адрес и номер порта, с которого передавалась информация, *IP*-адрес и номер порта, на который передавалась информация, количество переданных байт)».

провайдеров, обслуживающих отправителя и получателя. Но поскольку они не предоставляют информацию о содержимом сообщения, здесь как раз и требуется представление дополнительных доказательств аутентичности отправленного и полученного сообщений, которое лучше всего представлять в форме протокола осмотра нотариусом содержимого почтового ящика. В случае невозможности его представления, можно рассмотреть вопрос о назначении компьютерно-технической экспертизы для подтверждения факта отправки спорного сообщения с определенного компьютера в указанное время.

В литературе отмечается, что определенные проблемы с представлением электронных документов в качестве доказательств могут возникнуть вследствие наличия в процессуальном законодательстве требований представления оригиналов документов, поскольку российское законодательство не знает терминов «подлинник электронного документа» и «копия электронного документа»[1]. Так, в соответствии с п. 6 ст. 71 АПК РФ арбитражный суд не может считать доказанным факт, подтверждаемый только копией документа или иного письменного доказательства, если утрачен или не передан в суд оригинал документа, а копии этого документа, представленные лицами, участвующими в деле, не тождественны между собой и невозможно установить подлинное содержание первоисточника с помощью других доказательств. Арбитражный суд вправе потребовать представления подлинника письменного документа по своему усмотрению (п. 9 ст. 75 АПК РФ).

Следует отметить, что предпочтение подлинных документов копиям свойственно не только российскому праву. Например, англо-американскому процессуальное праву известно правило «лучшего доказательства» (*best evidence rule*), в соответствии с которым если существует оригинал письменного доказательства, то именно он и должен быть представлен суду в отсутствие уважительных обстоятельств, обосновывающих допустимость копии[2]. Правда, в Англии данное правило допустимости доказательства было фактически отменено в 2001 г. решением *Masquerade Music Ltd. v. Springsteen* и доказательственный вес копии документа оценивается в совокупности с иными доказательствами.

Федеральные правила о доказательствах США несколько иначе подошли к адаптации *best evidence rule* к современным реалиям, объявив подлинником письменного документа или записи в том числе и любую их копию, которой изготовившее или исполняющее ее лицо

[1] Правовые аспекты использования интернет-технологий / под ред. А.С. Кемрадж, Д.В. Головерова. С. 101.

[2] Black's Law Dictionary, Thomson Reuters. 9th ed. 2011. P. 635.

намеревалось придать такую же юридическую силу. Если данные хранятся в компьютере или другом подобном устройстве, то подлинником письменного материала или записи будет являться любая распечатка или иной способ их представления в форме, доступной для прочтения человеком, точно отражающей эти данные[1].

Аналогичных положений в российском законодательстве нет, как, впрочем, и законодательной дефиниции понятий «подлинник» и «копия». Исходя из положений ГОСТ Р 51141–98 подлинником является первый или единичный экземпляр документа. Аналогичное положение закреплено в п. 3.2 ГОСТ 6.10.4–84 относительно документа на машинном носителе[2]. Применимость данных дефиниций к электронным документам подвергается весьма обоснованному сомнению в литературе. По верному замечанию Н.И. Лукьяновой, первый экземпляр электронного документа ничем не отличается от второго, третьего или, скажем, его десятого экземпляра, в связи с чем становится непонятным, почему такой экземпляр будет считаться подлинником, а все последующие экземпляры – копиями[3].

В связи с этим в отечественной литературе получил широкую поддержку американский подход, в соответствии с которым все электронные копии электронных документов признаются подлинниками. Так, согласно позиции А.А. Косовца «целесообразней было бы считать полностью аутентичные копии (здесь термин «копия» употребляется не в юридическом смысле, а в смысле информационном) документа подлинниками, то есть признать, что электронный документ может иметь сколь угодно много подлинников»[4].

Соглашаясь в целом с указанным предложением, хотелось бы отметить, что более предпочтительным было бы включение прямой оговорки в процессуальное законодательство о неприменимости положений, разграничивающих статус копий и подлинников, к электронным документам. Это создаст гораздо меньше проблем на практике, нежели попытки определить, насколько данная конкретная техническая копия электронного документа является аутентичной первоначально созданному документу с целью придания ей статуса подлинника. Такой

---

[1] Federal Rules of Evidence, Rule 1003.

[2] *Карев Я.А.* Указ. соч. С. 142.

[3] См.: *Лукьянова Н.И.* Использование документов и материалов, изготовленных посредством электронной связи, в качестве средств доказывания в арбитражном процессе Российской Федерации // Государство и право. 2000. № 6. С. 98.

[4] *Косовец А.А.* Правовое регулирование электронного документооборота // Вестник Московского университета. Сер. 11. Право. 1997. № 4. См. также: *Карев Я.А.* Указ. соч. С. 144.

анализ предполагает наличие возможности сравнения такой электронной копии с чем-то «эталонным», что далеко не всегда возможно, да и влечет неоправданное усложнение процесса. Гораздо эффективнее предоставить судье возможность определить «качество» такого электронного доказательства в процессе его оценки в совокупности с иными доказательствами.

§ 3. Распечатки информации с веб-сайтов как доказательство в гражданском и арбитражном процессе

При рассмотрении споров, возникающих в сфере электронной коммерции, неизбежно встает вопрос о процессуальном статусе информации, содержащейся на веб-сайтах сети Интернет. Необходимость ее представления в суд может обусловливаться, к примеру, необходимостью анализа договорных условий или их части, изложенных на веб-сайте, или размещенной информации о товаре (услуги) на предмет ее достоверности и достаточности. К тому же следует помнить о возможности предъявления деликтных исков по фактам нарушения интеллектуальных прав, размещения сведений, порочащих деловую репутацию, или иных проявлений недобросовестной конкуренции.

Как отмечается, процессуально-правовая природа информации, получаемой из сети Интернет, требует дополнительного исследования. Некоторые специалисты рассматривают ее как разновидность вещественных доказательств. По мнению И.В. Решетниковой, в ситуациях, когда речь идет об обеспечении арбитражными судами доказательств, распололженных на веб-сайтах, «скорее всего, речь идет о фиксации вещественного доказательства путем его осмотра, о чем составляется протокол»[1]. В качестве вещественных доказательств распечатки с интернет-ресурсов рассматриваются английскими судами[2]. С нею отчасти согласен А.Т. Боннер, отмечающий, что «на данном этапе развития процессуального законодательства и науки процессуального права условно можно говорить о сайтах в Интернете как о неких специфических вещественных доказательствах», добавляя при этом, что не все нормы о вещественных доказательствах применимы в данном случае, в частности о хранении вещественных доказательств[3]. В любом случае безотносительно к тому, какова природа соответствующих до-

[1] См.: *Решетникова И.В.* и др. Комментарий судебных ошибок в практике применения АПК РФ. М., 2006. С. 130.

[2] R. v. Coventry Magistrates Court [2004]. A.C. 74.

[3] *Боннер А.Т.* Указ. соч. С. 527.

казательств, тот факт, что информация, полученная из сети Интернет, имеет доказательственное значение как в судах общей юрисдикции, так и в арбитражных судах, не вызывает сомнений[1]. Ключевой вопрос заключается в том, в каком виде ее представить в суд.

В американской судебной практике распечатки с официальных веб-сайтов принимаются в качестве доказательств при условии, что они содержат *URL* и дату распечатки[2]. При этом должны быть представлены доказательства того, что данная распечатка отражает сведения, которые содержались на веб-странице на тот момент времени. Как правило, данное обстоятельство может быть доказано путем представления заявления или аффидавита от лица, которое обладает таким знанием (*someone with knowledge*). В некоторых случаях суды требуют, чтобы такое заявление исходило от владельца сайта[3]. Правда, как отмечается в американской литературе, в большинстве случаев суды относятся более либерально к условиям допустимости распечаток страниц веб-сайтов[4]. Например, в одном из дел в качестве достаточного доказательства аутентичности распечатки содержимого веб-сайта суд принял пояснения истца о том, как была сделана распечатка: представитель истца лично ввел в браузер адрес *www.losjarritos.com*, получил доступ к сайту и распечатал соответствующую страницу[5]. Обычно данное заявление оценивается в совокупности с иными доказательствами. Если же ресурс, с которого была распечатана информация, принадлежит третьему лицу (не стороне по спору), то заявления владельца ресурса о том, что распечатки соответствуют данным ресурса, обычно достаточно[6].

---

[1] *Боннер А.Т.* Указ. соч. С. 519–522, 532.

[2] U.S. Equal Emp't Opportunity Comm'n v. E.I. DuPont De Nemours & Co., No. 03-1605, 2004 (E.D. La. Oct. 18, 2004). Справедливости ради надо отметить, что дата распечатки содержимого интернет-страницы может иметь доказательственное значение и в российских судах. См.: Определение ВАС РФ от 10 февраля 2012 г. № ВАС-16311/11 по делу № А40-7557/11-152-86: «Поскольку заявитель апелляционной жалобы – общество «ДИ САНЛИ» – указывал, что исследованная судом первой инстанции распечатка *web*-страницы с интернет-сайта *www.disanli.com/imushestvo.htm* подтверждает только дату ее распечатку – 07.12.2010, а не дату размещения информации, суд апелляционной инстанции, приняв новое доказательство по делу – аналогичную распечатку указанной страницы, но уже с датой распечатки от 26.11.2010, представленную судебным приставом-исполнителем, признал размещение информации о торгах в сети Интернет в срок, установленный законом».

[3] Costa v. Keppel Singmarine Dockyard PTE, Ltd. (C.D. Cal. 2003); United States v. Jackson, 208 F.3d (7th Cir. 2000).

[4] *Goode S.* Op. cit. P. 14.

[5] Jarritos, Inc. v. Los Jarritos, No C-05-02380 (N.D. Cal. 2007) revised on other grounds (9th Cir. 2009). См. также: Kassouf v. White (Ohio App. 2000).

[6] Telewizja Polska USA, Inc. v. EchoStar Satellite Corp. No 02 C 3293 (N.D. Ill. 2004).

Распечатки с сайтов официальных органов принимаются в качестве доказательства без необходимости представления дополнительных доказательств их подлинности в порядке правила 902 (5)[1] Федеральных правил о доказательствах.

Российские реалии несколько отличаются от американских. Как отмечается в литературе, просто распечатать на принтере страницу с веб-сайта либо сохранить ее на каком-нибудь носителе, а затем представить суду означает не представить ничего[2]. Объясняется это тем, что информация на распечатке веб-сайта может существенно отличаться от первоисточника. Соглашаясь в целом с данным выводом, необходимо отметить, что суды в некоторых случаях все же принимают в качестве доказательств обычные распечатки веб-сайтов.

Так, в одном из дел фирма была привлечена к ответственности по ч. 2 ст. 15.19 КоАП РФ (отсутствие у лица, осуществляющего профессиональную деятельность на рынке ценных бумаг, информации о расчете размера собственных средств на странице сайта в сети Интернет). В качестве главного доказательства фигурировали скриншоты – снимки экрана монитора, на которых был зафиксирован факт отсутствия необходимой информации на определенную дату. Суд отклонил довод ответчика о том, что скриншоты не могут быть приняты в качестве надлежащих и достоверных доказательств[3]. На доказательственный характер распечатки страницы с веб-сайта указано и в Постановлении Пленума ВАС РФ от 17 февраля 2011 г. № 12, в котором указано, что иным документом в смысле п. 9 ч. 1 ст. 126 АПК РФ может являться в том числе распечатанная на бумажном носителе и заверенная подписью истца или его представителя копия страницы официального сайта регистрирующего органа в сети Интернет, содержащей сведения о месте нахождения юридического лица и дату этих сведений обновления[4].

Как отмечается, суды общей юрисдикции также все более активно принимают распечатки с сайтов в качестве доказательств доставки почтового отправления (сайт Почты России), в качестве доказа-

---

[1] Данный пункт содержит указание о том, что официальные публикации государственных органов «свидетельствуют сами о себе» (*self-authenticating*).

[2] *Юзефович В.Б.* Доказательства и доказывание в арбитражном процессе: анализ правоприменительной практики. Выводы судебного юриста. М., 2012. С. 63.

[3] Постановление ФАС Западно-Сибирского округа от 30 августа 2011 г. № А70-23/2011.

[4] Постановление Пленума ВАС РФ от 17 февраля 2011 г. № 12 «О некоторых вопросах применения Арбитражного процессуального кодекса Российской Федерации в редакции Федерального закона от 27 июля 2010 г. № 228-ФЗ «О внесении изменений в Арбитражный процессуальный кодекс Российской Федерации»».

тельств места нахождения организации (сайт Федеральной налоговой службы)[1].

Представляется, что суды должны принимать распечатки с сайтов федеральных органов государственной власти без каких-либо требований об их заверении владельцами таких сайтов. В качестве основания для такого вывода можно указать на необходимость применения средств электронной цифровой подписи к публикуемому информационному наполнению таких сайтов, сертифицированных ФСБ России или ФСТЭК России[2], что обеспечивает достаточную гарантию аутентичности содержимого таких веб-сайтов.

Тем не менее рассчитывать на то что российский суд благосклонно воспримет распечатку с обычного (негосударственного) веб-сайта, представленную частным лицом, а не государственным органом в порядке производства из публично-правовых отношений, все же несколько самонадеянно. Особенно если такая распечатка имеет своей целью доказывание обстоятельств, от которых в значительной степени зависит решение дела, либо если есть основания полагать, что другая сторона будет всячески оспаривать достоверность информации, содержащейся в ней[3]. В связи с этим имеет смысл позаботиться о придании такой распечатке дополнительной убедительности. Это может быть реализовано путем судебного или нотариального обеспечения доказательств.

Несмотря на то что институт обеспечения доказательств отражен и в гражданском, и в арбитражном процессе, только АПК РФ предусматривает возможность *досудебного* обеспечения доказательств, которое имеет особую ценность в интернет-спорах. Так, в соответствии со ст. 72 АПК РФ лицо может обратиться в арбитражный суд с заявлением об обеспечении доказательств до предъявления иска по существу спора, если есть основания опасаться, что представление таких

[1] *Иванова Ю.В.* В области защиты интеллектуальных прав все еще немало «Белых пятен», которыми беззастенчиво пользуются правонарушители [Интервью с О.Д. Анциферовым] // Адвокат. 2012. № 1.

[2] Требования о защите информации, содержащейся в информационных системах общего пользования, утв. Приказом ФСБ России и ФСТЭК России от 31 августа 2010 г. № 416/489, п. 17.

[3] Постановление ФАС Московского округа от 5 февраля 2013 г. по делу № А40-135406/11-19-276: представленная истцами распечатка с интернет-сайта http://corpcollection.ru от 2 ноября 2011 г. не может быть принята в качестве надлежащего доказательства распространения порочащих деловую репутацию истцов сведений, поскольку данные доказательства не обеспечены в порядке, установленном законодательством о нотариате, ходатайство об осмотре информации, размещенной в телекоммуникационной сети в режиме реального времени истцом не заявлялось». Аналогичные выводы изложены и в постановлении ФАС Уральского округа от 26 марта 2012 г. № Ф09-9858/11 по делу № А76-2698/2011.

доказательств впоследствии будет невозможным и затруднительным. Поскольку информация в сети Интернет может быть легко удалена с веб-сайта либо вместе с таким веб-сайтом, можно говорить о том, что представление доказательств, содержащих информацию с веб-сайта, может быть невозможным или затруднительным в случае непринятия своевременных мер по ее закреплению[1]. При условии, что заявитель приведет убедительные доводы для применения предварительного обеспечения доказательств, укажет обстоятельства, для подтверждения которых необходимы доказательства, а также причины, побудившие обратиться с заявлением об их обеспечении, арбитражный суд удовлетворяет ходатайство о предварительном обеспечении доказательств[2].

На основании определения арбитражного суда об удовлетворении ходатайства о предварительном обеспечении доказательств судебный пристав с участием специалиста в порядке исполнительного производства производит осмотр веб-сайта в сети Интернет с целью выявления факта нарушения прав заявителя, фиксирует полученную информацию с составлением акта осмотра. Очевидно, что информация о содержимом веб-сайта, полученная с использованием такой процедуры, не вызовет у арбитражного суда сомнений относительно ее допустимости и относимости.

Наиболее эффективной альтернативой досудебному обеспечению доказательств арбитражным судом является обеспечение доказательств нотариусом. В соответствии с ч. 1 ст. 102 Основ законодательства о нотариате (далее – Основы о нотариате) по просьбе заинтересованных лиц нотариус обеспечивает доказательства, необходимые в случае возникновения дела в суде или административном органе, если имеются основания полагать, что представление доказательств впоследствии станет невозможным или затруднительным.

При этом причины, по которым представление доказательств может стать невозможным или затруднительным, Основами о нотариате не указываются. Представляется, что применительно к заверению

[1] Что не означает, что суд готов удовлетворять все ходатайства об обеспечении доказательств, размещенных в сети Интернет. См., например: постановление ФАС Московского округа от 29 июля 2009 г. № КГ-А40/6565-09 по делу № А40-43441/07-5-399. В данном деле было отказано в обеспечении доказательства в виде копии сайта «*compomat.ru*» и лог-файлов к нему, так как заявитель не доказал необходимость принятия мер по обеспечению доказательств, указанных в заявлении, не представил какой-либо информации о реальной угрозе невозможности или затруднительности использования источника необходимых сведений.

[2] Пункт 17 информационного письма Президиума ВАС РФ от 7 июля 2004 г. № 78 «Обзор практики применения арбитражными судами предварительных обеспечительных мер».

страниц веб-сайта в данном случае может использоваться та же мотивировка, что и для обеспечения аналогичных доказательств в арбитражном суде. Как отмечено в Письме Федеральной нотариальной палаты, «Информация, размещенная в сети Интернет, объективно выражена только в электронном виде. По своей природе информация в сети Интернет отличается от письменных и вещественных доказательств, поскольку может быть уничтожена любыми лицами в кратчайшие сроки посредством удаления из сети Интернет»[1].

Действуя в соответствии с п. 18 ст. 35, ст. 102–103 Основ о нотариате, нотариус фиксирует в присутствии сторон и заинтересованных лиц содержание страницы в Интернете, на которой находятся спорные сведения, тем самым обеспечивая необходимые доказательства до предъявления иска в суд.

В ходе совершения указанного нотариального действия нотариус осматривает соответствующий информационный ресурс начиная с главной (стартовой страницы) веб-сайта, распечатывает его содержимое на бумажный носитель и составляет протокол осмотра доказательств. В целях предотвращения возможных фальсификаций на практике в процессе осмотра доказательств в Интернете нередко применяются специальные программы-утилиты, направленные на повышение достоверности полученных данных, в частности: сервис *WhoIS*, позволяющий определить администратора доменного имени, под которым размещен осматриваемый веб-сайт; программа *nlookup*, позволяющая определить *IP*-адрес веб-сайта с использованием данных, полученных с помощью сервиса *WhoIS*; программа *ping*, позволяющая проверить, совпадает ли определенный посредством программы *nlookup IP*-адрес с тем, к которому обращается браузер; а также программа *tracert* (в *ОС Windows*), с помощью которой отслеживается маршрут доступа к целевому веб-сайту[2]. Хотя польза от использования последней программы несколько сомнительна, поскольку она предназначена для диагностики проблем связи и является способом проверки, существует ли для запроса открытый путь к получателю и нет ли задержек соединения. Сведения, отображаемые данной программой, не являются гарантией того, что в маршрут не «вклинился» какой-нибудь подложный веб-сайт.

Специалистами в области нотариата отмечается, что обширное применение технических мер при оценке достоверности расположения искомого веб-сайта по определенному адресу не в полной мере впи-

[1] Письмо ФНП от 13 января 2012 г. № 12/06-12 «Об обеспечении нотариусом доказательств» // Нотариальный вестник. 2012. № 4.

[2] См. подробнее: *Бегичев А.В.* Указ. соч. С. 176–178.

сывается в понятие осмотра письменного доказательства и выходит за рамки полномочий нотариуса по осмотру доказательств, что может являться основанием для оспаривания протокола и исключения его из числа доказательств, поскольку нотариус подменяет собой эксперта[1]. В связи с этим, по их мнению, рекомендуется привлекать к осмотру эксперта как лица, обладающего специальными познаниями в области компьютерных технологий.

В случае, если содержание сайта изложено на иностранном языке, то после распечатывания осмотренной информации ее письменно переводит переводчик, подлинность подписи которого свидетельствует нотариус. На практике это означает, что к распечаткам подшивается письменный перевод текста с удостоверительной надписью нотариуса, затем весь этот комплект подшивается к протоколу осмотра в качестве приложения[2].

В протоколе отражаются технические средства и программы (в том числе веб-браузер), которые применялись в процессе осмотра, дата и время проведения осмотра. Разумеется, использованные программы должны быть лицензионными, в противном случае будут основания утверждать о том, что доказательство было получено с нарушением закона.

В соответствии со ст. 103 Основ законодательства о нотариате осмотр доказательств производится в присутствии заявителя и заинтересованных сторон, к числу которых может быть отнесен и владелец сайта, осмотр которого осуществляется. В литературе указывалось на необходимость исключения из общего правила положения о том, что осмотр доказательства происходит в присутствии сторон и заинтересованных лиц. Во-первых, в случае уведомления потенциального ответчика о подобном действии ему не составит особого труда изменить содержащуюся на сайте информацию, а во-вторых, если становится известно время и место выхода нотариуса в Интернет на конкретные сайты, технически возможно направить информацию четко определенного содержания на компьютер нотариуса, что может исказить действительное содержание доказательства[3].

Пока соответствующие изменения не внесены, однако правоприменительная практика уже идет по пути следования этим рекомендациям. Так, в указанном ранее Письме ФНП отмечается, что «поскольку

[1] Там же. С. 175. В этом случае, по мнению автора, поскольку данные вопросы относятся более к компетенции эксперта как лица, обладающего специальными познаниями в области компьютерных технологий, именно его рекомендуется привлекать к осмотру.

[2] *Бегичев А.В.* Указ. соч. С. 195.

[3] *Лещенко А.И., Лещенко А.И.* Актуальные вопросы обеспечения доказательств нотариусом // Закон. 2008. № 9; *Юзефович В.Б.* Указ. соч. 2012. С. 65.

обеспечение доказательств нотариусом осуществляется до возникновения судебного разбирательства, «сторон» в процессуальном понимании этого термина на момент совершения нотариального действия еще не существует. При этом лица, которые предположительно могут выступать в будущем судебном разбирательстве в качестве ответчиков или третьих лиц, как правило, не заинтересованы в обеспечении нотариусом доказательства, подтверждающего нарушение прав заявителя». В связи с этим делается вывод о том, что «извещение нотариусом заинтересованных лиц о времени и месте проведения осмотра информационного ресурса в сети Интернет может привести к утрате доказательства, за обеспечением которого к нотариусу обратился заявитель, вследствие чего заявитель лишится возможности доказать в суде факт нарушения своего права»[1]. Арбитражная практика также исходит из допустимости протокола осмотра веб-сайта, совершенного в отсутствие лица, разместившего эту информацию[2].

Следует особо подчеркнуть, что ч. 2 ст. 102 Основ законодательства о нотариате не допускает возможность обеспечения нотариусом доказательств по делам, находящимся в производстве суда. Данная норма является следствием соблюдения принципа непосредственности судебного разбирательства, закрепленного в ч. 1 ст. 10 АПК РФ, согласно которой арбитражный суд при разбирательстве дела обязан непосредственно исследовать все доказательства по делу[3], а также следствием наличия процедуры обеспечения доказательств непосредственно в ГПК РФ[4].

Арбитражные суды обычно признают недопустимыми доказательства, обеспеченные нотариусом по заявлению заинтересованных лиц, в то время как дело, по которому обеспечено законодательство, находилось в производстве суда[5].

---

[1] Письмо ФНП от 13 января 2012 г. № 12/06-12 «Об обеспечении нотариусом доказательств» // Нотариальный вестник. 2012. № 4.

[2] Постановления ФАС Северо-Западного округа от 10 февраля 2011 г. по делу № А56-14567/2010; ФАС Московского округа от 21 мая 2010 г. № КГ-А40/4810-10 по делу № А40-10765/09-93-112; определение Санкт-Петербургского городского суда от 20 июня 2011 г. № 33-9194/2011.

[3] Постановление ФАС Московского округа от 11 сентября 2012 г. по делу № А40-111324/11-141-944.

[4] Как отмечено в п. 7 Пленума Верховного Суда РФ от 15 июня 2010 г. № 16 «О практике применения судами Закона РФ «О средствах массовой информации»»: «по делам, связанным с распространением сведений через телекоммуникационные сети, не исключается возможность обеспечения доказательств судьей, поскольку круг доказательств, которые могут быть обеспечены законом, неограничен (ст. 64–66 ГПК РФ).

[5] Постановления Девятого арбитражного апелляционного суда от 12 апреля 2010 г. № 09АП-4914/2010-ГК по делу № А40-72761/09-8-542; ФАС Московского округа от 15 августа 2012 г. по делу № А40-118696/11-27-1014.

В связи с этим, если дело уже принято судом к производству, можно подать заявление об обеспечении доказательства путем осмотра информационного ресурса в сети Интернет в порядке ст. 78 АПК РФ. Для осуществления осмотра веб-сайта может быть использована помощь специалиста. Отказ суда в удовлетворении заявления об обеспечении доказательств в виде проведения осмотра информационных ресурсов, опубликованных в сети Интернет, может являться основанием для отмены вынесенного решения и направления дела на новое рассмотрение[1]. На возможность проведения судом осмотра размещенной в сети Интернет информации в режиме реального времени в случаях, не терпящих отлагательства, при подготовке дела к судебному разбирательству, а также в ходе самого разбирательства указывает и Пленум Верховного Суда РФ. Такой осмотр проводится в порядке, предусмотренном ст. 58 и 184 ГПК РФ (с извещением участвующих в деле лиц, с фиксированием результатов в протоколе, с привлечением при необходимости специалиста)[2].

Применительно к доказательствам, полученным из сети Интернет, очень актуальным является вопрос о том, можно ли найти какой-нибудь способ доказать, как выглядела та или иная веб-страница в определенный момент времени. Нередко информация, некогда размещенная на веб-сайте, на момент возникновения спора либо удалена, либо изменена. Однако ошибочно предполагать, что она исчезает бесследно. Во-первых, она может сохраниться в кэш-памяти поисковых систем. Во-вторых, она может сохраниться у интернет-провайдера, предоставлявшего услуги хостинга владельцу информационного ресурса. В-третьих, копия страницы веб-сайта может сохраниться в специализированных интернет-архивах, наиболее известным и обширным из которых является *Wayback Machine* (англ. – «машина времени»). В самом общем виде суть сервиса *Wayback Machine* можно свести к систематическому копированию содержания интернет-страниц по состоянию на определенный момент времени с последующим включением их в специальный архив, используя который любое заинтересованное лицо может посмотреть, как выглядела та или иная интернет-страница в определенный момент времени, введя соответствующий запрос на сайте *www.archive.org*.

Для функционирования интернет-архива *Wayback Machine* используется специальное программное обеспечение («поисковые роботы»),

[1] Постановление ФАС Московского округа от 10 сентября 2012 г. по делу № А40-101177/11-34-904.

[2] Пункт 7 Пленума Верховного Суда РФ от 15 июня 2010 г. № 16 «О практике применения судами Закона РФ «О средствах массовой информации»».

посредством которого осуществляется просмотр интернет-страниц, анализ их содержимого, его индексирование, поиск ссылок, существующих на такой интернет-странице, и переход по ним на другие интернет-страницы с последующим повторением указанного процесса. При отсутствии определенных ограничений, установленных владельцем интернет-ресурса (о которых будет сказано далее), интернет-страница включается в состав интернет-архива и становится доступной для пользователей *Wayback Machine* через определенное время. Указанные процессы полностью автоматизированы и осуществляются без человеческого участия[1].

Сервис *Wayback Machine* предоставляется некоммерческой организацией *Internet Archive*, которая имеет официальный статус библиотеки в соответствии с законодательством штата Калифорния и является одним из соучредителей и участников Международного консорциума по сохранению Интернета (*International Internet Preservation Consortium*) наряду с национальными библиотеками Франции, Германии, Австралии, Нидерландов, Китая, Швейцарии, Южной Кореи, Японии, США и многих других стран[2].

Нахождение данных архива под контролем авторитетной независимой от сторон спора организации и автоматизированный процесс формирования данных интернет-архива, исключающий возможность манипуляций с содержимым данного архива заинтересованной стороной, обусловили доверие судов к данным (распечаткам), полученным из указанного источника.

Так, распечатки интернет-страниц из архива *Wayback Machine* принимаются в качестве доказательств американскими[3], канадскими[4],

---

[1] С деталями функционирования данного сервиса и существующими техническими ограничениями можно ознакомиться на официальном сайте в разделе «Часто задаваемые вопросы». Internet Archive Frequently Asked Questions. http://archive.org/about/faqs.php

[2] С полным перечнем участников указанного Консорциума можно ознакомиться его на официальном интернет-сайте*: http://www.netpreserve.org/about-us/members*

[3] См., например: Telewizja Polska USA Inc. v. EchoStar Satellite Corp. (N.D. Ill, 2004). В данном споре распечатки из интернет-архива *Wayback Machine* были использованы в качестве доказательства использования компанией *Telewizja Polska* на своем интернет-сайте товарного знака, принадлежащего компании *Echostar*, после истечения срока действия лицензионного соглашения.

[4] ITV Technologies Inc. v. WIC Television Ltd, 2003 FC 1056 (CanLII). В данном решении судья указал, что, «используя сервис *Wayback Machine*, стороны смогли получить доступ к веб-сайтам в том виде, в каком они существовали в определенный момент времени. Я признаю, что веб-сайт *www.archive.org* является достоверным и что Суд может опираться на его цифровую библиотеку как на точное отображение веб-сайтов в сети Интернет по состоянию на определенный момент времени». Впоследствии на данную позицию неоднократно ссылались иные суды: Candrug Health Solutions Inc. v. Thorkelson,

немецкими[1] судами. Использование данных сервиса *Wayback Machine* является сложившейся практикой при рассмотрении споров, связанных с доменными именами, в рамках Единого регламента рассмотрения споров о доменных именах (*The Uniform Domain Names Dispute Resolution Policy*, *UDRP*)[2].

Примечательно, что распечатки из интернет-архива *Wayback Machine* вполне охотно принимаются и отечественными арбитражными судами.

В частности, они были использованы в качестве доказательства факта исполнения договора на разработку и поддержку веб-сайта[3] или, напротив, в качестве доказательства отсутствия факта такого исполнения[4], поскольку данные интернет-архива позволяют проследить динамику изменений, происходящих на веб-сайте применительно к определенным датам.

Достаточно часто данные из интернет-архива *Wayback Machine* были использованы сторонами арбитражного процесса в спорах, связанных с нарушением товарных знаков. В частности, в качестве доказательства, подтверждающего факт использования товарного знака правообладателем (корпорацией *Mozilla*)[5]; факт использования доменного имени для осуществления деятельности, аналогичной той, в отношении которой был зарегистрирован товарный знак[6].

Приведенные судебные решения позволяют сделать вывод, что как зарубежные суды, так и отечественные арбитражные суды в об-

2007 FC 411 (CanLII); St. Joseph Media Inc. v. Starwood Hotels & Resorts Worldwide, Inc., 2010 TMOB 188 (CanLII).

[1] Oberlandesgericht Karlsruhe, Urteil 6 U 1/02 vom 12.02.2003. В данном деле суд принял в качестве доказательства в споре о нарушении товарного знака регистрацией доменного имени предоставленную ответчиком информацию из интернет-архива (*Webseitenarchiv*) за период 1996–2000 гг., демонстрировавшую, что зарегистрированное доменное имя в данный период фактически не использовалось.

[2] База данных решений Арбитражного центра при Всемирной организации интеллектуальной собственности содержит более 400 ссылок на использование сервиса *Wayback Machine* при рассмотрении соответствующего спора. http://www.wipo.int/amc/en/domains/search/fulltext_decisions.jsp?q=-Wayback+Machine&start=20

[3] Постановление Девятого арбитражного апелляционного суда от 7 августа 2008 г. по делу № А40-985/08-112-4.

[4] Решение арбитражного суда Ульяновской области от 5 марта 2013 г. по делу № А72-9996/2012. В аналогичных целях материалы из архива *Wayback Machine* были использованы и в деле А40-19689/13, рассмотренном Арбитражным судом г. Москвы 24 июня 2013 г.

[5] Решение Арбитражного суда г. Москвы от 14 сентября 2012 г. по делу № А40-8334/12.

[6] Решение Арбитражного суда г. Москвы от 11 июля 2013 г. по делу № А40-26695/13.

щем и целом рассматривают данные, полученные из архива *Wayback Machine*, в качестве возможных доказательств по делу, подлежащих оценке наряду с другими доказательствами. Использование таких распечаток, желательно предварительно заверенных нотариусом, как минимум может повлечь перераспределение бремени доказывания: другая сторона будет вынуждена доказывать их недостоверность, приводя необходимые доказательства этого.

В принципе нет никаких препятствий для использования данных из интернет-архива *Wayback Machine* в качестве доказательства по диффамационным спорам, спорам о нарушении авторских прав, потребительским спорам и во всех иных случаях, когда необходимо обратиться к информации, которая однажды была размещена на общедоступном веб-сайте.

Глава 5. Веб-сайт как основной инструмент электронной коммерции

§ 1. Понятие веб-сайта. Его правовая природа и особенности охраны

Ведение систематической коммерческой деятельности в сети Интернет невозможно без создания веб-сайта (*web* – дословный пер. с англ. – паутина; *site* – дословный пер. с англ. – местоположение; *web site* – местоположение в Интернете). Как отмечалось ранее, в зависимости от используемой субъектом электронной коммерции бизнес-модели они могут как носить информационно-рекламный характер, так и содержать в себе функционал интернет-магазинов, принимая и обрабатывая заказы на товары и услуги в онлайн-режиме, а в ряде случаев и исполняя их (продажа цифрового контента, различного рода сетевых услуг и пр.). С определенной долей условности можно говорить о том, что в современных условиях веб-сайт выполняет функцию представительства лица в сети Интернет[1].

Под веб-сайтом обычно понимают совокупность электронных документов (файлов), объединенных под одним адресом (доменным именем или *IP*-адресом). При этом веб-сайт является сложным объектом, состоящим из различных компонентов. К ним относится: 1) «движок» веб-сайта (система управления содержимым сайта), представляющий собой компьютерную программу, предоставляющую инструменты для добавления, редактирования, удаления информации на сайте; 2) дизайн веб-сайта, включающий в себя логическую структуру веб-страниц, эскизы главной и типовых страниц, а также пользовательский интерфейс (расположение меню, навигация сайта, обратная связь с пользователем и т.п.); 3) текст веб-страниц, изложенный с использованием специального языка – *HTML* (*HyperText Markup Language*), который впоследствии

[1] Интересно, что именно эту представительскую функцию ЦБ РФ выставил в качестве основной при формулировании дефиниции веб-сайта. В Письме от 7 мая 2003 г. № 70-Т «О рекомендациях по информационному содержанию и организации *web*-сайтов кредитных организаций» *web*-сайт был определен как «совокупность информационно-технических средств, обеспечивающих представительство в сети Интернет».

интерпретируется браузером, выстраивающим визуальное отображение веб-страницы на компьютере пользователя[1]; 4) информационное наполнение веб-сайта в виде текстов, графических изображений, музыки и иных объектов, в том числе доступных для скачивания.

Долгое время в российском законодательстве отсутствовала легальная дефиниция понятия «веб-сайт», что спровоцировало шквал дискуссий на тему правовой природы веб-сайта[2]. Всю совокупность точек зрения по данному вопросу, существовавших до введения в действие части четвертой ГК РФ, можно свести к следующим трем[3]:

1) веб-сайт является разновидностью компьютерной программы. Как известно, под компьютерной программой понимается представленная в объективной форме совокупность данных и команд, предназначенных для функционирования ЭВМ и других компьютерных устройств, в целях получения определенного результата (ст. 1261 ГК РФ). По мнению некоторых юристов, поскольку команды языка разметки *HTML* интерпретируются специальной программой – браузером, гипертекстовый документ потенциально подпадает под вышеуказанное определение компьютерной программы;

2) веб-сайт является разновидностью базы данных. Под базой данных понимается представленная в объективной форме совокупность самостоятельных материалов (статей, расчетов, нормативных актов, судебных решений и иных подобных материалов), систематизированных таким образом, чтобы эти материалы могли быть найдены и обработаны с помощью ЭВМ (п. 2 ст. 1260 ГК РФ)[4]. Поскольку со-

---

[1] *HTML*-язык является важным объединяющим элементом, обеспечивающим единство веб-сайта и его иерархическую структуру. *HTML*-язык позволяет реализовывать так называемые гиперссылки – выделенные графически фрагменты *HTML*-документа, указывающие на другую веб-страницу или объект, который может быть расположен в Интернете.

[2] Определение правовой природы того или иного технического или социального явления, нередко сопровождающееся выработкой его легальной дефиниции, представляет собой средства, посредством которых право переводит такие явления на собственный язык, вводя их в определенную систему правовых координат. Поэтому в данной работе достаточно много внимания уделяется вопросам правовой квалификации того или иного явления из сферы электронной коммерции, принимая во внимание, что данный вопрос является отправной точкой любого последующего обсуждения такого явления в правовой плоскости. Да и в условиях динамично изменяющегося законодательства и практики в указанной сфере анализ данных вопросов будет поддерживать актуальность книги в течение гораздо более продолжительного времени.

[3] *Близнец И., Робинов А.* Правовой статус гипертекстовых документов и целесообразность их регистрации в Роспатенте // Интеллектуальная собственность. Авторское право и смежные права. М., 2002. № 7.

[4] Следует отметить отличительную особенность российского подхода к регулированию баз данных, ограничивающего данное понятие лишь электронными базами

вокупность веб-страниц систематизирована определенным образом посредством гиперссылок, это позволяет говорить некоторым авторам о возможности отнесения веб-сайтов к базам данных и их регистрации в качестве таковых[1]. В литературе, правда, указывалось на принципиальное различие между базами данных и веб-сайтом, выражающееся в способе систематизации материалов. В базе данных систематизация осуществляется со строго определенным числом материалов, в рамках технически обусловленных границ. Веб-сайт не является замкнутой системой, систематизации в рамках него подвергаются не только материалы, размещенные непосредственно на нем, но и материалы, размещенные на других сайтах, что становится возможным за счет механизма гиперссылок[2];

3) веб-сайт является объектом особого рода *sui generis*, состоящим из различных видов информации[3]. Или в ином варианте: «особой формой организации электронной информации»[4].

Представляется, что вряд ли все же можно квалифицировать веб-сайт в качестве компьютерной программы. Несмотря на то что при создании и функционировании веб-сайта используется *HTML*-язык, его нельзя отнести к языкам программирования[5]. Он является языком разметки гипертекста. В него не входят основные элементы всех языков программирования (функции, циклы, переменные и пр.). В противном случае любой файл, существующий в цифровой форме, придется квалифицировать в качестве компьютерной программы, поскольку он так или иначе содержит структурированные данные, которые позво-

данных, т.е. предполагающими применение компьютера для своего функционирования. Европейский подход в данном случае несколько шире и включает в себя в том числе и классические, «бумажные», базы данных. См.: Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the Legal Protection of Databases (ст. 1 (2)).

[1] *Петровский С.* Защита прав автора сайта // Российская юстиция. 2001. № 1. Наиболее верной с точки зрения законодательства квалификацию веб-сайта в качестве базы данных считает и А. Серго, признавая возможным, впрочем, и отнесение его к категории программ для ЭВМ. См.: *Серго А.* Неопределенный сайт // эж-Юрист. 2004. № 1; *Он же*. Интернет и право. М., 2003. С. 93. О целесообразности квалификации веб-сайта в качестве базы данных утверждает и В.О. Калятин (*Калятин В.О.* Право в сфере Интернета. С. 94–95).

[2] См.: *Басманова Е.С.* Интернет-сайт как объект имущественных прав: дис. ... канд. юрид. наук. М., 2010. С. 110.

[3] Перспективность подобного подхода высказывается, в частности, П.В. Барабыкиным. См.: *Барабыкин П.В.* Гражданско-правовое регулирование создания и использования сайтов сети Интернет: дис. ... канд. юрид. наук. СПб., 2005. С. 33–34.

[4] *Гулак А.С.* Место сайта сети Интернет в системе объектов гражданских правоотношений // Вестник Удмуртского университета. 2006. № 6.

[5] *Graham Smith*. Op. cit. P. 760.

ляют достигать определенного результата. Но необходимо разделять собственно компьютерную программу, которая интерпретирует файл (аудиоплеер, текстовый редактор, браузер), и сам интерпретируемый файл, который содержит данные, но не является компьютерной программой. В связи с этим сложно согласиться с Е.С. Басмановой в том, что гипертекстовые страницы веб-сайта являются программой для ЭВМ и могут быть зарегистрированы в качестве таковой[1].

Что касается третьего варианта квалификации, то она является весьма привлекательной на первый взгляд. Всегда заманчива перспектива решить проблему квалификации какого-либо явления, уклонившись от нее путем навешивания ярлыка о ее особом роде. Несмотря на то что соответствующая позиция, безусловно, имеет право на существование, она обычно мало что дает с практической точки зрения, поскольку не позволяет решить главный вопрос, ради которого осуществляется квалификация, – определить применимые нормы. Тем не менее в качестве преимущества рассматриваемого подхода можно указать тот факт, что он позволяет по крайней мере не ограничивать составляющие веб-сайта исключительно рамками авторского права и охватывать собой иные объекты интеллектуальной собственности, которые могут быть включены в него. Например, запатентованные методологии вроде *1-click ordering*, позволяющей совершать покупки в интернет-магазине совершением одного клика мышью[2]. К тому же не исключена возможность регистрации оригинального дизайна веб-сайта в качестве промышленного образца (ст. 1352 ГК РФ). Как отмечается, такая практика существует в Роспатенте[3].

Квалификация веб-сайта в качестве базы данных позволяет обеспечить его дополнительной правовой защитой, что в условиях закрытого перечня охраняемых объектов интеллектуальной собственности (ст. 1225 ГК РФ) является весьма актуальным[4]. В случае установления факта наличия существенных финансовых, материальных, организационных или иных затрат, понесенных при создании веб-сайта

---

[1] См.: *Басманова Е.С.* Указ. соч. С. 61.

[2] В США патент на данный метод принадлежит *Amazon Com Inc*. (US5960411). Право на его использование было лицензировано, в частности, компанией *Apple Inc*. для использования в *iTunes Store* и *App Store*.

[3] См.: *Басманова Е.С.* Указ. соч. С. 58.

[4] Исчерпывающий характер перечня охраняемых объектов интеллектуальной собственности, содержащийся в ст. 1225 ГК РФ, был подчеркнут в совместном постановлении пленумов ВАС и ВС РФ № 5/29 от 26 марта 2009 г. «О некоторых вопросах, возникших в связи с введением в действие части четвертой Гражданского кодекса Российской Федерации» (п. 9.1).

(презюмируемого при наличии не менее 10 000 информационных элементов в таком сайте), при квалификации последнего в виде базы данных появляется возможность ссылаться на наличие особого смежного права на веб-сайт. Суть данного права сводится к возможности контролировать перенос всего содержимого веб-сайта или существенной части составляющих его материалов на другой информационный носитель с использованием любых технических средств и в любой форме (ст. 1334 ГК РФ), что позволило бы квалифицировать полное или частичное копирование веб-сайта другим лицом в качестве нарушения смежного права.

Правда, судебная практика пошла по иному пути[1]. Вместо того чтобы причислить веб-сайт к разряду баз данных ввиду очевидной родственности данных категорий, обусловленной наличием систематизированности и компьютера как необходимого элемента для их существования, суды предпочли использовать понятие составного произведения, являющегося родовым по отношению к понятию «база данных».

Квалификацию веб-сайта в качестве составного произведения, если сайт представляет собой результат творческого труда по подбору или расположению материалов, предложил ВАС РФ. Было отмечено, что контент сайта представляет собой специальным образом подобранные и расположенные материалы (тексты, рисунки, фотографии, чертежи, аудиовизуальные произведения и т.д.), которые могут быть использованы с помощью компьютерной программы (компьютерного кода), являющейся элементом сайта. Как следствие, несанкционированное заимствование всего контента или его части при создании другого веб-сайта может рассматриваться как нарушение авторского права на составное произведение[2].

Так, например, нарушением может быть признано копирование описания товара, продаваемого на одном сайте, другим сайтом. В качестве примера можно привести дело, где ответчика обязали удалить с сайта *www.kniga.ru* скопированные с сайта *www.ozon.ru* изображения и описания книг[3]. Примечательно, что в данном деле суд провел аналогию между контентом веб-сайта и «витриной» интернет-магазина,

---

[1] Так, например, в решении Арбитражного суда Ростовской области от 12 февраля 2009 г. по делу № А53-21574/2008-С2-20 судом была высказана позиция относительно несоответствия веб-сайта легальной дефиниции базы данных.

[2] Постановление ВАС РФ от 22 апреля 2008 г. № 255/08. См. также: постановление ФАС Дальневосточного округа от 12 февраля 2013 г. № Ф03-1/2013.

[3] Постановление ФАС Московского округа от 21 июня 2011 г. № КГ-А40/5623-11.

включающей в себя созданные в результате творческого труда изображения и описания предлагаемого товара[1].

Для того чтобы требование о защите прав вследствие несанкционированного заимствования контента веб-сайта было удовлетворено, необходимо доказать а) наличие исключительного права на заимствованный контент, а также то, что он б) является охраноспособным, т.е. отвечает требованиям, предъявляемым к объектам авторского права.

Наличие исключительного права на контент может доказываться ссылками на то, что он был создан работниками истца в ходе исполнения их трудовых обязанностей (служебный характер соответствующих произведений – ст. 1295 ГК РФ). В таком случае необходимо быть готовым к предъявлению трудовых договоров, содержащих описание трудовых обязанностей работника, в числе которых фигурирует создание соответствующих произведений, либо содержащих отсылку к должностным инструкциям (локальный нормативный акт организации), которая бы содержала подобную обязанность. Помимо этого, наличие исключительного права на контент может обосновываться наличием гражданско-правовых договоров, по которым исключительное право было отчуждено истцу или была предоставлена исключительная лицензия. К таким договорам может, в частности, относиться договор на создание веб-сайта, в котором содержатся соответствующие элементы договоров на отчуждение исключительного права или лицензионного договора. В принципе, не исключена ссылка на приобретение исключительного права на контент в порядке универсального правопреемства: в порядке наследования или по результатам произошедшей реорганизации юридического лица. Правда, в таком случае может возникнуть необходимость предъявить не только доказательства произошедшего правопреемства (свидетельство о праве на наследство или передаточный акт), но и доказательства принадлежности исключительного права правопредшественнику.

Охраноспособность заимствованного ответчиком контента является еще одним условием защиты прав владельца сайта. Далеко не все, что размещается на веб-сайте, может быть признано отвечающим данному требованию. Как известно, основным условием охраноспособности объекта средствами авторского права является создание его творческим

[1] Решение Арбитражного суда г. Москвы от 20 октября 2010 г. по делу № А40-35771/10-26-279. В связи с этим возникает интересный вопрос о возможности применения положений п. 2 ст. 494 ГК РФ о признании выставления товара на витрине публичной офертой к отношениям, связанным с продажей товара через веб-сайт. Подробнее данный вопрос будет рассмотрен далее.

трудом (ст. 1228, 1257 ГК РФ). При этом законодательство не содержит критериев такого творческого труда[1]. На наш взгляд, о наличии творческого подхода к созданию того или иного объекта можно говорить в том случае, когда он не является следствием прямого копирования другого произведения и при его создании у автора была возможность выбора того или иного выражения своей идеи. Именно в наличии свободы выбора и проявляется творческое начало: творческий акт состоит не в создании чего-либо из ничего (*from scratch*), а в установлении новых связей между существующими компонентами знания.

Применительно к веб-сайтам вопрос о наличии у него отдельных элементов охраноспособности является весьма актуальным. Включение в состав веб-сайта многих элементов является следствием стандартизации и утилитарных соображений, что естественно, не позволяет говорить о наличии творчества в таких случаях. Так, в одном деле суд по результатам произведенного анализа текстов, приведенных на сайте истца и на сайте ответчика, пришел к выводу, что «содержание рубрик «преимущества», «как работаем», «типовые ситуации», «основные особенности нашей работы» носит исключительно информационный характер. В них сообщалось о концепциях, принципах, способах решения задач, стоящих перед исполнителем при оказании услуг. При этом сферы оказания этих услуг истцом и ответчиком идентичны. Тексты не отличались оригинальностью и, как было указано выше, согласно нормам гражданского законодательства авторские права не распространяются на идеи, концепции, принципы, методы, процессы, способы решения задач»[2].

Квалификация судами веб-сайта в качестве составного произведения является весьма разумным решением в условиях отсутствия специального правового режима в отношении веб-сайтов, учитывающего их комплексную природу. Правда, она годится в основном для целей

[1] Обзор мнений, существующих в доктрине по данному вопросу, см.: *Кашанин А.В.* Уровень требований к творческому характеру произведения в отечественном юридическом дискурсе // Законы России: опыт, анализ, практика. 2012. № 9; *Андреев Ю.Н.* Судебная защита исключительных прав: цивилистические аспекты: монография. М., 2011.

2 См.: постановление Девятого арбитражного апелляционного суда от 28 мая 2012 г. № 09АП-10525/2012-ГК по делу № А40-83853/11-51-730, оставленное в силе постановлением ФАС Московского округа от 10 сентября 2012 г. по делу № А40-83853/11-51-730. См. также: постановление ФАС Северо-Западного округа от 23 марта 2009 г. по делу № А56-11416/2008. В данном деле суд указал, что информация, размещенная ответчиком на своем сайте, содержит только общие сведения о характере оказываемых услуг в области аудита, «не обладает признаками оригинальности», «не отличается творчеством и новизной», что, по мнению суда, говорит об отсутствии «признаков, позволяющих отнести эти тексты к результатам творческой деятельности».

защиты нарушенных прав и не может обеспечить адекватный оборот таких объектов: передать права на веб-сайт, включающий в себя множество различных компонентов с разным правовым режимом, становится не так просто. Велик риск что-нибудь упустить из виду.

В связи с этим вполне понятными являются попытки определить веб-сайт посредством каких-либо иных категорий, которые появились после введения в действие части четвертой ГК РФ. В частности, посредством категорий «сложный объект» и «мультимедийный продукт».

Как известно, одной из новелл части четвертой ГК РФ явилась ст. 1240, посвященная использованию результата интеллектуальной деятельности в составе сложного объекта. Первоначально имея перед собой пример в виде кинематографических произведений[1], понятие сложного объекта ныне включает в себя аудиовизуальные произведения, театрально-зрелищные представления, мультимедийные продукты и единую технологию. Указанные объекты объединяет то, что, с одной стороны, они представляют собой единое целое (единый объект), а с другой стороны, имеют сложный состав (структуру), образуемый из совокупности разнородных результатов интеллектуальной деятельности[2].

Так, кинофильм не может существовать без сценария, современная компьютерная игра – без звукового сопровождения и пр. Характерной особенностью правового режима сложного объекта является наличие особой фигуры – организатора его создания, который, несмотря на свое «нетворческое» участие в процессе создания, приобретает права использования объектов, входящих в состав такого сложного объекта, на особых условиях, обеспечивающих общий правовой режим всех компонентов, облегчающий последующую коммерциализацию сложного объекта. Как отмечалось ранее, веб-сайт включает в себя ряд различных компонентов: программную основу («движок»), дизайн, *HTML*-текст веб-страниц, разнообразное информационное наполнение. Причем данные компоненты обладают особой сложной «многослойной» взимосвязью: в отсутствие одного из них рабочего веб-сайта не получится. Поэтому веб-сайт вполне может быть отнесен

[1] См.: *Дозорцев В.А.* Право на фильм как сложное многослойное произведение // Интеллектуальные права: Понятие. Система. Задачи кодификации: сборник статей. М., 2005. С. 144–179; *Он же*. Право. Новая эра в охране исключительных прав. Система права и система законодательства // Интеллектуальные права: Понятие. Система. Задачи кодификации: сборник статей. М., 2005. С. 11–31.

[2] Заключение Исследовательского центра частного права по вопросам толкования и возможного применения отдельных положений части четвертой ГК РФ // Вестник гражданского права. 2007. № 3. Т. 7. С. 124.

к категории сложного объекта[1]. Такая квалификация позволяет воспользоваться специальными положениями, содержащимися в ст. 1240 ГК РФ: 1) презумпцией приобретения заказчиком прав на результаты интеллектуальной деятельности, входящие в состав сложного объекта, на основании договора об отчуждении исключительного права; 2) презумпцией всемирного и «вечного» (ограниченного сроком действия исключительного права) характера лицензии, предоставляемой на такие объекты (если права на них не были приобретены на основании договора об отчуждении прав); 3) недействительностью условий лицензионных договоров, ограничивающих условия последующего использования результатов интеллектуальной деятельности, входящих в состав сложного объекта.

Правда, квалификация веб-сайта в качестве сложного объекта может натолкнуться на то, что он прямо не поименован в качестве такового в ст. 1240 ГК РФ, а перечень объектов, которые могут быть квалифицированы в качестве сложных, может быть интерпретирован в качестве закрытого[2]. Отсюда попытки квалификации веб-сайта в качестве мультимедийного продукта[3]. Учитывая отсутствие легальной дефиниции указанной категории, такая квалификация представляется вполне корректной при наличии в большинстве современных сайтов признаков интерактивности (т.е. направленности продукта на активное взаимодействие с пользователем в процессе его использования), традиционно считающихся одними из ключевых критериев мультимедийного продукта[4].

В настоящее время соответствующее определение содержится в Законе об информации, согласно которому под сайтом в сети Интернет понимается совокупность программ для электронных вычислительных машин и иной информации, содержащейся в информационной

---

[1] К данному выводу приходит, в частности, Е.С. Басманова. См.: *Басманова Е.С.* Указ. соч. С. 95.

[2] Мнения о том, что представленный в п. 1 ст. 1240 ГК РФ перечень видов сложных объектов является исчерпывающим, придерживается коллектив авторов следующей книги: Комментарий к Гражданскому кодексу Российской Федерации, части четвертой (постатейный) / под ред. Л.А. Трахтенгерц. М., 2009. С. 64 (автор комментария – Е.А. Павлова).

[3] См.: Заключение Исследовательского центра частного права по вопросам толкования и возможного применения отдельных положений части четвертой ГК РФ // Вестник гражданского права. 2007. № 3. Т. 7; *Котенко Е.С.* Мультимедийный продукт как объект авторских прав: дис. ... канд. юрид. наук. М., 2012. С. 98.

[4] *Stamatoudi I.A.* Copyright and Multimedia Products: A Comparative Analysis. Cambridge University Press. 2003. P. 24; *Mille A.* The legal status of multimedia works // Copyright bulletin. Vol. 31. No 2. 1997. P. 26; Sega Enterprises Lid v. Galaxy Electronics Pty Ltd 35 IPR 161 [1997].

системе, доступ к которой обеспечивается посредством информационно-телекоммуникационной сети Интернет по доменным именам и (или) по сетевым адресам, позволяющим идентифицировать сайты в сети Интернет. Данная дефиниция была введена тем же Федеральным законом, который ввел реестр сайтов, содержащих вредную информацию, доступ к которым ограничивается в установленном законом порядке[1]. Очевидно, что первоочередной целью данной дефиниции является «обслуживание» потребностей данного Закона, в силу чего она базируется преимущественно на технических аспектах веб-сайта. Его гражданско-правовая природа в силу указанных причин не нашла своего адекватного отражения в данной дефиниции, поэтому вряд ли она может помочь владельцам сайта в защите своих прав на него, ее цель состоит скорее в обратном – в реализации механизма защиты прав, нарушение которых, по мнению законодателя, осуществляется посредством таких веб-сайтов.

Гражданско-правовая природа явления лучше всего может быть прояснена самим ГК РФ. Не случайно, что в проекте изменений в ГК РФ предложено дополнить п. 2 ст. 1260 ГК РФ абз. 3 следующего содержания: «Интернет-сайтом является представленная в объективной форме совокупность самостоятельных материалов, систематизированных таким образом, чтобы эти материалы могли быть размещены в сети Интернет». Правда, при этом не указывается, какие именно материалы могут составлять такую совокупность, что отличает данную дефиницию от определения базы данных, где такая конкретизация содержится («...статей, расчетов, нормативных актов, судебных решений и иных подобных материалов»). Помимо введения указанной дефиниции проектом предлагается дополнить ст. 1240 ГК РФ прямым указанием на интернет-сайт в качестве одного из видов сложного объекта. Таким образом, интернет-сайт получит одновременно и статус составного произведения, который за ним признается существующей судебной практикой, но с самостоятельной дефиницией, и статус сложного произведения, который в настоящее время может быть выведен только косвенно из понятия мультимедийного продукта.

Данный подход вызвал определенную критику в литературе как противоречивый, поскольку составные и сложные объекты имеют разный правовой режим и неэффективный ввиду того, что правовой

[1] Федеральный закон от 28 июля 2012 г. № 139-ФЗ «О внесении изменений в Федеральный закон «О защите детей от информации, причиняющей вред их здоровью и развитию» и отдельные законодательные акты Российской Федерации» (далее – Закон о внесении изменений в Закон о защите детей от информации).

статус объекта оказывается «висящим между двух стульев»[1]. Представляется, что квалификация объекта в качестве составного или сложного не является взаимоисключающей. Положения ст. 1240 ГК РФ не содержат перечня результатов интеллектуальной деятельности, которые могут входить в состав сложного объекта. Поэтому ничто не мешает выступить в качестве компонента сложного объекта составному произведению. К тому же положения о сложном объекте и о составном произведении имеют несколько разную сферу действия. Нормы ст. 1240 ГК РФ ориентированы на регламентацию *внутренних отношений* между разными лицами, вовлеченными в процесс создания мультимедийного продукта, и организатором данного процесса. Нормы о составном произведении определяют условия охраноспособности совершенного подбора и расположения материала, что больше ориентировано *на внешние отношения*, в рамках которых осуществляется использование такого продукта третьими лицами, а также защита от его несанкционированного использования.

Так что одновременное придание веб-сайту статуса сложного объекта и составного произведения с самостоятельной дефиницией можно только всячески приветствовать как способствующее внесению бóльшей определенности в его правовой статус. Статус сложного объекта позволит облегчить концентрацию прав на различные составные части веб-сайта у лица, организовавшего его создание (как правило, заказчика по договору на разработку веб-сайта), а вместе с ней и его последующий оборот. Статус составного произведения позволяет обеспечить защиту такому компоненту веб-сайта, как дизайн-макет, который может включать в себя оригинальное расположение различных материалов и интерфейс, тем самым предоставив защиту от копирования такого дизайна полностью или в части иными лицами.

В завершение рассмотрения вопроса о гражданско-правовой природе веб-сайта необходимо несколько слов сказать о возможности квалификации оного в качестве средства массовой информации. Данный вопрос весьма активно обсуждался в течение длительного времени. В рамках этой работы не хочется вдаваться в подробности данной дискуссии[2], учитывая, что она во многом устарела с принятием в 2011 г.

[1] *Котенко Е.С.* Указ. соч. С. 95.

[2] Подробнее см., например: *Петровский С.В.* Сайт – иное СМИ: коллизии права // Журнал российского права. 2001. № 2; *Наумов В.Б.* Право и Интернет: Очерки теории и практики. С. 68–95; *Серго А.* Интернет и право. С. 101–111; *Калятин В.О.* Право в сфере Интернета. С. 177–188; Юридическое заключение по вопросу о правовой природе сайтов в сети Интернет (подготовлено кафедрой ЮНЕСКО) // Информационное право. 2007. № 1.

поправок в Закон РФ «О средствах массовой информации» (далее – Закон о СМИ)[1]. Данные поправки внесли в Закон определение сетевого издания, под которым понимается «сайт в информационно-телекоммуникационной сети Интернет, зарегистрированный в качестве средства массовой информации в соответствии с настоящим Законом». При этом, как указано в ст. 8 данного Закона, «сайт в информационно-телекоммуникационной сети Интернет может быть зарегистрирован как сетевое издание в соответствии с настоящим Законом. Сайт в информационно-телекоммуникационной сети Интернет, не зарегистрированный в качестве средства массовой информации, средством массовой информации не является». Таким образом, веб-сайт может являться СМИ в случае осуществления его регистрации в качестве такового *в добровольном порядке*. Получение статуса СМИ влечет определенные преимущества, в частности распространение норм о недопустимости цензуры, возможность аккредитации на мероприятия или получение информации от властей. Однако одновременно появляется и ряд обязанностей. Например, обязанность указания выходных данных СМИ (зарегистрировавший его орган и регистрационный номер), а также ответственность за комментарии, оставляемые пользователями такого сетевого СМИ. Если на веб-сайте, зарегистрированном в качестве средства массовой информации, комментарии читателей размещаются без предварительного редактирования (например, на форуме), то в отношении содержания этих комментариев применяются положения Закона о СМИ для авторских произведений, идущих в эфир без предварительной записи. В случае поступления обращения уполномоченного государственного органа, установившего, что размещенные комментарии являются злоупотреблением свободой массовой информации, редакция веб-сайта вправе удалить их с сайта либо отредактировать. Если этого не будет сделано, то редакция сетевого СМИ может быть привлечена к ответственности[2]. Таким образом, вопрос о целесообразности регистрации веб-сайта в качестве СМИ должен решаться путем тщательного взвешивания всех плюсов и минусов такого шага.

Для того чтобы веб-сайт стал частью сети Интернет и был доступен ее пользователям, обычно необходимо пройти три основных этапа: 1) разработка веб-сайта; 2) заключение договора с провайдером хос-

[1] См.: Федеральный закон от 14 июня 2011 г. № 142-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации в связи с совершенствованием правового регулирования в сфере средств массовой информации».

[2] Пункт 23 постановления пленума ВС РФ от 15 июня 2010 г. № 16 «О практике применения судами Закона Российской Федерации «О средствах массовой информации»».

тинга; 3) выбор и регистрация доменного имени[1]. Рассмотрим данные этапы подробнее.

§ 2. Разработка веб-сайта

Приведенные ранее положения, касающиеся комплексной структуры веб-сайта, с достаточной очевидностью свидетельствуют о том, что его создание требует немало времени, а также наличия специальных познаний в этой области. В связи с этим, как правило, веб-сайты создаются привлеченными специалистами на основе особых соглашений – договоров на разработку веб-сайта. В судебной практике и доктрине такие договоры квалифицируются по-разному: 1) как договоры подряда[2]; 2) договоры возмездного оказания услуг[3]; 3) договоры авторского заказа[4]. Встречается также и квалификация данного договора в качестве смешанного, с элементами договора подряда и договора возмездного оказания услуг[5].

Как видно, квалификация договора на разработку веб-сайта в качестве договора подрядного типа является превалирующей в судебной практике. Выделяется она и в отечественной доктрине[6]. Такой подход видится наиболее адекватным. Во-первых, создание веб-сайта вполне укладывается в рамки определения договора подряда, содержащегося в ст. 702 ГК РФ: «По договору подряда одна сторона (подрядчик) обязуется выполнить по заданию другой стороны (заказчика) определенную работу и сдать ее результат заказчику, а заказчик обязуется принять результат работы и оплатить его». Веб-сайт создается по заданию заказчика, представляет собой отделимый от личности исполнителя результат, подлежащий сдаче заказчику. К тому же положения гл. 37 ГК РФ о договоре подряда содержат наиболее детальное регулирование

---

[1] *Klosek J.* The Legal Guide to E-Business. Westport, Connecticut, London, 2003. P. 10.

[2] См., например, постановления Тринадцатого арбитражного апелляционного суда от 3 декабря 2009 г. по делу № А56-13527/2009; ФАС Северо-Западного округа от 7 июня 2011 г. по делу № А56-4382/2010; Девятого арбитражного апелляционного суда от 29 апреля 2013 г. № 09АП-12471/2013-ГК по делу № А40-148075/12-12-684; ФАС Волго-Вятского округа от 9 марта 2010 г. № А17-2284/2009.

[3] Постановления Одиннадцатого арбитражного апелляционного суда от 6 октября 2011 г. по делу № А55-2984/2011; Седьмого арбитражного апелляционного суда от 16 июня 2010 г. № 07АП-2156/10 по делу № А03-11831/2009.

[4] Постановление Шестого арбитражного апелляционного суда от 20 ноября 2012 г. № 06АП-5030/2012 по делу № А73-4956/2012.

[5] Постановление ФАС Уральского округа от 22 апреля 2010 г. № Ф09-3004/10-С2 по делу № А76-20390/2009-2-856.

[6] *Калятин В.О.* Право в сфере Интернета. С. 96; *Барабыкин П.В.* Указ. соч. С. 72.

вопросов, связанных с процессом создания определенного результата по заданию заказчика, его сдачи-приемки, распределения рисков необходимости проведения дополнительных работ, ответственности за недостатки и пр.

Примечательно, что даже те суды, которые квалифицируют отношения по созданию веб-сайта в виде возмездного оказания услуг (обычно следуя терминологии, использованной в договоре), применяют в субсидиарном порядке нормы о договоре подряда, руководствуясь положениями ст. 783 ГК РФ. Аналогичные возможности открываются и при квалификации договора на разработку веб-сайта в качестве смешанного с элементами договора подряда и договора возмездного оказания услуг, только в таком случае нормы о договоре подряда могут применяться напрямую, а не в субсидиарном порядке (п. 3 ст. 421 ГК РФ). Представляется, что целесообразнее сразу называть вещи своими именами и квалифицировать соответствующий договор в качестве подряда, избежав «окольных» путей, направленных на применение положений о нем.

Сильное желание одной из сторон квалифицировать данные отношения в виде возмездного оказания услуг в большинстве случаев может быть объяснено лишь возможностью применения ст. 782 ГК РФ, предоставляющей безусловное право на одностороннее расторжение договора, в то время как схожие положения ст. 717 ГК РФ допускают регламентацию данного вопроса в договорном порядке и по своим финансовым последствиям менее выгодны заказчику (ср.: возмещение фактически понесенных расходов по ст. 782 ГК РФ и цену договора пропорционально выполненным работам с возможностью взыскания убытков). Однако вряд ли конъюнктурные соображения одной из сторон могут оказывать решающее влияние на квалификацию договора. Как известно, ключевыми признаками услуги, отличающими ее от работы, являются неотделимость ее результата от процесса работы[1], а также нематериальный характер[2]. К тому же, как указал Конституционный Суд РФ, предмет договора возмездного оказания услуг не включает в себя достижение результата, ради которого он заключается[3], что также

[1] *Романец Ю.В.* Система договоров в гражданском праве России. М., 2001. С. 369.

[2] См.: *Шешенин Е.Д.* Предмет обязательства по оказанию услуг // Сб. учен. тр. Свердловск, 1964. Вып. 3. С. 177; *Иоффе О.С.* Обязательственное право. М., 1975. С. 419.

[3] Постановление Конституционного Суда РФ от 23 января 2007 г. № 1-П «По делу о проверке конституционности положений пункта 1 статьи 779 и пункта 1 статьи 781 Гражданского кодекса Российской Федерации в связи с жалобами общества с ограниченной ответственностью «Агентство корпоративной безопасности» и гражданина В.В. Макеева» // Вестник Конституционного Суда РФ. 2007. № 1. Можно не соглашаться

формально не позволяет использовать нормы о договоре возмездного оказания услуг для регулирования отношений, возникающих в связи с созданием веб-сайта.

Что же касается возможной применимости конструкции авторского договора к отношениям по разработке веб-сайта, то здесь необходимо сказать следующее. С одной стороны, данная конструкция вроде бы специально предназначена для регулирования отношений, связанных с созданием объектов авторского права, к числу которых можно отнести и веб-сайт. В соответствии со ст. 1288 ГК РФ по договору авторского заказа одна сторона (автор) обязуется по заказу другой стороны (заказчика) создать обусловленное договором произведение науки, литературы или искусства на материальном носителе или в иной форме. Однако, с другой стороны, данный договор характеризуется специальным субъектным составом – выступлением в качестве исполнителя *непосредственно автора* создаваемого объекта. Таким образом, положения о договоре авторского заказа могут быть применены к отношениям по разработке веб-сайта только в том случае, если в качестве исполнителя по договору на разработку веб-сайта выступает *физическое лицо* или физические лица (верстальщик, дизайнер, программист); возможно применение специальной договорной конструкции – договора авторского заказа. В том случае, если исполнителем выступает юридическое лицо, конструкция договора авторского заказа неприменима.

Правовой режим договора авторского заказа имеет ряд отличий от договора подряда, обусловленных тем, что, во-первых, в качестве результата работ выступает результат творческой деятельности, а во-вторых, в качестве контрагента заказчика выступает сам автор произведения. К указанным отличиям относятся правило о льготном сроке (п. 2, 3 ст. 1289 ГК РФ) и ограниченная возмещением реального ущерба ответственность за неисполнение или ненадлежащее исполнение авторского договора (ст. 1290 ГК РФ). Однако следует подчеркнуть, что договор авторского заказа не содержит ряда полезных положений, которые наличествуют в нормах о договоре подряда и в отличие от договора возмездного оказания услуг не предусматривают возможность субсидиарного применения норм о договоре подряда. Поэтому в том случае, когда используется конструкция договора авторского заказа, необходимо достаточно детально прописывать положения, касающиеся встречных обязанностей заказчика, приемки результата, ответственности за скрытые недостатки, гарантий качества и пр. В противном

с выводами и аргументацией данного Постановления, но отрицать его наличие и возможное юридическое значение при анализе рассматриваемого вопроса было бы некорректно.

случае единственной возможностью восполнения пробелов нормами о договоре подряда будет их применение в порядке аналогии закона (ст. 6 ГК РФ), что весьма проблематично.

Таким образом, мы приходим к выводу о целесообразности квалификации договора на разработку веб-сайта именно в качестве договора подряда. Однако данный договор регламентирует лишь *процесс* создания веб-сайта. Существует еще один пласт отношений, которые требует тщательной регламентации при создании веб-сайта: распределение исключительных прав на него. Учитывая проблематичность квалификации веб-сайта в качестве базы данных и невозможность его квалификации в качестве компьютерной программы, специальные положения, посвященные распределению прав на них при создании по договору (ст. 1297 ГК РФ), потенциально неприменимы[1]. Регламентация данных вопросов в договоре повлечет включение в него элемента договора на отчуждение исключительного права или лицензионного договора[2] и квалификацию такого договора в качестве смешанного.

Рассмотрев вопрос о правовой квалификации договора на разработку веб-сайта, необходимо остановиться на описании его предмета. Как ранее уже неоднократно отмечалось, веб-сайт включает в себя множество компонентов, образующих единое целое. В связи с этим его разработка обычно распадается на несколько этапов.

На первом этапе осуществляется *проектирование* будущего сайта, которое заключается в создании дизайн-макета сайта, включающего в себя шаблоны главной страницы и всех остальных (так называемых типовых) страниц. От параметров дизайна сайта во многом зависит его эстетическая привлекательность и, как следствие, популярность среди пользователей, поэтому ему следует уделить особое внимание. Интуитивная понятность расположения элементов управления сайтом, приятная цветовая гамма, оригинальные решения – все это может служить важным элементом успеха в условиях высокой конкуренции, свойственной сфере электронной коммерции. На выходе дизайн-макет веб-сайта представляет собой совокупность файлов с изображениями.

[1] В проекте изменений в части четвертой ГК РФ эту ситуацию предполагается исправить, распространив положения ст. 1297 ГК РФ на случаи создания любых объектов авторского права на заказ.

[2] В принципе, аналогичная ситуация возникает и применительно к договору на создание компьютерной программы. Он также может быть квалифицирован в качестве смешанного, с элементами договора подряда и договора на распоряжение результатами интеллектуальной деятельности (см. подробнее: *Савельев А.И.* Лицензирование программного обеспечения в России. Законодательство и практика. С. 269–272).

На втором этапе осуществляется *верстка* – создание на базе разработанных шаблонов отдельных страниц с использованием *HTML*- и *CSS*-языков. *HTML* отвечает за логическую структуру страницы, *CSS* – за ее внешний вид. В результате создается код, который может быть интерпретирован браузером.

На третьем этапе осуществляется *программирование* – интеграция шаблона с системой управления контентом (*CMS*), что позволяет впоследствии существенно облегчить поддержку сайта и его обновление, подключение программных модулей и сервисов. По окончании данного этапа образуется целостная иерархическая структура сайта с необходимым функционалом (поиск, обратная связь и пр.), готовая к наполнению контентом.

На четвертом этапе осуществляется *наполнение сайта контентом* (изображениями, текстом, аудиовизуальными произведениями, музыкальными произведениями и т.п.). Данные объекты могут быть как специально созданными для данного сайта, так и ранее созданными без указанной цели.

В качестве финального этапа обычно фигурирует *тестирование сайта*. Тестирование осуществляется на предмет корректности отображения в различных браузерах, с различными размерами шрифтов и разрешениями экрана; корректности функционирования различного рода сценариев и модулей и т.д. Применительно к веб-сайтам, которые будут выступать платформой для интернет-магазинов, нередко проводятся так называемые стресс-тесты, в ходе которых проверяется возможность сайта работать под нагрузкой.

Детальное описание требований к веб-сайту и обусловленного им объема работ в совокупности с четкими и ясными результатами, достигаемыми на каждом этапе, и критериями их приемки являются наиболее важными положениями с точки зрения заказчика[1]. Техническое задание должно включать не только требования к визуальному отображению сайта, его функциональным характеристикам, но и параметры программно-аппаратного обеспечения, на котором веб-сайт должен работать. Во избежание споров рекомендуется в договоре указывать не только описание работ, производимых на каждом отдельно взятом этапе, но и конкретный результат, которым такие работы должны заканчиваться: графические файлы дизайн-макета сайта; файлы, содержащие верстку страниц сайта; программный код движка сайта; четкое и полное описание объектов, созданных разработчиком для информационного наполнения сайта. Такой подход позволит

[1] *Graham Smith*. Op. cit. P. 758.

внести прозрачность в процесс регламентации распределения исключительных прав на такие объекты между заказчиком и разработчиком, а также обеспечить единство веб-сайта как передаваемого объекта.

Следует отметить, что приведенная выше этапность разработки веб-сайта является скорее идеальной моделью и нередко на практике обрастает дополнительными этапами.

Так, разработчик веб-сайта нередко сам разрабатывает техническое задание, детально регламентирующее требования к веб-сайту. Это связано с тем, что заказчик обычно не обладает специальными познаниями в данной области, в связи с чем не может грамотно и относительно исчерпывающим образом сформулировать свои требования. В таком случае исполнитель разрабатывает техническое задание на основе так называемого брифа, в котором заказчик излагает свои пожелания относительно визуального представления и структуры сайта, иногда со ссылками на примеры сайтов конкурентов. При подготовке технического задания на создание веб-сайта самим исполнителем оно подлежит последующему утверждению заказчиком, после чего приобретет статус задания заказчика в контексте ст. 702 ГК РФ и станет основой для выполнения последующих работ по разработке веб-сайта.

К тому же, для того чтобы протестировать наполненный контентом веб-сайт, его необходимо опубликовать, т.е. поместить на хостинговую площадку. Однако, поскольку хостинг является самостоятельной услугой, нередко оказываемой иным лицом, нежели разработчик веб-сайта, он будет рассмотрен отдельно.

Учитывая, что договор на разработку веб-сайта по своей природе является договором подряда, к числу существенных условий помимо описания объема работ относится указание начального и конечного сроков, отсутствие которых может повлечь признание договора незаключенным[1].

Не менее важной является регламентация в договоре на разработку веб-сайта порядка распределения исключительных прав на объекты, выступающие его составными частями[2]. Здесь существуют различные варианты, наиболее предпочтительным из которых для заказчика является переход исключительных прав на такие объекты к нему. Это не только

[1] См.: п. 6 информационного письма Президиума ВАС РФ от 25 ноября 2008 г. № 127 «Обзор практики применения арбитражными судами статьи 10 Гражданского кодекса Российской Федерации». См. также: определения ВАС РФ от 30 мая 2012 г. № ВАС-6830/12 по делу № А04-1367/2011; от 25 июня 2010 г. № ВАС-7668/10 по делу № А27-9091/2009.

[2] *Kunze C.* Web Site Legal Issues // Santa Clara Computer & High Technology Law Journal. Vol. 14. 1998. P. 479–482; *Graham Smith.* Op. cit. P. 757.

позволяет облегчить возможную миграцию веб-сайта впоследствии, обеспечив высокую степень независимости от разработчика, но и повысить привлекательность веб-сайта для инвесторов в тех случаях, когда такой сайт является неотъемлемой частью успешного бизнеса в сети Интернет[1]. Но самое важное заключается в том, что веб-сайт динамичен по своей природе и требует периодических обновлений. Причем необходимость таких обновлений касается не только информационного наполнения (что и так очевидно), но и более фундаментальных компонентов веб-сайта в виде его движка и дизайна, необходимость обновления которых может быть вызвана постоянно меняющимися технологиями. Поскольку совершаемые обновления могут подпадать под понятие производного произведения[2], совершение подобных действий требует согласия правообладателя. Очевидно, что если правообладателем выступает то лицо, которое производит обновления, никаких проблем с получением отдельного согласия (лицензии) на совершение таких действий нет. В отсутствие у заказчика статуса правообладателя в отношении компонентов веб-сайта необходимо позаботиться о том, чтобы предоставленная от исполнителя лицензия помимо всего прочего включала право на переработку таких компонентов.

Разумеется, разработчик веб-сайта заинтересован в том, чтобы иметь возможность использования тех наработок, которые он сделал для заказчика, в своих будущих проектах[3]. Такие наработки могут иметь немалую ценность, составляя конкурентное преимущество разработчика и позволяя минимизировать затраты времени и средств путем использования проверенных решений. Указанные факторы обусловливают стремление разработчика веб-сайта сохранить за собой определенные права на такие наработки. Представляется, что в качестве неплохого компромисса может быть использовано решение, предложенное в ст. 1296 ГК РФ применительно к компьютерным программам и базам данных, созданным на заказ. Диспозитивные нормы данной статьи предусматривают принадлежность исключительного права на указанные объекты заказчику с сохранением за исполнителем возможности их использования для собственных нужд на условиях простой (неисключительной) лицензии в течение всего срока действия исключительного права[4].

---

[1] Как известно, чем прочнее права на объект, тем выше его цена.

[2] В соответствии с п. 2 ст. 1259 ГК РФ под производными произведениями понимаются произведения, представляющие собой переработку другого произведения.

[3] *Klosek J.* Op. cit. P. 12.

[4] Здесь, правда, могут возникнуть вопросы относительно толкования понятия «собственные нужды». Но, как представляется, оно является достаточно широким,

К сожалению, как отмечалось выше, положения ст. 1296 ГК РФ не могут применяться к договорам на разработку веб-сайта напрямую, поскольку данный объект не может быть квалифицирован в качестве компьютерной программы или базы данных, несмотря на некоторые функциональные сходства с ними. Но ничто не мешает включить аналогичные положения в договор на разработку веб-сайта в качестве решения, отражающего интересы обеих сторон.

В отсутствие в части четвертой ГК РФ каких-либо положений об ответственности за юридическую чистоту предоставляемых прав на результаты интеллектуальной деятельности целесообразно предусмотреть в договоре ответственность разработчика за то, что предоставляемые компоненты веб-сайта не нарушают исключительных прав третьих лиц. Необходимо предусмотреть обязательство разработчика при наличии таких претензий вступить в процесс на стороне заказчика[1] и сделать все возможное для его защиты от предъявленных требований, а в случае неблагоприятного исхода – компенсировать заказчику возникшие убытки и судебные издержки[2].

Предоставление таких гарантий может сопровождаться встречными обязанностями заказчика: 1) незамедлительным уведомлением разработчика о факте предъявления требования третьим лицом и 2) предоставлением разработчику контроля над ведением переговоров и (или) ведения

чтобы охватить ситуации использования результата интеллектуальной деятельности компанией в целях осуществления своего основного вида деятельности.

[1] С точки зрения российского процессуального права это означает вступление в процесс в качестве третьего лица без самостоятельных требований на стороне ответчика (ст. 51 АПК РФ, ст. 43 ГПК РФ). Такое лицо пользуется правами, предоставленными стороне, кроме права признать иск или заключить мировое соглашение, предъявить встречный иск.

[2] Соответствующие условия в практике англосаксонских стран обычно именуются *indemnification* и регламентируют ответственность одной стороны перед другой, которая возникает у такой другой стороны по отношению к третьим лицам вследствие действий первой стороны. См.: *Ward Classen*. Op. cit. P. 54. В контексте российского права подобные условия, как представляется, есть не что иное, как регламентация объема и порядка возмещения убытков, заранее определенных в договоре. Как правило, такие убытки представляют собой ответственность в порядке регресса. Указанный тип ответственности возникает, как отмечает М.Н. Малеина, «когда должник исполнил обязательство по возмещению вреда за непосредственного причинителя вреда и предъявил обратное требование (регресс) к этому нарушителю». Гражданское право. Часть первая: учебник / под ред. А.Г. Калпина, А.И. Масляева. 2-е изд., перераб. и доп. М., 2002. С. 524. Российскому законодательству известны положения, весьма похожие на *indemnification*. Речь идет о ст. 462 ГК РФ, в соответствии с которой «если третье лицо по основанию, возникшему до исполнения договора купли-продажи, предъявит к покупателю иск об изъятии товара, покупатель обязан привлечь продавца к участию в деле, а продавец обязан вступить в это дело на стороне покупателя».

судебного процесса с таким третьим лицом. Данные обязанности вполне объяснимы. Чем быстрее разработчик узнает о наличии такого требования и о субъекте, от которого оно исходит, тем больше возможностей будет у него для того, чтобы проанализировать его обоснованность, собрать необходимые доказательства и как следствие минимизировать возможные издержки. Второе условие также является логичным с учетом того факта, что разработчик принимает на себя обязательство возместить все убытки и судебные издержки, понесенные лицензиатом в связи с предъявленным требованием. Неумелое ведение лицензиатом переговоров или процесса может повлечь их значительное увеличение. К тому же существует риск того, что такое решение может создать нежелательный прецедент или иметь неблагоприятное преюдициальное значение при рассмотрения иных споров, в которые будет вовлечен разработчик.

Наконец, необходимо отметить, что, если программное обеспечение, используемое для системы управления контентом, не пишется разработчиком веб-сайта с нуля, а используется готовый программный продукт, заказчику необходимо позаботиться о получении лицензии на использование такой программы от его правообладателя. При этом, как представляется, целесообразно заключение прямого лицензионного договора между заказчиком и правообладателем, а не сублицензирование прав на использование программы через разработчика. Это связано с тем, что данная программа является одним из ключевых компонентов веб-сайта и прекращение возможности ее использования вследствие расторжения сублицензионного договора разработчиком формально не дает возможности продолжить использование веб-сайта и влечет существенные юридические риски. Разработчик же может использовать достаточно широкие и неопределенно сформулированные основания для расторжения сублицензионного договора в качестве длящегося инструмента давления на заказчика.

§ 3. Размещение веб-сайта на хостинговой площадке

Для нормального функционирования веб-сайт должен быть размещен на программно-аппаратном комплексе, осуществляющем круглосуточную работу и имеющем постоянное подключение к сети Интернет. При наличии необходимого оборудования и собственного канала доступа в сеть Интернет это не проблема. Однако далеко не каждое лицо может похвастаться их наличием. В связи с этим широкое распространение получили услуги хостинга или услуги по размещению информационного ресурса в сети Интернет.

В доктрине под хостингом обычно понимают услуги по предоставлению провайдером дискового пространства для размещения веб-сайта пользователя на сервере, подключенном в сети Интернет под постоянным *IP*-адресом, с его последующим техническим обслуживанием[1].

На практике выделяют различные виды хостинга: виртуальный хостинг, физический хостинг и так называемый *co-location*.

В том случае, когда веб-сайт размещается на сервере провайдера хостинга под одним постоянным *IP*-адресом, выделенном такому сайту, такой хостинг именуют физическим.

Услуга размещения на одном *IP*-адресе нескольких веб-сайтов с различными доменными именами получила название «виртуальный хостинг»[2].

Наконец, существуют ситуации, когда владелец веб-сайта обладает собственным сервером, который размещается в дата-центре провайдера, обеспечивающего его постоянное подключение к сети Интернет и техническое обслуживание. Такой вид хостинга получил название *co-location*. В отличие от ранее перечисленных видов хостинга пользователь приобретает не определенное количество дискового пространства на сервере хостинг-провайдера, а, условно говоря, определенное географическое место. Это место может характеризоваться особым географическим положением провайдера, включенностью в оптимальную для пользователя телекоммуникационную инфраструктуру, близостью к главному офису клиента и т.д.[3]

Достаточно долго в отечественном законодательстве отсутствовала дефиниция хостинга. Однако тем же Федеральным законом, который ввел реестр «вредных» сайтов, было введено и понятие провайдера хостинга, из которого можно вывести определение хостинга[4]. Так, провайдером хостинга является лицо, оказывающее услуги по предоставлению вычислительной мощности для размещения информации в информационной системе, постоянно подключенной к сети Интернет. Отсюда следует, что под хостингом понимаются услуги по предоставлению вычислительной мощности для размещения ин-

---

[1] См. подробнее: *Басманова Е.С.* Указ. соч. С. 71; *Камфер Ю., Бойкова М.* Интернет: от сложного к простому // Бухгалтерское приложение к газете «Экономика и жизнь». 2000. № 52; *Савельев А.И.* Гражданско-правовое регулирование договоров между клиентом и интернет-провайдером в сети Интернет: дис. ... канд. юрид. наук. М., 2008. С. 18.

[2] См., например: *Барабыкин П.В.* Указ. соч. С. 55–56.

[3] Подробнее о видах и особенностях договора хостинга см.: *Савельев А.И.* Гражданско-правовое регулирование договоров между клиентом и интернет-провайдером в сети Интернет.

[4] Закон о внесении изменений в Закон о защите детей от информации.

формации в информационной системе, постоянно подключенной к сети Интернет[1].

Несмотря на появление в законодательстве дефиниции хостинга, до сих пор отсутствует однозначное понимание относительно возможности отнесения его к услугам связи и телематическим услугам связи в частности. В то же время данный вопрос является весьма актуальным, поскольку от этого зависит необходимость получения лицензий.

С одной стороны, законодательство в сфере связи не упоминает понятия «хостинг», в том числе и в актах, посвященных лицензированию услуг связи. Не упоминается хостинг и в Руководящем документе отрасли «Телематические службы»[2], в котором приведены примеры телематических служб (факсимильные службы, службы электронных сообщений, службы голосовых сообщений, службы аудио-, видеоконференции, а также службы доступа к информации, хранящейся в электронном виде).

С другой стороны, существующие нормы законодательства о связи сформулированы достаточно широко и неопределенно, что создает простор для их применения в отношении услуг хостинга. Так, в соответствии с Постановлением Правительства РФ от 18 февраля 2005 г. № 87[3] предоставление пользователю возможности приема и передачи телематических электронных сообщений охватывается понятием телематической услуги связи. При этом само определение телематической услуги связи отсутствует как в данном Постановлении, так и в Правилах оказания телематических услуг связи[4], что не способствует сколько-нибудь однозначному пониманию данного термина. А поскольку услуги хостинга предполагают прием и передачу телематических электронных сообщений с использованием определенных протоколов (*HTTP*, *SMTP*, *POP3* и др.)[5] (например, в ходе организации «обратной связи» с пользователем веб-сайта, при функционировании различ-

[1] Данное определение вряд ли можно признать удачным, поскольку ключевой термин «вычислительные мощности», на котором оно зиждется, является весьма неопределенным.

[2] Руководящий документ отрасли «Телематические службы», утв. Приказом Министерства РФ по связи и информатизации от 23 июля 2001 г. № 175.

[3] Постановление Правительства РФ от 18 февраля 2005 г. № 87 «Об утверждении перечня наименований услуг связи, вносимых в лицензии, и перечней лицензионных условий».

[4] Постановление Правительства РФ от 10 сентября 2007 г. № 575 «Об утверждении Правил оказания телематических услуг связи».

[5] В соответствии с Правилами оказания телематических услуг связи под телематическим электронным сообщением понимается одно или несколько сообщений электросвязи, содержащих информацию, структурированную в соответствии с протоколом

ного рода форумов), то получается, что услуги хостинга подпадают под понятие телематических услуг связи и получение лицензии на их оказание становится весьма целесообразным.

Услуги хостинга вполне могут подпасть также и под определение услуги связи, содержащееся в ст. 2 Федерального закона от 7 июля 2003 г. № 126-ФЗ «О связи», под которой понимается деятельность по приему, обработке, хранению, передаче, доставке сообщений электросвязи или почтовых отправлений. Ведь, как отмечалось ранее, функционирование веб-сайта, размещенного на сервере провайдера хостинга, предполагает обмен сообщениями с пользователями, т.е. их прием, обработку и передачу, иногда и хранение. Из отнесения хостинга к категории услуг связи следует, в частности, тот вывод, что договор хостинга является публичным в силу ст. 426 ГК РФ[1]. Хотя и нельзя признать это разумным решением, поскольку требование об обеспечении равенства условий оказания услуг хостинга в отношении всех потребителей (п. 2 ст. 426 ГК РФ) противоречит существу хостинга, так как эти условия в значительной степени зависят от характеристик веб-сайта и целей его использования.

Предмет договора хостинга конкретизируется путем указания на объем дискового пространства, предоставляемого под веб-сайт пользователя; платформу, на базе которой будет размещен сайт, именуемую иногда в специальной литературе «хостинговая среда»[2]; предоставляемые дополнительные сервисы (например, ведение статистики посещаемости сайта, поддержка защищенных соединений и пр.).

Особое внимание следует уделить вопросам качества оказываемой услуги (нередко именуемой в англоязычной литературе как *performance standards*). Качество услуги хостинга нередко характеризуется следующими параметрами: пропускная способность канала (*bandwidth*); время реакции на запрос к серверу (*response time*); время доступности серверов провайдера (*website availability*)[3].

Одним из существенных показателей, характеризующих качество услуги хостинга, является пропускная способность линии связи, используемой провайдером хостинга, характеризующая объем данных,

обмена, поддерживаемым взаимодействующими информационной системой и абонентским терминалом (п. 2).

[1] См. подробнее: *Савельев А.И.* Применение судами норм Гражданского кодекса Российской Федерации о публичных договорах // Вестник гражданского права. 2009. № 4.

[2] См.: *Гуров В.В.* Корпоративный веб-хостинг // Сети и системы связи. № 3 (165). 2008. С. 28.

[3] *Klosek J.* Op. cit. P. 17.

который может быть передан за единицу времени[1]. От нее напрямую зависит количество пользователей, которые могут одновременно использовать веб-сайт с определенным уровнем комфорта. Данный параметр должен особо приниматься во внимание применительно к размещению «тяжелых» сайтов, изобилующих графикой, скриптами и иными объектами, требующими больших объемов трафика.

Немалое значение имеет время реакции на запрос к серверу, под которым понимается период времени между получением сервером запроса от пользователя на просмотр веб-страницы и отправкой сервером данных, содержащих запрашиваемую страницу на компьютер пользователя. Указанный параметр влияет в конечном счете на скорость загрузки страницы сайта, который является исключительно важным показателем для хостинга, поскольку при длительной загрузке страниц сайта у пользователей может пропасть желание заходить туда и популярность сайта резко снизится. Значительная часть пользователей Интернета покидает сайт в случае, если его загрузка длится более 15–20 секунд[2]. Как отмечается, средним показателем времени реакции сервера является 85 миллисекунд[3].

Еще одним важным параметром качества услуги хостинга является время доступности серверов провайдера хостинга пользователям Интернета. Так, если взять за основу исчисления один месяц, то в нем содержится 720 часов. Если интернет-провайдер гарантирует доступность сайтов пользователей 99,9% указанного периода, то это означает, что сайт будет доступен 712 часов из 720, если же интернет-провайдер гарантирует лишь 95%, то это будет составлять 684 часа. Как отмечается в зарубежной литературе, в скором будущем стандартом в указанной сфере будет обеспечение доступности сайтов на уровне 99,999%[4]. Так или иначе время доступности сайта должно быть определено в договоре хостинга либо в процентном соотношении, либо в виде общего количества часов, в течение которого сайт может находиться в офлайн-режиме. При этом необходимо предусмотреть механизм контроля над соблюдением данного параметра, в частности, путем предоставления отчетов провайдером хостинга, в том числе сгенерированных техническими средствами.

Наконец, целесообразно отразить в договоре хостинга положения, касающиеся судьбы веб-сайта в случае расторжения договора. Приме-

---

[1] *Graham Smith*. Op. cit. P. 765.

[2] *Калятин В.О.* Право в сфере Интернета. С. 98; см.: Online Contract Formation. Ed. by Stephan Kinsella and Andrew Simpson. Oceana Publications. N.Y., 2004. P. 355.

[3] *Roditti E.* Computer Contracts: Vol. I. Mathew Bender. 2006. P. 1951.

[4] *Roditti E.* Op. cit. P. 1828.

нительно к крупным веб-сайтам имеет смысл прописать процедуру миграции сайта к другому провайдеру. Во избежание использования веб-сайта в качестве «заложника» со стороны провайдера хостинга можно прописать обязанность провайдера предоставлять полную копию веб-сайта клиенту с определенной периодичностью (например, раз в месяц). Это позволит обойтись минимальными потерями данных в случае экстренной необходимости перехода к другому провайдеру.

§ 4. Вопросы ответственности провайдера хостинга за контент веб-сайта

Одним из наиболее актуальных вопросов, возникающих в связи с размещением веб-сайта на хостинговой площадке, является вопрос пределов ответственности провайдера хостинга за контент, размещенный на данном сайте иными лицами (владельцем веб-сайта или его посетителями).

Специфика деятельности провайдера хостинга состоит в том, что, с одной стороны, услуга носит технический характер и провайдер обычно не обладает знанием о том, кто какой контент загружает на веб-сайт[1]. Но с другой стороны, провайдер хостинга создает технические условия для размещения такой информации[2], имеет техническую возможность блокирования доступа к ней, его личность и местонахождение можно установить без особых проблем. К тому же хостинг-провайдер как субъект предпринимательской деятельности обладает активами, на которые можно обратить взыскание. Это во многом объясняет желание правообладателей и иных лиц, чьи права были нарушены, направить свой гнев именно в отношении них, а не неких трудноидентифицируемых пользователей или владельцев сайта, которых надо сначала отыскать, а потом умудриться с них что-либо успешно взыскать.

Очевидно, что возложение на интернет-провайдеров полной ответственности за действия третьих лиц пагубно скажется на развитии электронной коммерции и всей сети Интернет в целом: повышение цен на услуги провайдеров за счет включения в них соответствующих рисков, повышенный консерватизм провайдеров по вопросам введения новых типов услуг и бизнес-моделей. К тому же такой подход повлечет введение цензуры с их стороны на размещаемый контент[3].

---

[1] *Reed C., Angel J.* Op. cit. P. 240.

[2] Как известно из курса логики, причина причины есть причина следствия.

[3] *Savin A.* Op. cit. P. 104.

С другой стороны, технические реалии функционирования сети Интернет не позволяют игнорировать их роль в качестве «хранителей врат» (*gatekeepers*) Интернета и обусловленный им потенциал, который может быть использован для защиты прав потерпевших в сети Интернет. К тому же выбор любого из крайних вариантов решения проблемы (полный иммунитет или полная ответственность интернет-провайдеров) повлечет шквал злоупотреблений со стороны тех участников отношений, в пользу которых будет принято такое решение. Хостинг-провайдеры, пользуясь своим иммунитетом, превратятся в рассадники пиратства или, наоборот, правообладатели будут использовать провайдеров в качестве средства для извлечения прибыли. Необходимо сбалансированное решение данного вопроса, поиском которого занимались суды и законодатели разных стран в течение длительного времени. К сожалению, в рамках данной работы не представляется возможным подробно рассмотреть данную проблематику в компаративном аспекте[1], однако все же необходимо в общем виде остановиться на наиболее важных моментах, учитывая, что в условиях трансграничной природы сети Интернет провайдерам хостинга приходится иметь дело с зарубежным законодательством.

Одной из первых стран, в которых появились соответствующие положения, стали США, где был принят ряд законов, устанавливающих условия освобождения интернет-провайдеров от ответственности. При этом в качестве отправной точки при разработке соответствующих положений законодательства выступила I поправка к Конституции США, гарантирующая свободу слова, что предопределило их соответствующую идеологию.

Одним из таких законов является Закон о благопристойности информации 1996 г., который содержит ст. 230 (*c*), именуемую положениями о «Добром самаритянине». Суть данных положений сводится к тому, что ни провайдер, ни пользователь интерактивной компьютерной услуги не будут рассматриваться в качестве публикатора или автора информации, полученной от другого лица. При этом факт принятия провайдером мер по фильтрации, модерированию или ограничению доступа к контенту, который провайдер или пользователь считает про-

[1] Одним из наиболее полных компаративных исследований по данной тематике является: *Edwards L.* Role and Responsibility of the Internet Intermediaries in the Field of Copyright and Related Rights. 2011. Текст доступен на сайте ВОИС: http://www.wipo.int/export/sites/www/copyright/en/doc/role_and_responsibility of_the_internetintermediaries_final.pdf. На русском языке достаточно подробно данные вопросы освещаются в работе: *Войниканис Е.* Указ. соч. С. 288–352.

тивоправным, не дает дополнительных оснований для возникновения ответственности за размещение такого контента.

Данное положение особенно часто применяется в отношении диффамационных споров, хотя применимо оно также и к размещению информации, нарушающей тайну частной жизни, недостоверной информации о товаре, рекламе проституции и т.д.[1] Так, в деле *Zeran v. AOL*[2] ответчик был признан невиновным за размещение материала, который порочил честь и достоинство истца. При этом иммунитет, предоставляемый данной статьей, распространяется на провайдера даже в том случае, когда он принимает активную роль в обеспечении доступности такой информации. Указанная норма применяется и в случае приведения на сайте сведений, полученных из иных источников, в том числе с других веб-сайтов, а также в случае создания контента коллективными усилиями пользователей, как это имеет место в случае с *Wikipedia*[3].

Другим законом, регламентирующим ответственность интернет-провайдеров, правда, только за контент, нарушающий авторские права, является Закон США 1998 г. «Об авторском праве в цифровую эпоху» (*Digital Millennium Copyright Act*), содержащий положения, именуемые на практике *safe harbor* (англ. – зона безопасности). Суть данных положений сводится к установлению *специальных* оснований освобождения их от ответственности за нарушение авторских прав. Применительно к провайдерам хостинга они предполагают выполнение следующих основных условий[4]: 1) отсутствие финансовой выгоды, непосредственно получаемой вследствие допущенных нарушений; 2) отсутствие сведений о размещении контента, нарушающего авторские права третьих лиц, а равно о фактах и обстоятельствах, очевидно свидетельствующих о таких нарушениях[5]; 3) оперативное удаление такого контента по получении уведомления от правообладателя или его агента (так называемая процедура *notice-and-take-down*[6]). В числе дополнительных условий закон указывает: 1) наличие политики защиты авторских прав, предусматривающей расторжение договора (удаление

[1] *Edwards L.* Op. cit. P. 11.

[2] 129 F.3d 327 (4th Cir. 1997).

[3] См. подробнее: *Reed C., Angel J.* Op. cit. P. 261–263.

[4] § 512 (c).

[5] При этом речь идет именно о знании о контрафактном характере размещенных конкретных объектов. См.: Viacom Int'l Inc. v. YouTube, Inc., F. Supp. 2d, 2010 (S.D.N.Y. 2010).

[6] Bellia, Schiff and Post's Cyberlaw: Problems of Policy and Jurisprudence in the Information Age. West Group Publishing. 2004. P. 523.

аккаунта) пользователей, неоднократно нарушающих авторские права; 2) назначение специального контактного лица, специализирующегося на взаимодействии с правообладателями; 3) непрепятствие и содействие в применении правообладателями технических средств защиты произведений.

В общем виде действие процедуры *notice-and-take-down* на практике можно проиллюстрировать в виде следующего алгоритма:

1. *A* размещает песню, правообладателем которой является *B* на сайте, хостируемом провайдером *C*.

2. *B* обнаруживает данный факт и отправляет уведомление *C*, в котором указывает: свои контактные данные; наименование произведения, права на которое нарушены; *URL*, по которому оно размещено; заявление о том, что *B* добросовестно полагает, что *A* не имеет разрешения от него или его агентов на размещение данной песни; заявление о достоверности приведенной в уведомлении информации.

3. *C* на основании полученного заявления удаляет песню с сайта и направляет об этом уведомление *A*.

4. *A* имеет право направить контруведомление, указав свои контактные данные; наименование удаленной песни; заявление под страхом ответственности за дачу ложных сведений о том, что песня была удалена неправомерно; согласие на юрисдикцию американского суда на случай последующей передачи дела в суд.

5. *C*, получив контруведомление, уведомляет *B* и ждет 10–14 рабочих дней.

6. Если *B* не подает иск в течение вышеуказанного срока, *C* восстанавливает песню.

Несмотря на всю сложность указанной процедуры, она доказала свою жизнеспособность на практике и в целом достаточно неплохо отражает баланс интересов провайдера, правообладателя и пользователя. Она особенно эффективна против анонимных правонарушителей, которые не будут спорить с правообладателем по поводу удаления из Сети размещенного ими материала. К тому же данный механизм не возлагает существенных организационных или финансовых обременений на провайдера.

Во многом схожие положения были реализованы в Европейском союзе. В соответствии с Директивой ЕС об электронной коммерции 2000 г.[1] провайдер не несет ответственность за информацию, разме-

[1] Положения Директивы были имплементированы в национальное законодательство стран – участниц ЕС. В частности, в Германии – в Закон об электронной коммерции 2001 г. (*Electronische Geschaeftsverkehr-Gesetz*); во Франции – в Закон о доверии в цифровой

щенную при предоставлении услуг хостинга, если он не был осведомлен об ее противоправном характере, а также о фактах или об обстоятельствах, из которых такой противоправный характер очевиден[1], и после получения соответствующих сведений оперативно удалил противоправную информацию или прекратил доступ к ней (ст. 14).

Указанное освобождение от ответственности носит общий характер и распространяется на все возможные ее основания: нарушение исключительных прав, диффамационные сведения, неблагопристойную информацию и т.д. Следует особо подчеркнуть, что тот факт, что хостинг-провайдер не подпадает под рассматриваемое специальное защитное положение, не предрешает *автоматически* вопрос о его виновности. Это просто означает, что она будет определяться в общем порядке, в соответствии с правилами, применимыми к ответственности за распространение того или иного вида информации (нормами о диффамации, об ответственности за нарушение исключительных прав и т.п.), в рамках применения которых провайдер хостинга может быть также освобожден от ответственности.

При этом в Директиве особо подчеркивается недопустимость установления в национальном законодательстве государств – членов ЕС общей обязанности провайдеров осуществлять мониторинг передаваемой (размещаемой) информации, а равно обязанности искать факты или обстоятельства, свидетельствующие о незаконной деятельности (ст. 15). Указанная норма позволяет интернет-провайдерам оставаться пассивными до момента получения соответствующего уведомления от правообладателя. С другой стороны, оно не препятствует установлению в национальном законодательстве обязанности провайдера по информированию компетентных органов о выявленных фактах незаконной деятельности пользователей, а также по предоставлению таким органам идентифицирующей пользователей информации по их запросу.

Данное положение было предметом толкования Европейского суда, признавшего не соответствующим европейскому праву требования в отношении интернет-провайдера доступа по внедрению им системы фильтрации проходящих через его серверы электронных коммуникаций (в том числе связанных с пиринговыми сетями), которая применяется ко всем его абонентам и устанавливается за его собственный счет на неограниченный период времени. Как следствие, предписание

экономике 2004 г. (*Loi pour la confiance dans l'économie numérique*); в Англии – в Закон об электронной коммерции 2002 г. (*Electronic Commerce Regulations*).

[1] Данная оговорка может быть актуальной, в частности, применительно к популярным пиратским файлообменным сайтам (см.: *Savin A.* Op. cit. P. 116).

Бельгийского суда об обязании интернет-провайдера прекратить нарушения исключительных прав путем принятия мер, делающих невозможным для пользователей получение или рассылку музыкальных произведений, защиту которых осуществляет истец, было признано недопустимым[1]. Несколько позже схожая позиция была высказана Европейским судом еще раз, уже в отношении провайдеров хостинга[2].

Подобная позиция обусловлена в основном тем, что возложение обязанности по мониторингу контента в совокупности с таким условием исключения ответственности, как отсутствие знания о незаконности контента, фактически приведет к неизбежности блокировки провайдером незаконного, по его мнению, контента. Это повлечет ряд неблагоприятных последствий. Внедрение специальных систем мониторинга требует значительных затрат, которые в итоге будут переложены на самих пользователей, негативно сказываясь на доступности Интернета. К тому же такой мониторинг будет означать не что иное, как цензуру, которая будет к тому же весьма избыточной по причине стремления провайдеров к перестраховке. С технической точки зрения существует также риск избыточного блокирования, которое может повлечь нарушение законных прав владельцев иных сайтов, размещенных под тем же *IP*-адресом, что и заблокированный (виртуальный хостинг). Таким образом, возложение на интернет-провайдеров обязанности мониторинга контента повлечет больше вреда, нежели принесет пользы.

Прогрессивные нормы об ограничении ответственности информационных посредников (интернет-провайдеров) за материалы, размещенные третьими лицами, не являются исключительно достоянием законодательства США и европейских стран. Во многих азиатских странах (например, Япония[3], Сингапур[4]) содержатся схожие нормы. Даже в Китае вопреки распространенному в российской доктрине ошибочному мнению о полной ответственности провайдеров за действия пользователей[5] реализован принцип возложения на провайдера

---

[1] Scarlet Extended SA v. Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM), ECJ Case C-70/10, 24 November 2011.

[2] Belgische Vereniging van Auteurs, Componisten en Uitgevers CVBA (SABAM). v. Netlog NV. ECJ Case C-360/10, 16 February 2012.

[3] Закон Японии 2001 г. об ограничениях ответственности провайдеров телекоммуникационных услуг за убытки и о праве требовать раскрытия информации об отправителе № 137. Неофициальный английский перевод: www.isc.meiji.ac.jp/~sumwel_h/doc/codeJ/provider-e.htm

[4] *Graham Smith*. Op. cit. P. 639–641.

[5] См., например: *Рассолов И.М.* Указ. соч., § 3 гл. 3; *Примакова О.М.* Нарушение авторского права в сети Интернет // Правовые вопросы связи. 2011. № 1; *Наумов В.Б.* Право и Интернет: Очерки теории и практики. С. 19.

ответственности лишь при наличии у него сведений о противоправном характере размещенного контента. Провайдер хостинга обязан удалить нарушающий авторские права материал после того, как ему стало известно о нем или после получения уведомления от правообладателя с приложением доказательств. Он также обязан предоставить правообладателю имеющуюся информацию о пользователе; в противном случае на него самого будет возложена ответственность за нарушение авторских прав[1].

В России вопрос о пределах ответственности интернет-провайдеров является не менее актуальным[2]. Подобно тому, как это имеет место в США, в России к разным типам информации применяются нормы разных законов.

Общие положения об ответственности информационных посредников в сети Интернет содержатся в Законе об информации, положения которого исключают гражданско-правовую ответственность лиц, оказывающих услуги по хранению информации и обеспечению доступа к ней за распространение определенной информации, которое ограничено или запрещено законом, при условии, что это лицо не могло знать о незаконности распространения такой информации (п. 3 ст. 17). Данные положения потенциально применимы к различным лицам: как к хостинг-провайдеру, так и к владельцу интернет-сайта, на котором была размещена соответствующая информация[3]; потенциально применимы к любым основаниям возникновения ответственности за распространение противоправного контента (например, к ответственности за диффамацию), за исключением одного – они не распространяются на отношения, связанные с нарушением интеллектуальных прав (п. 2 ст. 1).

Судебная практика по вопросу ответственности провайдеров хостинга за размещение на веб-сайте материалов, нарушающих интеллектуальные права третьих лиц, находится в стадии формирования. Одним из основных прецедентов по данной тематике является решение

[1] См.: разъяснения Верховного суда КНР по вопросам применения закона в спорах, связанных с нарушением авторских прав в сети Интернет, от 22 ноября 2000 г.; Регуляции о защите права на коммуникации посредством информационных сетей 2006 г. Цит по: *Graham Smith.* Op. cit. P. 556–557.

[2] См.: п. 2.5 разд. VII Концепции развития гражданского законодательства Российской Федерации // Вестник ВАС РФ. 2009. № 11.

[3] См., например: постановление Четвертого арбитражного апелляционного суда от 27 февраля 2012 г. по делу № А19-13532/2011 (в данном деле владелец интернет-сайта был освобожден от ответственности за распространение сведений, порочащих честь, достоинство и деловую репутацию истца, по причине того, что он не мог знать о противоправном характере такой информации).

ВАС РФ по делу «Мастерхост»[1]. В нем суд сформулировал правовую позицию, в большинстве своем основанную на европейском опыте, в соответствии с которой провайдер не несет ответственности за передаваемую информацию, если он не инициирует ее передачу, не выбирает получателя информации и не влияет на целостность передаваемой информации. Как видно, в данном деле суд не посчитал нужным дифференцировать основания освобождения от ответственности в зависимости от типа интернет-провайдера, указав в качестве основных критерии, принятые в европейском праве в отношении интернет-провайдеров доступа (а не провайдеров хостинга). По мнению ВАС РФ, в данном случае «Мастерхост» отвечал данным критериям, так как осуществлял исключительно технические функции по размещению оборудования абонента и его техническое обслуживание. При этом он не имел доступа к оборудованию абонента, а в договоре было предусмотрено, что абонент несет полную ответственность за соответствие размещенной на его оборудовании информации действующему законодательству. Таким образом, отсутствовал факт самостоятельного использования провайдером соответствующих произведений. При этом Президиум ВАС РФ сделал оговорку, согласно которой при ведении своей деятельности провайдер должен действовать добросовестно и с надлежащей осмотрительностью, что подразумевает принятие им превентивных мер по пресечению нарушений с использованием предоставленных провайдером услуг. В частности, это может подразумевать надлежащее реагирование (приостановление или прекращение оказания услуг) после получения от третьих лиц обоснованных претензий или достоверных сведений, касающихся нарушения исключительных прав[2].

---

[1] Постановление Президиума ВАС РФ от 23 декабря 2008 г. № 10962/08.

[2] В качестве примера можно привести дело, где правообладатель (истец) обратился к хостинг-провайдеру ООО «Рамблер Интернет Холдинг» (ответчику) с требованием прекратить размещение в сети Интернет видеоклипа в связи с его несанкционированным использованием. Хостинг-провайдер ответил на претензию, однако не принял меры по выявлению лица, поместившего спорное музыкальное произведение в компьютерной сети, что повлекло привлечение его к ответственности за нарушение авторских прав. См.: постановление Девятого арбитражного апелляционного суда от 1 февраля 2010 г. № 09АП-26277/2009-ГК по делу № А40-89751/09-51-773, оставленное в силе постановлением ФАС Московского округа от 11 мая 2010 г. № КГ-А40/3891-10. Как видно, по мнению суда, для освобождения от ответственности провайдер хостинга должен был совершить ряд положительных действий по пресечению правонарушения: приостановление размещения спорного материала до урегулирования претензий, а также сообщение правообладателю имеющихся сведений о личности пользователя, разместившего материал. Если же такие сведения не будут предоставлены, а также будут отсутствовать иные доказательства того, что противоправный контент был размещен

Критерии освобождения провайдеров хостинга, изложенные в Постановлении по делу «Мастерхост», были детализированы и дополнены в Постановлении ВАС РФ по делу «Агава-софт»[1]. Судам при рассмотрении споров о привлечении к ответственности за нарушение исключительных прав хостинг-провайдеров было предписано проверять: 1) получил ли провайдер прибыль от деятельности, связанной с использованием исключительных прав других субъектов, которую осуществляли лица, пользующиеся услугами этого провайдера; 2) установлены ли ограничения объема размещаемой информации, ее доступности для неопределенного круга пользователей; 3) наличие в пользовательском соглашении обязанности пользователя по соблюдению законодательства Российской Федерации при размещении контента и безусловного права провайдера удалить незаконно размещенный контент; 4) отсутствие технологических условий (программ), способствующих нарушению исключительных прав, а также 5) *наличие специальных эффективных программ, позволяющих предупредить, отследить или удалить размещенные контрафактные произведения*. ВАС РФ указал, что судам следует также оценивать действия провайдера по удалению, блокированию спорного контента или доступа нарушителя к сайту при получении извещения правообладателя о факте нарушения исключительных прав, а также в случае иной возможности узнать (в том числе из широкого обсуждения в средствах массовой информации) об использовании его интернет-ресурса с нарушением исключительных прав других лиц. При отсутствии со стороны провайдера в течение разумного срока действий по пресечению таких нарушений либо в случае его пассивного поведения, демонстративного и публичного отстранения от содержания контента суд может признать наличие вины провайдера в допущенном правонарушении и привлечь его к ответственности.

Как справедливо отмечается в литературе, из данного Постановления не ясно, какие конкретно действия должен совершить провайдер хостинга, для того чтобы считать себя в безопасности[2]. К тому же в отличие от постановления по делу «Мастерхост», где ВАС РФ ориентировал на анализ принятых мер в соответствии с условиями договора между пользователем и провайдером, в Постановлении «Агава-софт» ВАС РФ ориентирует суды на то, чтобы наличие специальных про-

иным лицом, к которому должны быть предъявлены требования из нарушения авторских прав, ответственность может понести провайдер хостинга.

[1] Постановление Президиума ВАС РФ от 1 ноября 2011 г. № 6672/11 по делу № А40-75669/08-110-609.

[2] *Войниканис Е.* Указ. соч. С. 340.

грамм по предупреждению и отслеживанию контрафактных произведений и их эффективность анализировалось в *любом* случае. Правда, не понятно, как суд будет оценивать их эффективность в контексте достаточности для освобождения от ответственности. Ведь сам факт того, что дело дошло до суда, уже свидетельствует о том, что эти программы не сработали по какой-то причине. Общепринятые стандарты в данной области отсутствуют, что оставляет решение данного вопроса в субъективной плоскости судейского усмотрения.

Также примечателен тот факт, что ВАС РФ прямо указал, что уведомление правообладателя не является единственным источником информации, который может лишить провайдера защиты. В качестве таковых могут выступать «в том числе широкие обсуждения в средствах массовой информации», а также, по-видимому, иные источники, на что указывает использование фразеологизма «в том числе».

Как видно, ВАС РФ в отсутствие соответствующих положений в российском законодательстве восполнил указанный пробел в порядке судебного нормотворчества. Однако очевидно, что регулирование столь важного вопроса на уровне постановления по конкретному делу не является адекватным. В связи с этим соответствующие положения были досрочно внесены в ГК РФ[1].

Ответственность провайдеров хостинга (в терминологии части четвертой ГК РФ – информационных посредников, предоставляющих возможность размещения материалов в сети Интернет) урегулирована в п. 3 ст. 1253[1] ГК РФ.

Данное лицо не несет ответственности за нарушения интеллектуальных прав, произошедшие в результате размещения в сети Интернет материала третьим лицом, при одновременном соблюдении информационным посредником следующих условий:

«1) он не знал и не должен был знать о том, что использование соответствующего результата интеллектуальной деятельности или средства индивидуализации, содержащегося в таком материале, является неправомерным;

2) он 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. Перечень

[1] Федеральный закон от 2 июля 2013 г. № 187-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации по вопросам защиты интеллектуальных прав в информационно-телекоммуникационных сетях».

необходимых и достаточных мер и порядок их осуществления могут быть установлены законом»[1].

Данное положение было принято досрочно, т.е. в отрыве от иных поправок, предусмотренных проектом изменений в части четвертой ГК РФ. Такая спешка была обусловлена принятием нашумевшего «антипиратского» закона, направленного на борьбу с нелегальным распространением фильмов в сети Интернет. Стало очевидным, что в свете планируемого усиления борьбы с пиратством нельзя было сохранять неопределенность в вопросах пределов ответственности информационных посредников.

Однако вряд ли принятие указанной статьи в данной редакции достигло этой цели. В частности, неясно, как следует толковать фразу о том, что интернет-провайдер «не должен был знать» о неправомерном использовании объекта интеллектуальной собственности. Означает ли это, что он должен отслеживать сообщения и публикации в средствах массовой информации и сети Интернет, касающиеся творящихся на подконтрольном ему веб-сайте нарушений. Формулировка «не должен был знать» содержит в себе значительный потенциал объективного вменения и предоставляет значительный простор для усмотрения правоприменителей при ее толковании. Очевидно, что со временем будут выработаны более-менее четкие критерии толкования данного термина, однако сколько участников оборота падут жертвами произвола до этого момента – остается только гадать.

Второй момент, который хотелось бы отметить, – это то, что содержание предлагаемых в данной статье условий освобождения провайдера хостинга от ответственности явно беднее тех, которые сформулированы судебной практикой ВАС РФ. Например, в статье ничего не говорится о необходимости принятия превентивных мер («специальных программ по предупреждению и отслеживанию контрафактных произведений»), на наличие и эффективность которых ВАС РФ предписал обращать внимание. Если же по-прежнему этот критерий является актуальным, то как наличие и эффективность этих мер будут влиять на толкование формулировки «не должен был знать»? Ответа на данный вопрос пока нет.

В связи с этим возникает вопрос о соотношении положений ст. 1253[1] и разъяснений ВАС РФ. Конечно, с формальной точки зрения текст

[1] В отличие от *DMCA* ст. 1253[1] не содержит в себе положений, детализирующих процедуру взаимодействия между провайдером, клиентом и правообладателем. В ходе обсуждений было принято решение вывести ее реализацию на уровень отдельного закона (см.: *Калятин В.О.* О некоторых тенденциях развития законодательства об ответственности интернет-провайдеров // Закон. 2012. № 7. С. 34).

ГК РФ будет иметь преимущественную силу и постановления ВАС РФ могут применяться лишь в части, не противоречащей ему. Однако ответ на вопрос о том, являются ли «творческое» дополнение и конкретизация высшим судом критериев, заложенных в законе, противоречием ему или всего лишь толкованием, не так очевиден. Особенно учитывая, что рассмотрение споров, связанных с нарушением прав на фильмы в сети Интернет, отнесено к компетенции Мосгорсуда, для которого разъяснения ВАС РФ, мягко говоря, необязательны. Представляется, что в такой ситуации понадобятся дополнительные разъяснения высшей судебной инстанции по данному вопросу.

Несмотря на то что положения ст. 1251^{1} ГК РФ в целом отражают зарубежный опыт регулирования такого рода отношений, необходимо отметить, что содержание предлагаемых в данной статье условий освобождения провайдера хостинга от ответственности явно беднее тех, которые сформулированы судебной практикой ВАС РФ. В связи с этим может возникнуть вопрос об их соотношении. Формально текст ГК РФ будет иметь преимущественную силу и постановления ВАС РФ смогут применяться лишь в части, не противоречащей ему. Ответ на вопрос о том, являются ли «творческое» дополнение и конкретизация высшим судом критериев, заложенных в законе, противоречием ему или всего лишь толкованием, не так очевиден. Особенно учитывая, что рассмотрение споров, связанных с нарушением прав на фильмы в сети Интернет отнесены к компетенции Мосгорсуда, для которого разъяснения ВАС РФ, мягко говоря, необязательны. Представляется, что в такой ситуации необходимы дополнительные разъяснения ВАС РФ и ВС РФ по данному вопросу.

§ 5. Выбор и регистрация доменного имени

Выбор правильного доменного имени является важным условием успешного бизнеса в сфере электронной коммерции. Подобно тому как местонахождение офиса в реальном мире имеет немалое значение для привлечения клиентов, доменное имя обладает значительным потенциалом для привлечения пользователей сети Интернет.

Суть доменного имени можно вкратце обозначить следующим образом. Каждый компьютер, подключенный к сети Интернет, имеет уникальный *IP*-адрес, идентифицирующий его. Именно по этому адресу осуществляются поиск и взаимодействие компьютеров в данной сети. Поскольку *IP*-адрес представляет собой последовательность из четырех чисел, разделенных точками, то запомнить его в таком виде сложно.

Для удобства запоминания и восприятия была создана система доменных имен (*Domain Name System – DNS*), позволяющая сопоставлять абстрактное символьное имя конкретному *IP*-адресу в Сети[1]. В доктрине под доменным именем понимается *зарегистрированное в установленном порядке символьное обозначение, заменяющее цифровой IP-адрес компьютера, подключенного к сети Интернет, и предназначенное для идентификации информационных ресурсов в этой сети, а также адресации запросов в ней*[2]. С недавних пор российское законодательство пополнилось легальной дефиницией данного понятия, которая в целом соответствует доктринальным представлениям о доменном имени: «обозначение символами, предназначенное для адресации сайтов в сети Интернет в целях обеспечения доступа к информации, размещенной в сети Интернет»[3].

Существование системы доменных имен не отменяет и не заменяет использование *IP*-адресов, но делает функционирование системы *IP*-адресов незаметным для пользователя Интернета. Если же пользователь знает точный *IP*-адрес, то он может и не применять доменное имя, поскольку *IP*-адрес уже содержит информацию, достаточную, чтобы провайдер, используя таблицы маршрутизации, обеспечил необходимое соединение. Поэтому доменное имя, формально говоря, не является неотъемлемой частью веб-сайта. Однако оперировать *IP*-адресами в процессе повседневной деятельности в сети Интернет для пользователя достаточно сложно, подобно тому, как сложно оперировать и обычными телефонными номерами без записной книги. Недаром Всемирная организация интеллектуальной собственности определяет понятие доменных имен следующим образом: «Доменные имена являются понятными для человека формами интернет-адресации обычно для определения места нахождения веб-сайтов»[4].

После того как лицо подберет обозначение, которое оно желает зарегистрировать в качестве доменного имени, это обозначение должно быть включено в систему доменных имен и получить статус доменного имени, только после этого оно сможет стать частью Интернета. Иначе говоря, доменное имя возникает как объект только с момента регистрации. В связи с этим регистрация доменного имени является моментом его возникновения и, следовательно, необходимым условием для возникновения права на доменное имя. Таким образом, создание доменного имени складывается из двух этапов: выбора подходящего

[1] *Серго А.Г.* Интернет и право. С. 29.
[2] *Калятин В.О.* Доменные имена. С. 14.
[3] Статья 2 Закона об информации.
[4] http://www.wipo/int/amc/en/center/flag/domains.html

обозначения заявителем и регистрации данного обозначения в качестве доменного имени.

Выбор подходящего наименования определяется фантазией лица, но ограничен рядом факторов: семантическими (ограничение на характер и количество используемых символов)[1]; архитектурой сети Интернет, предопределяющей требование уникальности доменного имени (отсутствие ранее зарегистрированного аналогичного доменного имени); соображениями морали[2].

Требование уникальности доменного имени не только создает сложности при его выборе и повышает ценность удачного наименования, но и является сильным конфликтогеном в отношениях с правообладателями товарных знаков и фирменных наименований. Юридическая чистота доменного имени не является условием его регистрации. Обычно в своих правилах регистраторы прямо указывают непринятие на себя ответственности за возможность существования конфликта зарегистрированного доменного имени с другими средствами индивидуализации и подчеркивают приверженность принципу регистрации «первого заявителя» (*first come, first served*)[3]. О том, как рассматриваются подобного рода конфликты, будет подробнее сказано далее. Сейчас хотелось бы остановиться на вопросах регистрации доменного имени.

Регистрация и поддержка доменных имен осуществляются на началах саморегулирования специальными организациями, каждая из которых отвечает за свою часть доменных имен сети Интернет. Координи-

[1] См.: п. 3.1.1 Правил регистрации доменных имен в домене *ru*. и .рф, утв. решением Координационного центра национального домена сети Интернет от 5 октября 2011 г. № 2011-18/81 http://www.cctld.ru/ru/docs/rules.php (далее – Правила регистрации доменных имен). В частности, доменное имя должно содержать от 2 до 63 символов, начинаться и заканчиваться буквой латинского алфавита или цифрой. Промежуточными символами могут быть буквы латинского алфавита, цифры или дефис. Доменное имя не может содержать дефисы одновременно в 3-й и 4-й позициях.

[2] См.: п. 3.1.5 Правил регистрации доменных имен о недопустимости использования слов непристойного содержания, призывов антигуманного характера, оскорбляющих человеческое достоинство либо религиозные чувства. Существует так называемый стоплист доменных имен, который содержит в себе примеры подобного рода словоупотребления. Нахождение доменного имени в стоп-листе является безусловным основанием для отказа в его регистрации.

[3] См.: п. 3.1.3, 3.1.4 Правил регистрации доменных имен: «Поскольку регистратор не вправе отказать в регистрации выбранного пользователем доменного имени на основаниях, не предусмотренных настоящими Правилами, пользователь (администратор) самостоятельно несет ответственность за выбор доменного имени и за возможные нарушения прав третьих лиц, связанные с выбором и регистрацией доменного имени, а также несет риск убытков, связанных с такими нарушениями. Пользователю рекомендуется перед подачей заявки убедиться в отсутствии сходных с регистрируемым доменным именем товарных знаков и иных объектов интеллектуальной собственности».

рующую роль во всей структуре доменных имен играет некоммерческая Корпорация Интернета для специализированных адресов и номеров (*ICANN – Internet Corporation For Assigned Names and Numbers*). *ICANN* несет общую ответственность за распределение *IP*-адресов и осуществляет общий контроль над управлением функциональными доменами (*gTLD*)[1] и национальными доменами высшего уровня (*ccTLD*).

В России координатором национальных доменов верхнего уровня *.ru* и *.рф* выступает Автономная некоммерческая организация «Координационный центр национального домена сети Интернет». Он обладает полномочиями по выработке правил регистрации доменных имен в указанных доменах верхнего уровня, аккредитации регистраторов и исследованию перспективных проектов, связанных с развитием российских доменов верхнего уровня. Фактические действия по регистрации доменных имен осуществляются аккредитованными регистраторами доменных имен в доменах *.ru* и *.рф*, которые являются коммерческими организациями[2]. Регистрация доменных имен носит явочный (заявительный) характер и осуществляется на основании публичного договора об оказании услуг регистрации (ст. 426 ГК РФ)[3], который также является и договором присоединения (ст. 428 ГК РФ). Заявительный характер регистрации доменных имен является общепринятым во всем мире и обусловлен необходимостью обеспечения оперативности регистрации и минимизации ее стоимости, что обусловлено динамичной природой отношений в сети Интернет.

Регистрация доменного имени представляет собой внесение регистратором в специальный реестр сведений о доменном имени, его администраторе и иных сведений, установленных правилами. Такая

[1] Длительное время система функциональных доменов верхнего уровня состояла из семи доменов. Домен *.com* был предназначен для коммерческих организаций, *.org* – для некоммерческих организаций, *.net* – для организаций, деятельность которых связана с Интернетом, *.edu* – для учреждений системы образования, *.int* – для международных организаций, *.gov*, *.mil* – соответственно для правительства и Министерства обороны США. С 2001 г. корпорация внедрила доменные зоны *.info*, *.biz*, *.name*, *.coop*, *.museum*, *.aero*, *.pro*, *.travel*, *.jobs*, *.cat*, *.asia*, *.eu*, *.mobi*, *.tel*, *.tv*. При этом в *ICANN* намерены и в дальнейшем следовать политике расширения адресного пространства за счет создания новых доменов верхнего уровня, в том числе с использованием символов национальных алфавитов.

[2] Список таких регистраторов доступен на сайте Координационного центра национального домена сети Интернет // http://cctld.ru/ru/registrators/

[3] Ранее, в связи с тем что регистрацию доменных имен осуществляла некоммерческая по своему статусу организация РосНИИРОС, суды отказывали в признании соответствующего договора публичным, что лишало заявителей мощного орудия борьбы с возможным произволом регистратора. См. подробнее: *Савельев А.И.* Применение судами норм Гражданского кодекса Российской Федерации о публичных договорах.

регистрация носит срочный характер: 1 год с неограниченной возможностью продления.

От регистрации следует отличать так называемое делегирование доменного имени, под которым понимаются размещение и хранение информации о доменном имени и соответствующих ему серверах *DNS* на серверах *DNS* домена верхнего уровня, что является необходимым условием для функционирования доменной адресации в сети Интернет.

Таким образом, у зарегистрированного доменного имени может быть два состояния: «делегирован» (*delegated*), т.е. когда при наборе доменного имени пользователь сети Интернет попадает на определенный сайт, и «не делегирован» (*not delegated*), когда домен зарегистрирован, но еще не «прикреплен» к интернет-сайту. Владелец доменного имени может «прикрепить» его также к чужому сайту. На один и тот же сайт может указывать два и более доменных имени (при наборе любого из них в браузере пользователь попадает на один и тот же интернет-сайт).

Вопрос о правовой природе доменного имени является одним из наиболее интригующих. Возникает множество вопросов: является ли право на доменное имя абсолютным, будучи разновидностью объекта интеллектуальной собственности, или оно носит относительный характер, выступая порождением договора с регистратором? Является ли доменное имя разновидностью права интеллектуальной собственности или же оно выполняет исключительно техническую функцию средства адресации?[1]

Зарубежная доктрина и судебная практика пока не выработали однозначного ответа на данные вопросы.

В Англии суды склоняются к договорно-правовой природе прав на доменные имена[2]. При этом в одном из наиболее авторитетных трудов по интернет-праву Англии содержится достаточно жесткая позиция о том, что право на доменное имя не относится к категории прав на объект интеллектуальной собственности, а является лишь одним из средств реализации исключительного права на товарный знак, подобному размещению его в рекламе или на упаковке товара[3].

В США судебная практика по вопросу о правовой природе доменного имени является неоднозначной. Существуют решения, в которых суды отказывали в признании за правом на доменное имя качества

[1] *Hurter E.* International Domain Name Classification Debate – Are Domain Names Virtual Property, Intellectual Property, Property, or Not Property at All // Comparative and international law journal of Southern Africa. No 42. 2009. P. 289.

[2] Pitman Training Limited & Another v Nominet UK & Another [1997] FSR 797; *Murray A.* Internet Domain Names: The Trade Mark Challenge // International Journal of Law and Information Technology. No 6. 2001. P. 294–295.

[3] *Graham Smith.* Op. cit. P. 171.

права собственности, отмечая его тесную связь с договором на оказание услуг, заключенным с регистратором[1]. С другой стороны, в Законе США 1999 г. «О защите потребителей от кибersквоттинга»[2] говорится о возможности предъявления иска к самому доменному имени (*in rem action*) в случае невозможности нахождения ответчика или установления над ним юрисдикции американским судом, что привело некоторые суды к выводу о том, что доменное имя стало объектом права собственности[3]. Так, в одном решении было отмечено, что доменное имя является формой бестелесной собственности (*intangible property*), поскольку: 1) является четко определенным объектом; 2) является объектом исключительного контроля; 3) притязание обладателя на такой исключительный контроль носит законный характер[4].

В Голландии доминирующей является точка зрения, согласно которой права на доменное имя носят договорно-правовой характер, что не мешает в то же время рассмотрению главным регистратором доменных имен в Голландии (*Stichting Internet Domein Registratie Nederland*) таких прав как абсолютных с применением к ним процедур изъятия, предусмотренных для объектов права собственности[5].

Вопрос правовой природы доменного имени был недавно предметом рассмотрения Европейского суда. В деле *PAEFFGEN GMBH* против Германии было высказано мнение, что данные объекты, не являясь физическим, осязаемым объектом, представляет собой договорное право на исключительное использование такого имени (*contractual right to the exclusive use of domain names*). Это исключительное право на использование доменов имеет экономическую ценность и, следовательно, представляет собой «имущество» для целей применения положений ст. 1 Конвенции о защите прав человека и основных свобод о недопустимости произвольного лишения имущества. Однако в данном случае, по мнению Суда, соответствующие ограничения (принятие немецкими судами судебных приказов, запрещающих компании-заявителю использовать соответствующие домены или распоряжаться ими и требующих обратиться

[1] Network Solutions Inc v Umbro International, Inc 529 SE 2d 80 (Va 2000); Dorer v Arel 60 F Supp 2d 558 (E.D. Va 1999); Farmology.com v Perot Sys Corp 158 F Supp. 2d 589 (E.D. Pa. 2001).

[2] US Anticybersquatting Consumer Protection Act (ACPA). Под кибersквоттингом (англ. – *cybersquatting*) понимается регистрация доменных имен, содержащих товарный знак, принадлежащий другому лицу, с целью последующей перепродажи такого доменного имени владельцу товарного знака или недобросовестного использования.

[3] Ceasars World, Inc v Ceasars – palace.com 2 F Supp. 2d 502 (E.D. Va 2000); Porsche Cars North America v Porsche.net 64 USPQ 1248 (CA 4 2002).

[4] Kremen v Cohen 99 F Supp. 2d 1168 (N.D. Cal. 2000).

[5] *Graham Smith*. Op. cit. P. 265–266.

за их аннулированием) были обусловлены легитимным общественным интересом в обеспечение защиты прав на товарные знаки и не являлись чрезмерными[1]. Таким образом, Европейский суд высказался за договорную, а не абсолютно правовую природу права на доменное имя. Факт распространения на него возможности защиты в целях применения положений вышеуказанной Конвенции не должен смущать. Практика Европейского суда по правам человека (ЕСПЧ) свидетельствует о весьма широком толковании им понятия «имущество», относя к нему: «... движимое и недвижимое имущество, материальные и нематериальные интересы, такие как акции, патенты, искомое решение арбитража, право на пенсию, право домовладельца на взыскание арендной платы, экономические интересы, связанные с ведением бизнеса, право заниматься той или иной профессией, правомерное ожидание применения определенных условий к индивидуальной ситуации, требующей правового разрешения, правопритязание и вопрос о посещении кинотеатра зрителями»[2]. Европейский суд в данном случае лишь принял на вооружение практику ЕСПЧ применительно к одному узкому вопросу, но не более того.

Отечественная доктрина не отстает от зарубежных коллег в попытках определения правовой природы доменных имен. Из многочисленных точек зрения по данному вопросу в отечественной доктрине можно выделить две основные: доменное имя как средство индивидуализации[3] и доменное имя как средство адресации в Интернете[4].

Так, по мнению В.О. Калятина, «поскольку применение доменного имени является основным способом доступа к сайту в Интернете, значение доменного имени оказывается еще более важным, чем значение товарного знака в «реальном» мире. Если доменное имя сайта никому не известно, то на такой сайт долго может не заглядывать ни один посетитель; вряд ли такая ситуация возможна с реальным магазином, пусть даже без вывески. Таким образом, индивидуализирующие функции

[1] Paeffgen GmbH v. Germany. 18.09.2007. No 25379/04, 21688/05, 21722/05 и 21770/05

[2] Европейская конвенция о защите прав человека и основных свобод. Право на собственность: сборник. М., 2002. С. 4.

[3] См., например: *Наумов В.Б.* Право и Интернет. Очерки теории и практики. С. 160; *Кемрадж А.С.* Использование адресного пространства: доменные имена, защита прав владельцев доменных имен, пресечение недобросовестной конкуренции в области использования доменных имен // Правовые аспекты использования интернет-технологий. М., 2002. С. 46; *Серго А.* Доменные имена как средство индивидуализации // Хозяйство и право. 2011. № 5.

[4] См., например: *Бабкин С.А.* Интеллектуальная собственность в сети Интернет. С. 422; *Милютин З.Ю.* Правовой статус доменного имени // Патенты и лицензии. 2005. № 6; *Невзоров И.* О соотношении доменного имени с объектами интеллектуальной собственности // Хозяйство и право. 2006. № 1.

доменного имени оказываются шире, чем функции только товарных знаков (знаков обслуживания) или фирменных наименований»[1].

Примечательно, что в проекте части четвертой ГК РФ существовал параграф под названием «Право на доменное имя» (§ 5 гл. 76), который как раз рассматривал доменные имена в качестве одного из средств индивидуализации. В проекте содержалось определение доменного имени, закреплялось исключительное право на доменное имя в соответствии со ст. 1229 ГК РФ, возникновение которого связывалось с моментом регистрации. Однако в процессе рассмотрения законопроекта данная глава была исключена главным образом потому, что она образовывала определенное противостояние между обозначениями, защищаемыми как доменные имена, и обозначениями, защищаемыми в режиме товарного знака, к тому же смущала и новизна указанных объектов вкупе с отсутствием опыта их законодательного регулирования за рубежом[2]. Поначалу, видимо, в качестве своего рода компенсации за удаление главы упоминание о доменном имени было включено в ст. 1483 ГК РФ как одно из оснований для отказа в государственной регистрации товарного знака. В соответствии с подп. 3 п. 9 данной статьи не могли быть зарегистрированы в качестве товарных знаков обозначения, тождественные промышленному образцу, знаку соответствия, доменному имени, права на которые возникли ранее даты приоритета регистрируемого товарного знака. Таким образом, в отношении доменного имени был установлен режим самостоятельного объекта гражданского права, который в определенных случаях согласно принципу «старшинства» права мог стать барьером на пути регистрации товарного знака, причем по любым классам МКТУ, что ставило владельца доменного имени в весьма привилегированное положение[3]. Правда, долго эта норма не прожила: в октябре 2010 г. упоминание о доменных именах из данной нормы было исключено[4]. Единственными положениями ГК РФ,

[1] *Калятин В.О.* Доменные имена. С. 19.

[2] См.: заключение Комитета по экономической политике, предпринимательству и туризму на текст проекта части четвертой ГК РФ. Цит. по: *Архипов Е.В.* Доменное имя как объект правового регулирования // Предпринимательское право. Приложение «Бизнес и право в России и за рубежом». 2012. № 3.

[3] *Еременко В.И.* О совершенствовании правового регулирования доменных имен в Российской Федерации // Законодательство и экономика. 2012. № 10.

[4] Федеральный закон от 4 октября 2010 г. № 259-ФЗ «О внесении изменений в часть четвертую Гражданского кодекса Российской Федерации». Во многом это было связано с тем, что предоставление приоритета доменному имени над товарным знаком в таких случаях противоречило бы соглашению *TRIPS*. Доменные имена, не являющиеся объектом интеллектуальной собственности согласно соглашению *TRIPS*, не могут иметь больший приоритет по сравнению с товарным знаком (см.: п. 1253 Доклада Рабочей

где доменные имена упоминаются, остались нормы в ст. 1484 и 1519 ГК РФ как способы использования (законного или незаконного – судя по обстоятельствам) соответственно товарных знаков и наименований мест происхождения товаров.

Противники рассмотрения доменного имени в качестве средства индивидуализации и потенциального кандидата на новый вид объекта интеллектуальной собственности отмечают, что доменное имя не является самостоятельным объектом интеллектуальной собственности, а является реквизитом, позволяющим пользователям сети Интернет идентифицировать конкретную информацию, зафиксированную на компьютере (сервере) третьего лица, и в первую очередь служит именно цели идентификации документа с информацией в сети Интернет[1].

Возражая сторонникам первого подхода, они отмечают, что уникальность доменного имени определяется используемой системой регистрации, в связи с чем отсутствует потребность в его квалификации в качестве средства индивидуализации. З. Милютин указывает в связи с этим: «...в Интернете доменное имя в такой защите не нуждается. Никто и так не сможет зарегистрировать и публично эксплуатировать в Интернете доменное имя, идентичное уже зарегистрированному»[2]. Схожую позицию поддерживает и С. Бабкин: «...доменное имя не может утратить индивидуализирующую функцию иначе чем в результате действий лица, управляющего системой адресации. Никакие третьи лица не могут своими действиями лишить доменное имя индивидуализирующей функции или ослабить его связь с определенным оконечным устройством»[3]. По существу, сторонники данного подхода отрицают наличие у прав на доменное имя абсолютного характера, сводя его суть к имущественному праву требования, существующему в рамках договора.

Представляется, что обе точки зрения представляют собой варианты крайних подходов к правовой природе доменных имен и не учитывают динамику их развития. Отрицать наличие у доменного имени адресной функции означает отрицать очевидное. Но не менее очевиден тот факт, что данный подход характеризует природу доменного имени преимущественно с технической стороны. С другой стороны, нельзя отрицать тот факт, что доменные имена появились именно потому, что перво-

группы по присоединению Российской Федерации к Всемирной торговой организации от 17 ноября 2011 г. // СПС «КонсультантПлюс»).

[1] *Невзоров И.В.* Правовая природа доменного имени и его соотношение с объектами интеллектуальной собственности // Предпринимательское право. 2005. № 4.

[2] *Милютин З.Ю.* Соотношение доменных имен со средствами индивидуализации: дисс. ... канд. юрид. наук. М., 2005. С. 78, 81.

[3] *Бабкин С.А.* Интеллектуальная собственность в сети Интернет. С. 422.

начальный способ адресации, принятый в сети Интернет (*IP*-адреса), являлся слишком неудобным, требовалось нечто, что обладало бы большей отличительной способностью, нежели набор цифр. Особенно это было актуально на начальных этапах коммерциализации Интернета, когда компании, деятельность которых осуществлялась в офлайн-режиме, начали размещать свои веб-сайты в сети Интернет и, разумеется, хотели использовать те обозначения, с которыми их уже давно ассоциируют потребители. Здесь, безусловно, можно говорить о явно выраженной индивидуализирующей составляющей доменного имени. Однако с развитием мощи поисковых систем Интернета эта составляющая в значительной степени ослабла. Дело в том, что в настоящее время большинство пользователей (более 85%) находят тот или иной ресурс, включая интернет-магазин, не столько путем ввода по памяти того или иного доменного имени, сколько путем использования поисковых систем[1]. Пользователь вводит в качестве запроса искомый товар, и далее поисковая система выдает ряд ресурсов, где он может быть приобретен. Обычно пользователь «гуляет» по ссылкам, не запоминая доменных имен тех сайтов, где он побывал. Конечно, существуют гиганты электронной коммерции, которые у всех на слуху (*Amazon*, *Ozon*, *Steam* и пр.), но в данном случае индивидуализирующая функция является следствием их репутации и многочисленных рекламных кампаний. Иными словами, индивидуализирующая функция у доменного имени, безусловно, присутствует, но она не свойственна всем доменным именам даже в коммерческой сфере. Грамотная раскрутка сайта интернет-магазина в поисковых системах нередко способна компенсировать отсутствие запоминающегося доменного имени. Другое дело, что по мере роста репутации интернет-магазина и его популярности возникает риск паразитирования на ней с последующим появлением сайтов со схожими наименованиями и доменными именами, отвлекающих потенциальных покупателей на себя. Подобные действия могут охватываться понятием недобросовестной конкуренции, и их пресечение не требует с необходимостью придания доменному имени статуса средства индивидуализации. При указанных обстоятельствах абсолютизация функции индивидуализации у доменного имени представляется в большинстве своем следствием привнесения в принципиально новую среду Интернета элементов, механически скопированных из эпохи «до Интернета».

Возможно, со временем ситуация изменится и законодатель встанет перед необходимостью придания доменному имени особого право-

[1] *Юрасов А.В.* Указ. соч. С. 284.

вого статуса, но до этого времени вряд ли этот результат может быть достигнут в доктринальном порядке.

В России в настоящее время доменное имя не поименовано в качестве охраняемого объекта интеллектуальной собственности в ст. 1225 ГК РФ, содержащей закрытый перечень таких объектов. Следовательно, на доменное имя не возникает исключительного права, а права на него не могут предоставляться с использованием договорных конструкций, закрепленных в части четвертой ГК РФ (лицензионный договор, договор на отчуждение исключительного права). Так, например, передача прав на домен может быть осуществлена на основании договора о передаче права администрирования другому лицу[1], который по своей правовой природе может быть отнесен к договору уступки права требования (гл. 24 ГК РФ). Таким образом, в настоящее время доменное имя как объект гражданского права представляет собой относительное имущественное право, но никак не объект права интеллектуальной собственности и уж тем более не объект права собственности в классическом понимании.

§ 6. Споры в сфере доменных имен

Учитывая неизбежные конфликты между владельцами доменных имен и обладателями прав на фирменные именования и товарные знаки, не может не вызывать удивления существование обильной судебной практики по данному вопросу. На данную тему в России опубликовано немало хороших и актуальных работ, в силу чего в данной книге нет смысла пересказывать их положения[2], но хотелось бы отметить следующее.

Традиционная судебная процедура не может в полной мере защитить законные интересы правообладателей. Она является слишком долгой и нередко весьма недешевой, особенно учитывая возможные юрисдикционные проблемы, часто сопутствующие спорам в сети Интернет. В то же время регистрация доменного имени занимает очень мало времени, скорость распространения информации в Интернете чрезвычайно велика, в связи с чем «контрафактный» сайт способен нанести вред интересам правообладателя в весьма короткие сроки. Да и затраты на доступ к правосудию, исчисляемые тысячами долларов,

[1] См.: ст. 6 Правил регистрации доменных имен.

[2] См., например: *Серго А.Г.* Доменные имена. Правовое регулирование. М., 2013; *Вацковский Ю.Ф.* Доменные споры. Защита товарных знаков и фирменных наименований. М., 2009; *Еременко В.И.* Указ. соч.

которые должен понести правообладатель, могут выступать сильным сдерживающим фактором для инициирования спора, что дает преимущества потенциальному нарушителю, который может зарегистрировать доменное имя за сумму всего в несколько десятков долларов. Все это обусловило появление и широкое использование альтернативной процедуры рассмотрения споров: Единого регламента рассмотрения споров о доменных именах (*The Uniform Domain Names Dispute Resolution Policy*, *UDRP*), разработанного Всемирной организацией интеллектуальной собственности (ВОИС) и принятого *ICANN* в 1999 г.[1]

UDRP изначально разрабатывался для разрешения споров и создания препятствий для недобросовестной регистрации доменных имен, а также использования товарных знаков в качестве доменных имен в функциональных доменах верхнего уровня (*.aero*, *.asia*, *.biz*, *.cat*, *.com*, *.coop*, *.info*, *.jobs*, *.mobi*, *.museum*, *.name*, *.net*, *.org*, *.pro*, *.tel and .travel*), а также в некоторых географических доменах верхнего уровня (*.nl*, *.es*, *.au*, *.fr*, *.ch* и др.[2]). Согласие с *UDRP* является необходимым условием заключения договора на регистрацию подобных доменных имен.

Споры в рамках процедуры *UDRP* в отношении функциональных доменов верхнего уровня рассматривают специально уполномоченные организации по выбору заявителя (далее – арбитражные центры): 1) Азиатский центр по разрешению споров о доменных именах (*Asian Domain Name Dispute Resolution Center*); 2) Арбитражный центр по рассмотрению интернет-споров Чешского арбитражного суда (*The Czech Arbitration Court Arbitration Center for Internet Disputes*); 3) Национальный арбитражный форум (*The National Arbitration Forum*); 4) ВОИС; 5) Арабский центр по рассмотрению споров в сфере доменных имен (*Arab Center for Domain Name Dispute Resolution*)[3]. Споры, связанные с географическими доменами верхнего уровня, рассматривают организации, определенные администратором такого домена.

Для удовлетворения требования правообладателя о прекращении регистрации доменного имени или о передаче прав на него он должен доказать наличие одновременно трех обстоятельств, указанных в ст. 4 (*a*) *UDRP*:

1) доменное имя идентично или сходно до степени смешения с товарным знаком или знаком обслуживания, правообладателем которых он является;

---

[1] http://www.icann.org/ru/dndr/udrp/policy-ru.htm

[2] Полный список см.: http://www.wipo.int/amc/en/domains/cctld/ .ru и .рф в их число не входят, равно как и *.US*.

[3] http://www.icann.org/en/help/dndr/udrp/providers

2) у владельца доменного имени нет прав или законных интересов в отношении него;

3) доменное имя было зарегистрировано и используется недобросовестно.

При этом устанавливается примерный перечень обстоятельств, свидетельствующих о недобросовестности владельца доменного имени: предложения о его продаже правообладателю, регистрация с целью причинения вреда бизнесу конкурента, попытка привлечь внимание пользователей к сайту, паразитируя на известности товарного знака правообладателя (ст. 4 (*b*)).

UDRP содержит также и другой примерный перечень, на сей раз указывающий на добросовестную регистрацию и использование доменного имени: использование или приготовление к использованию доменного имени для добросовестного предложения товаров или услуг; известность владельца доменного имени под этим именем; использование его в некоммерческих целях (ст. 4 (*c*)).

По результатам рассмотрения заявления арбитражный центр имеет право принять одно из следующих трех решений: 1) об отказе в удовлетворении требований заявителя; 2) о прекращении регистрации доменного имени; 3) о передаче прав на доменное имя заявителю. Никакие иные способы защиты нарушенных прав в рамках *UDRP* недоступны правообладателям (например, возмещение убытков).

Таким образом, *UDRP* содержит не только процессуальные, но и материальные нормы, представляя собой достаточно автономный источник регулирования соответствующих отношений, обеспечиваемый технической возможностью соответствующего регистратора исполнить вынесенное решение без необходимости содействия каких-либо иных лиц или органов (судов, судебных приставов и т.п.). При этом арбитражные центры не применяют национальное законодательство какой-либо из стран, руководствуясь исключительно положениями *UDRP*, что придает данной процедуре поистине внегосударственный характер[1].

Уникальность *UDRP* заключается еще и в том, что рассмотрение споров в рамках данной процедуры не охватывается традиционным понятием третейского разбирательства. Во-первых, для рассмотрения дела в третейском суде необходимо согласие на то всех сторон будущего

[1] С.А. Бабкин видит в *UDRP* наиболее яркий пример «экстерриториального» «интернет-права», успех которого может подвигнуть *ICANN* к дальнейшим нормотворческим инициативам (см.: *Бабкин С.А.* Интеллектуальная собственность в сети Интернет. С. 492).

разбирательства, выраженное в соглашении (арбитражной оговорки)[1]. В *UDRP* данный признак отсутствует, так как заявитель не имеет никаких предварительных соглашений с владельцем доменного имени, соответствующее соглашение связывает владельца доменного имени и регистратора. Получается весьма специфическая «арбитражная» оговорка в пользу заранее неопределенного лица[2]. Во-вторых, наличие арбитражной оговорки по общему правилу препятствует рассмотрению дела в государственном суде[3], в то время как заявитель по *UDRP* никоим образом не ограничен в возможности обращения за защитой своих прав в государственные суды. В-третьих, как отмечалось выше, решения, вынесенные в рамках *UDRP*, обладают качеством самоисполнимости, свойствами которой не обладают решения обычных третейских судов, предполагающие последующее их принудительное исполнение в рамках процедуры с участием государственных судов и иных исполнительных органов власти. В-четвертых, все решения, вынесенные в рамках *UDRP*, являются общедоступными, в то время как решения обычных арбитражей обычно носят конфиденциальный характер и предоставляются лишь сторонам по делу[4].

Представляет интерес рассмотрение вопроса о правовой природе разбирательства, проводимого в рамках *UDRP* по российскому праву. Очевидно, что в свете вышеуказанных отличий от классического третейского разбирательства оно не может быть отнесено к таковому. По мнению В.Б. Наумова и Д. Королева, «по российскому законодательству решение административной комиссии по *UDRP* – это продукт своеобразной системы услуг по предоставлению экспертной информации в спорах о доменах, экспертное заключение с рядом элементов третейского разбирательства»[5]. Правда, данный «продукт», по мнению ряда специалистов, не очень сочетается с российской правовой системой.

---

[1] См., например: ст. 5 Федерального закона от 24 июля 2002 г. № 102-ФЗ «О третейских судах в Российской Федерации» (далее – Закон о третейских судах): спор может быть передан на разрешение третейского суда при наличии заключенного между сторонами третейского соглашения; ст. 7 Закона РФ от 7 июля 1993 г. № 5338-I «О международном коммерческом арбитраже»: арбитражное соглашение – это соглашение сторон о передаче в арбитраж всех или определенных споров, которые возникли или могут возникнуть между ними в связи с каким-либо конкретным правоотношением, независимо от того, носило оно договорный характер или нет.

[2] *Бабкин С.А.* Интеллектуальная собственность в сети Интернет. С. 488.

[3] См.: подп. 6 п. 1 ст. 148 АПК РФ.

[4] *Woodard E.* UDRP, ADR, and Arbitration- Using Proven Solutions to Address Perceived Problems with the UDRP // Fordham Intell. Prop. Media & Ent. L.J. No 19. 2009. P. 1186.

[5] *Наумов В., Королев Д.* Процессуальный статус *UDRP* в России: возможности и парадоксы // http://www.russianlaw.net/law/doc/a32.htm

В соответствии с ч. 3 ст. 5 Закона о третейских судах «третейское соглашение о разрешении спора по договору, условия которого определены одной из сторон в формулярах или иных стандартных формах и могли быть приняты другой стороной не иначе как путем присоединения к предложенному договору в целом (договор присоединения), действительно, если такое соглашение заключено после возникновения оснований для предъявления иска». Это означает, по мнению А.Г. Серго и К.В. Сокерина, что включение положений о рассмотрении споров в порядке *UDRP* в договор о регистрации доменного имени в зоне *.ru*, и .рф является ничтожным[1]. А.В. Незнамов утверждает о том, что «формально положения о подведомственности спора о доменных именах некоему третейскому суду (административному трибуналу при какой-либо негосударственной структуре, коей является, например, *ICANN*) не могут применяться в Российской Федерации в силу того, что такого рода третейские соглашения не будут действительны»[2].

Формально-юридически данные позиции представляются вполне корректными при условии квалификации разбирательства в рамках процедуры *UDRP* в качестве третейского, что, несмотря на все отличия от такового, вполне возможно в отсутствие какой-либо иной признаваемой процессуальным законодательством Российской Федерации формы рассмотрения споров, кроме судебной или третейской. Тем не менее на практике данная позиция вряд ли актуальна: во-первых, существующие в Российской Федерации Правила регистрации доменных имен не содержат положений о *UDRP*, а владельцы функциональных доменных имен верхнего уровня вряд ли смогут с успехом ссылаться на нормы российского законодательства при рассмотрении соответствующих споров ввиду автономности норм *UDRP* и самоисполнимого характера выносимого арбитражным центром решения. Предложения же о создании российского аналога *UDRP* (*RuDRP*), будучи интересными в теории, вряд ли имеют серьезные перспективы на практике[3]. Если они будут отличаться от *UDRP*, то не выдержат в пограничных ситуациях конкуренции с *UDRP* в силу того, что Россия не имеет того влияния на развитие Интернета, которое имеют США и американские компании вроде *ICANN*. Если же они не будут отличаться от *UDRP*, то речь в таком

[1] *Серго А.Г.*, *Сокерин К.В.* Особенности защиты права на доменное имя // Юрист. 2007. № 6.

[2] *Незнамов А.В.* Подведомственность доменных споров специализированным центрам в системе критериев национальной подведомственности // Арбитражный и гражданский процесс. 2010. № 2.

[3] Подобно тому как не имеет практической ценности создание специальной «адаптированной для России» свободной лицензии.

случае будет идти скорее не о создании параллельного механизма, а об адаптации *UDRP* к российским реалиям, что не одно и то же.

Примечательно другое. Право, как известно, не терпит пробелов в регулировании. Не дожидаясь внесения каких-либо изменений в законодательные акты, ключевые положения *UDRP* были имплементированы в российское законодательство в порядке судебного нормотворчества ВАС РФ. Впервые это произошло в постановлении по делу «ДенСо», суть которого сводилась к следующему. Российская компания, общество «ДенСо», зарегистрировала у регистратора «*Denso Domain*» права на доменное имя *denso.com*. Впоследствии японская компания «*Denso Corporation*» обратилась в арбитражный центр ВОИС с жалобой и требованием о передаче ей этого доменного имени, поскольку его регистрацией нарушены ее исключительные права на товарный знак «*denso*» и фирменное наименование. Решением арбитражного центра ВОИС требование компании «*Denso Corporation*» о передаче ей названного доменного имени удовлетворено.

Общество «ДенСо», не согласившись с данным решением арбитражного центра, обратилось в Арбитражный суд г. Санкт-Петербурга и Ленинградской области с иском о признании права пользования доменом *denso.com*. Суд отказал в иске, сославшись на ст. 10 *bis* Конвенции по охране промышленной собственности, согласно которой под недобросовестной понимается всякий акт конкуренции, противоречащий честным обычаям в промышленных и торговых делах, к которым суд отнес положения *UDRP*, на применение которых общество «ДенСо» согласилось при регистрации своего доменного имени. После ряда последующих рассмотрений дела в итоге апелляционная инстанция признала за истцом право пользования доменным именем, указав, что общество «ДенСо» не является конкурентом компании, не размещает на своем сайте информацию о товарах и услугах, в отношении которых зарегистрирован товарный знак компании, а использует в качестве доменного имени свое фирменное наименование, свой товарный знак и не предлагает спорное доменное имя к продаже[1]. Кассационная инстанция оставила данное решение без изменений[2].

Президиум ВАС РФ, отменяя решения, указал, что суд первой инстанции правильно оценивал действия общества «ДенСо» с учетом соответствия их требованиям названных документов *ICANN* и исходил

[1] Постановление Тринадцатого арбитражного апелляционного суда от 5 октября 2007 г. по делу № А56-46111/2003.

[2] Постановление ФАС Северо-Западного округа от 11 января 2008 г. по делу № А56-46111/2003.

из того, что регистрация доменного имени может быть аннулирована, если будет доказано, что:

1) доменное имя идентично или сходно до степени смешения с товарным знаком третьего лица;

2) у владельца доменного имени нет каких-либо законных прав и интересов в отношении доменного имени;

3) доменное имя зарегистрировано и используется недобросовестно.

Первое условие было удовлетворено ввиду того, что доменное имя *denso.com* фактически воспроизводило товарный знак японской компании «*Denso Corporation*».

В отношении второго условия Президиум ВАС РФ указал, что на момент регистрации доменного имени *denso.com* за обществом «ДенСо» (12.10.2000) у него не было прав на товарный знак с таким же обозначением. Фирменное наименование общества также не могло свидетельствовать о наличии законных прав в отношении доменного имени, поскольку оно было зарегистрировано за день (11.10.2000) до получения прав на доменное имя *denso.com* и никогда не использовалось для реального предложения товаров и услуг под данным наименованием.

Применительно к третьему условию Президиум ВАС РФ сделал вывод о том, что общество «ДенСо» знало или не могло не знать о существовании правообладателя товарного знака *denso* – японской компании «*Denso Corporation*»; у общества не было реального намерения самому использовать спорное обозначение в коммерческом обороте, регистрация товарного знака со сходным словесным обозначением преследовала лишь цель избежать аннулирования регистрации доменного имени в соответствии с Единообразной политикой по разрешению споров в связи с доменными именами *ICANN*. Все это в совокупности свидетельствовало о недобросовестности общества «ДенСо».

Таким образом, ВАС РФ фактически благословил использование российскими судами ключевых положений *UDRP* при разрешении конфликтов между правообладателями товарных знаков и фирменных наименований и владельцами доменных имен. В Постановлении от 18 мая 2011 г. № 18012/10 по делу о доменном имени *mumm.ru* Президиум ВАС РФ еще раз воспроизвел содержащиеся в Постановлении по делу «ДенСо» три критерия процедуры *UDRP*. Так что в настоящее время их вполне можно считать составной частью правовой системы Российской Федерации.

Глава 6. Цифровой контент и виртуальная «собственность»

§ 1. Понятие цифрового контента и основные бизнес-модели его распространения

Ранее уже говорилось, что все многообразие заключаемых в сети Интернет договоров можно условно разделить на две большие группы: 1) договоры, которые заключаются в сети Интернет, но исполняются в реальном мире, и 2) договоры, которые заключаются и *исполняются* в сети Интернет.

Распространение цифрового контента является типичным примером второго типа договоров. Оно может принимать различные формы: реализация электронных экземпляров произведений, предоставление удаленного доступа к произведению без предоставления экземпляра (потоковое аудио и видео, «программное обеспечение как услуга») и распространения цифрового контента особого рода – объектов виртуальной собственности (типичный пример – реализация различного рода внутриигровых объектов).

Следует сказать пару слов об используемой терминологии. В настоящее время в большинстве своем пользователи и интернет-провайдеры в России и за рубежом оперируют понятием «контент», распространяя его в равной мере как на опубликованное произведение в цифровой форме, так и на всю информацию, которая наполняет интернет-пространство. Данный подход представляется более предпочтительным, нежели традиционное разделение информации, в зависимости от ее принадлежности к определенной сфере права (произведения, сообщения СМИ, рекламные сообщения, научные факты и пр.). Как справедливо указывает Е. Войниканис, «информации и продуктов интеллектуального труда, фактов и произведений как самостоятельных величин с качественно отличной природой не существует. В отношении общедоступных телекомуникационных сетей, образующих цифровое пространство, а также различных цифровых устройств можно говорить *только* об информации – более или менее ценной, по-разному защищаемой, особо ценной для общества как некое благо и ценной с точки

зрения коммерческой деятельности. Чтобы конкретизировать предмет регулирования, можно назвать такую информацию *контентом*»[1].

Последние исследования демонстрируют устойчивый рост рынков, связанных с дистрибуцией цифрового контента: музыкальная индустрия все более ориентируется на распространение цифровой музыки, потоковая демонстрация видео и услуга «видео по запросу» стали важной составляющей кинорынка, а доходы от электронных книг компенсируют спад от продаж печатных изданий[2]. Особый рост испытывает индустрия видеоигр, которая достаточно быстро адаптировалась к произошедшим изменениям в бизнес-моделях. Ведущим дистрибьютором игр в сети Интернет стал сервис *Steam*, который оказался успешным даже в России, где пиратство является настолько масштабной проблемой, что многие дистрибьюторы просто не хотят выходить на данный рынок. При этом, как отмечается, успех новых бизнес-моделей в сфере видеоигр кроется именно в отказе от физических носителей[3].

Помимо традиционных компьютерных игр все большие обороты набирают многопользовательские онлайн-игры, многие из которых бесплатны, а доход приносит продажа различных дополнительных функций и игрового инвентаря. Такого рода бесплатное распространение игр является помимо всего прочего эффективным способом борьбы с пиратством.

В целом появление феномена цифрового контента обязано своим развитием широкополосному доступу к сети Интернет: практически все объекты авторского права (произведения литературы, музыкальные произведения, фильмы, компьютерные программы) приобрели новое бытие в цифровой форме, которое позволяет их свободно распространять в рамках информационно-телекоммуникационных сетей. В результате появились параллельные системы распространения объектов авторских прав: традиционная (реализация на материальных носителях) и цифровая (реализация «электронных» экземпляров, предоставление удаленного доступа). При этом объект договора является одним и тем же, меняется лишь форма его доведения до потребителя. В то же время, несмотря на тождество объектов договора и экономической цели заключаемых договоров, их правовая квалификация и правовой режим с точки зрения сложившейся практики существенным образом различаются.

---

[1] *Войниканис Е.* Указ. соч. С. 35.

[2] Материалы регионального исследования «В стремлении к успеху» («*The Sky is Rising*»). Floor 64, 2013. http://www.techdirt.com/skyisrising2/

[3] Там же.

Распространение объектов авторских прав на традиционных материальных носителях осуществляется посредством договоров купли-продажи их экземпляров, где экземпляр выступает в качестве товара. Распространение объектов авторских прав в цифровой форме обычно осуществляется посредством лицензионных договоров, которые регламентируют порядок и пределы использования такого цифрового контента. При этом очевидны принципиальные различия правовых режимов, возникающих на основе указанных договоров. При приобретении экземпляра на материальном носителе права использования такого объекта в значительной степени регламентируются законом, в частности положениями об исчерпании прав (ст. 1272 ГК РФ), в случаях свободного использования произведения (ст. 1273–1275 ГК РФ), компьютерной программы (ст. 1280 ГК РФ). При приобретении цифрового контента его правовой режим устанавливается преимущественно лицензионным договором либо посредством договора оказания услуг. Тем самым регулирование возникающих отношений осуществляется в договорном порядке, а учитывая повсеместное использование в сети Интернет конструкций договора присоединения в виде *click-wrap-* и *browse-wrap*-соглашений, – фактически единолично правообладателем. Как следствие, многие права, предоставляемые правомерному владельцу экземпляра в силу закона, оказываются существенно ограниченными, особенно при подкреплении положений таких договоров средствами технической защиты авторских прав.

В связи с этим возникает ряд вопросов. Во-первых, насколько оправданно использование различных договорных конструкций применительно к однородным по существу отношениям? Возможно ли использование классического договора купли-продажи в отношении цифрового контента?[1] Применим ли принцип исчерпания прав и перечень случаев свободного использования произведения к цифровому контенту? Насколько применимо законодательство о защите прав потребителей к отношениям, возникающим при распространении цифрового контента?

Данные вопросы будут подробно рассмотрены далее. Однако следует оговориться, что на самом деле проблематика цифрового контента несколько шире. Многообразие возникающих в сети Интернет отношений не ограничивается лишь цифровым контентом в значении

[1] Данный вопрос особенно актуален в свете существующей неопределенности в правовой квалификации договоров, по которым распространяется программное обеспечение в «электронной форме», т.е. посредством предоставления ссылки в сети Интернет, по которой его можно скачать.

лицензируемых объектов авторского права. Существует достаточно большой блок объектов, которые в литературе и на практике обозначаются как объекты виртуальной собственности (*virtual property*). В качестве примеров приводятся внутриигровые объекты, приобретаемые за реальные деньги, и виртуальные аналоги реальных объектов, приобретаемые в виртуальных мирах вроде *Second Life*[1]. Данные объекты регулируются в настоящее время преимущественно в договорном порядке, в то же время обладая чертами, свойственными объектам права собственности и немалой экономической ценностью. Очевидно, что по мере развития электронной коммерции значение указанных объектов виртуальной собственности будет возрастать, что обусловливает целесообразность рассмотрения возможных способов ее регулирования и существующей зарубежной практике в данной области.

§ 2. Отличительные черты цифрового контента

Произведения, существующие в цифровой форме, обладают рядом существенных отличий от аналоговых произведений, которые накладывают существенный отпечаток на их правовой режим.

1. Информация, существующая в цифровой форме, обладает значительной степенью независимости от ее носителя. Это ее качество обозначается в литературе как «дематериализация информации»[2]. Информация может свободно перетекать с одного носителя на другой: с одного компьютера на другой, с *CD*-диска на флэш-носитель и т.п. Информация в аналоговой форме (печатные версии книг, виниловые пластинки, картины и т.п.), напротив, обладает более тесной связью с носителем, что обусловливает сложности в ее копировании и передаче. Легкость распространения цифрового контента создает дополнительные возможности для правообладателей, но в то же время и создает дополнительные стимулы для противоправных действий за счет снижения технических барьеров, свойственных традиционным носителям (необходимость специального оборудования, временны́е затраты и пр.)[3]. Эта особенность цифровой информации особенно

[1] *Second Life* – это трехмерный виртуальный мир с элементами социальной сети, который насчитывает свыше 1 млн активных пользователей. Проект был разработан и запущен в 2003 г. компанией «*Linden Lab*» // http://secondlife.com/

[2] *Graham Smith*. Op. cit. P. 16.

[3] The Digital Dilemma. Intellectual Property in the Information Age. National Academy Press. Washington, 2001. P. 38. Мало кто когда-либо крал компакт-диск или видеокассету из магазина. Но практически каждый когда-либо скачивал музыку или фильм с ресурсов, имеющих сомнительный статус.

усиливается спецификой сети Интернет, обеспечивающей легкость и дешевизну распространения информации безотносительно к ее характеру. Как следствие, поскольку то, что ранее было доступно лишь при наличии дорогостоящего оборудования и при прочих условиях, стало доступно отдельно взятому индивиду. Вследствие этого правообладатели стали больше внимания уделять контролю над частным использованием произведения.

2. Неразрывная взаимосвязь цифрового контента и процесса его копирования: для того чтобы получить к нему доступ, копия произведения или его фрагмент должны быть скопированы на устройство, с которого осуществляется доступ. Такое копирование осуществляется каждый раз, когда браузер реконструирует страницу веб-сайта или воспроизводит файл, содержащийся на нем. Просмотр фильма, прослушивание музыки, просмотр текста неизбежно влекут возникновение копий данных произведений или их фрагментов в памяти компьютера пользователя. Напротив, при прочтении печатной книги или просмотре видеокассеты не возникает никакой дополнительной копии произведения. Эта особенность цифрового контента неразрывно связана с основами функционирования компьютера, который является основным устройством, посредством которого он «потребляется». Разумеется, право должно учитывать такие особенности и отчасти уже это делает[1], поскольку в условиях, когда доступ к цифровой информации возможен лишь посредством ее копирования, контроль над ее копированием означает *контроль над доступом к ней*. В условиях, когда результаты интеллектуальной деятельности все чаще и чаще принимают цифровую форму, право интеллектуальной собственности постепенно превращается из средства защиты прав тех, кто создает интеллектуальные и культурные ценности, в сферу права, регулирующую доступ к информации и знанию[2].

3. Цифровая копия произведения неотличима от его оригинала. Если каждая последующая копия аналогового произведения была хуже оригинала (например, перезапись аудио- или видеокассеты), то в случае с цифровыми копиями можно говорить о потенциально бесконечном множестве копий, неотличимых от оригинала.

---

[1] В частности, не считается воспроизведением временная запись в память ЭВМ, если она составляет неотъемлемую и существенную часть технологического процесса, имеющего единственной целью правомерное использование произведения (подп. 2 п. 1 ст. 1270 ГК РФ). Схожие положения содержатся и в американском Законе об авторском праве (§ 117).

[2] *Войниканис Е.* Указ. соч. С. 114.

4. Цифровая информация является пластичной: она может быть подвергнута изменениям без особых сложностей. Если внесение изменений в печатную книгу или аналоговый экземпляр аудио- или видеозаписи может быть не таким простым делом, внесение изменений в информацию, размещенную на веб-сайте, может быть осуществлено без особых проблем. Подобная пластичность в совокупности с легкостью поиска оцифрованной информации за счет возможности ее индексирования создает беспрецедентные условия для создания производных произведений на ее основе. Как справедливо отмечается, для человека цифровой эпохи свобода означает не только свободу выражать свое мнение, а также не только свободу иметь доступ к информации, но и свободу творить, подразумевающую право на переработку и преобразование полученной информации[1]. Возможность использования потенциала цифровой информации для создания нового знания предполагает тем самым необходимость выработки более гибких условий переработки существующих произведений, нежели тех, которые имеют место быть сейчас.

5. Возможность одновременного доступа и использования одного экземпляра произведения в электронной форме множеством лиц. Если аналоговый экземпляр произведения (печатная книга или кассета) потенциально может использоваться весьма ограниченным кругом лиц в одно и то же время, то файл, размещенный на сервере, может быть использован тысячами лиц одновременно. Это создает условия для распространения цифрового контента путем предоставления доступа к нему в режиме онлайн, а также путем обеспечения доступности информационных ресурсов в целом.

6. Любое лицо, имеющее доступ к сети Интернет, может выступать публикатором цифрового контента. С одной стороны, это влечет беспрецедентные возможности для доведения своих идей и произведений до сведения третьих лиц без участия издательств, дистрибьюторов и иных посредников (так называемая дезинтермедиация). С другой стороны, как еще более чем 40 лет назад отмечал Герберт Симон, «в условиях богатства информации возникает бедность внимания»[2]. Чем больше контента доступно пользователю, тем сложнее ему ориентироваться в этом массиве и находить нужное, а также тем сложнее привлечь его внимание к определенному объекту. Для владельцев интернет-бизнеса многообразие цифрового контента влечет превращение внимания пользователя в ресурс, ценность которого обуслов-

[1] Там же. С. 204.

[2] *Simon H.* Designing Organizations for an Information-Rich World: Computers, Communications and Public Interest / ed. M. Greenberger. Baltimore, 1971.

лена его ограниченностью. Пользовательское внимание становится товаром особого рода, что находит свое отражение в новых моделях рекламы, приобретающей все более адресный характер и влечет ряд проблем в сфере защиты персональных данных пользователей и их права на частную жизнь.

§ 3. Лицензирование как основная модель распространения электронных экземпляров

Как отмечалось ранее, основной договорной моделью распространения цифрового контента в сети Интернет выступает лицензионный договор. На то есть ряд причин формально-догматического, исторического и утилитарного порядка.

Формально-юридически большинство объектов, распространяемых в сети Интернет, подпадают под понятие объектов авторского и смежного права (произведения науки, литературы и искусства, компьютерные программы, базы данных, фонограммы и пр.). Использование таких объектов возможно с согласия правообладателя, выраженного в лицензионном договоре, либо в случаях, прямо указанных в законе (ст. 1229 ГК РФ). При этом закон четко разделяет право собственности на материальный носитель и права на результат интеллектуальной деятельности, воплощенной в нем. Данные права существуют независимо друг от друга (ст. 1227 ГК РФ)[1]. Наличие в отношениях, связанных с распространением объектов авторского права, материальной составляющей в виде материальных носителей, выступающих объектом договоров, в рамках которых происходит переход права собственности на них, позволяет осуществлять данное разделение более-менее четко. Как только объект интеллектуальной собственности передается пользователю в электронной форме, а не на диске, становится все сложнее чувствовать разницу между правами на экземпляр и правами на использование самого объекта интеллектуальной собственности[2]. По причине отсутствия явно выраженного материального носителя стала неочевидной возможность применения положений об исчерпании прав, которые играют одну из ключевых ролей в определении прав, возникающих в силу закона при приобретении экземпляра про-

[1] Схожие положения содержатся в ст. 202 Закона об авторских правах США «авторское право или любое из исключительных прав, входящих в его состав, отлично от права собственности на материальный носитель, в котором произведение воплощено».

[2] *Moringiello J.* What Virtual Worlds Can Do for Property Law // Florida Law Review. No 62. 2010. P. 195.

изведения[1]. В силу нематериального характера предоставляемых прав и отсутствия материального носителя, сопровождающего произведение, неудивительно, что лицензионный договор становится основным источником прав и обязанностей сторон, возникающих в связи с распространением цифрового контента.

Историческая причина применения конструкции лицензионного договора к отношениям, связанным с распространением цифрового контента и виртуальной собственности, обусловлена особой ролью, которую сыграли сложившиеся практики распространения программного обеспечения. Дело в том, что люди склонны распространять на новые явления свои сложившиеся воззрения на вещи, которые наиболее близки по сути к такому новому явлению. Компьютерные программы с самого момента становления индустрии программного обеспечения распространялись «в связке» с лицензионными соглашениями. Теперь, когда пользователь принимает условия различного рода соглашений вроде «*Terms of Use*», «*Terms of Service*», существующих в сети Интернет в виде *click-wrap-* или *browse-wrap-*соглашений, он воспринимает их как нечто само собой разумеющееся, поскольку успел к ним привыкнуть в ходе использования компьютерных программ[2]. Лицензионные соглашения либо лицензионные условия в составе комплексных соглашений стали своего рода индустриальным стандартом в сферах, связанных с использованием высоких технологий, в том числе в сфере распространения цифрового контента[3].

Существуют и бесспорные положительные черты использования лицензионного договора. В совокупности с техническими средствами защиты авторских прав и адекватной платежной инфраструктурой он позволяет обеспечить доступ к произведениям и информации, предоставление которого традиционными средствами считалось бы нерентабельным или рискованным. Например, в виде предоставления ознакомительного доступа, возможности взять произведение «в прокат», предоставления более низких цен для некоммерческого использования произведения и т.п. В целом считается, что лицензирование обеспечивает более широкий выбор возможностей по обеспечению доступа к информации[4].

---

[1] Подробнее вопрос о возможности и целесообразности распространения положений об исчерпании права на «электронные» экземпляры будет рассмотрен далее.

[2] *Winston E.* Why Sell What You Can License – Contracting around Statutory Protection of Intellectual Property // George Mason Law Review. No 14. 2006. P. 100.

[3] См., например: Положения и условия *iTunes Store*: «Вы соглашаетесь с тем, что Продукты *iTunes* предоставляются Вам исключительно на условиях лицензии» // http://www.apple.com/legal/internet-services/itunes/ru/terms.html#SALE

[4] The Digital Dilemma. Intellectual Property in the Information Age. National Academy Press. Washington, 2001. P. 101.

Наконец, использование лицензионных договоров достаточно удобно для правообладателей и уполномоченных ими лиц, поскольку позволяет обеспечить гармонию с используемыми техническими средствами защиты авторских прав, которые становятся все более популярными в сфере распространения цифрового контента. Технические средства защиты авторских прав неразрывно связаны с правовым режимом, устанавливаемым в отношении объектов авторских прав, и их обход или устранение влекут те же последствия, что и нарушение исключительного права. Обосновать ограничения, налагаемые такими техническими средствами защиты авторских прав, гораздо проще, прибегнув к конструкции лицензионного договора, в которой правообладатель может единолично определить объем предоставляемых прав и их пределы. Напротив, как только речь идет о конструкциях вроде собственности и даже «собственности» в кавычках (вроде прав на средства, размещенные на банковском счете), любые ограничения, накладываемые на их дальнейшее использование, воспринимаются как исключение, но не общее правило. Лицензионный договор предоставляет тем самым больше возможностей для контроля над использованием цифрового контента, предоставляя правообладателю или иному уполномоченному им лицу (например, возможность расторжения договора в случае нежелательного поведения пользователя). Посредством конструкции лицензионного договора правообладатели стараются противопоставить имеющийся правовой арсенал существенно возросшим рискам несанкционированного распространения цифрового контента в сети Интернет. Как отмечается, «комбинация договорных и технологических мер приведет к уменьшению потребности в использовании систем правовой защиты *erga omnes*»[1], т.е. тех средств защиты, которые традиционно предоставлялись законодательством об интеллектуальной собственности.

§ 4. Распространение программного обеспечения в электронной форме посредством сети Интернет

Традиционные способы распространения компьютерных программ в виде коробочных версий (*retail version*) все более и более вытесняются их распространением в электронной форме: посредством предоставления ссылок для скачивания и в некоторых случаях также и ключей, необходимых для активации установленной программы. Это обусловлено

[1] *Hugenholtz B.* Code as Code, or the End of Intellectual Property as We Know It // Maastricht Journal of European and Comparative Law. 1999. No 6. P. 318.

простотой и оперативностью, которые имеют место быть при данной форме распространения программы: покупателю достаточно заполнить форму, оплатить программу с использованием одной из форм электронных платежей и доступ к программе появляется в считанные минуты. Это удобно и правообладателям, поскольку существенно сокращает их затраты на доведение программного продукта до конечного пользователя: отсутствует необходимость обеспечения физической доставки и прохождения необходимых таможенных процедур в случае импорта материальных носителей программы[1].

Однако правовая природа договоров, в рамках которых предоставляются подобного рода электронные экземпляры программных продуктов, является до сих пор неопределенной. Это во многом связано с существующими налоговыми аспектами распространения программного обеспечения. В соответствии с НК РФ не подлежит обложению НДС реализация прав использования компьютерных программ на основании лицензионных договоров (подп. 26 п. 1 ст. 149 НК РФ).

Данное положение было разъяснено Минфином России, который распространил действие данной льготы и на сублицензионные договоры[2]. Как следствие, дистрибьюторы и прочие лица, выступающие звеньями в цепочке посредников, участвующих в процессе реализации программных продуктов, начали для получения данной льготы всеми правдами и неправдами выдавать заключаемые ими договоры за лицензионные и сублицензионные. На сомнительность данной практики уже неоднократно указывалось в литературе[3]. Причиной указанной сомнительности является тот факт, что зарубежные правообладатели обычно не дают дистрибьюторам прав на установку и непосредственное использование программы, а дают лишь право

[1] В соответствии с письмом ФТС России от 17 марта 2006 г. № 15-14/8524 «О таможенном оформлении информации, передаваемой по сети Интернет» таможенному оформлению подлежит не информация (компьютерная программа, мобильный контент), перемещаемая в сети Интернет при помощи оптико-волоконной связи или по каналам спутниковой связи, а перемещаемый через таможенную границу Российской Федерации товар, содержащий указанную информацию, т.е. материальный носитель (лазерный диск, дискета, кассета и т.п.).

[2] Письмо Минфина России от 1 апреля 2008 г. № 03-07-15/44 «О взимании НДС с операций по передаче прав на использование результатов интеллектуальной деятельности».

[3] См., например: *Савельев А.И.* Лицензирование программного обеспечения в России: законодательство и практика; *Он же.* Отдельные вопросы применения норм об исчерпании прав в отношении программ для ЭВМ // Вестник гражданского права. 2011. № 3; *Домрачева Е.* Неоднозначная льгота // эж-Юрист. 2008. № 36; *Вычугжанин Р.А.* Лицензия на софт // эж-Юрист. 2009. № 3.

на распространение[1], в силу чего дистрибьютор не может передать конечному пользователю больше прав, чем имеет сам (п. 2 ст. 1238 ГК РФ). К тому же, с точки зрения самих правообладателей, право использования у конечного пользователя возникает, как правило, на основании лицензионного соглашения с конечным пользователем, заключаемым в упрощенном порядке, предусмотренном в п. 3 ст. 1286 ГК РФ (так называемые оберточные лицензии или *click-wrap*-лицензии). Данное соглашение заключается при загрузке или установке программного продукта. Однако, если право использования предоставляется на основании такого соглашения, легитимность которого не оспаривается ни в законодательстве, ни в судебной практике[2], оно не может одновременно предоставляться другим лицом на основании иного соглашения: одно и то же право не может возникнуть на основании двух разных соглашений с разными лицами. Таким образом, соглашения, заключаемые между посредниками и конечными пользователями в большинстве случаев не обладают признаками лицензионных или сублицензионных соглашений, так как по ним не предоставляется ни одного правомочия, входящего в состав исключительного права в соответствии со ст. 1270 ГК РФ.

Возникает вопрос, как тогда следует квалифицировать такие соглашения? Если в рамках такого договора осуществляется предоставление материального носителя, то такие договоры должны рассматриваться как договоры купли-продажи материальных носителей при условии, что предполагается последующее заключение лицензионного договора в порядке п. 3 ст. 1286 ГК РФ[3]. Однако вопрос в том, как квалифицировать аналогичные договоры, которые заключаются между посредниками и конечными пользователями и в рамках которых не предоставляется материальный носитель, а предоставляется лишь ссылка и (или) ключ активации.

Как отмечалось ранее, сублицензионным договором такие соглашения с гражданско-правовой точки зрения в большинстве случаев

---

[1] См., например: пояснения компании по вопросам лицензионной политики в решении Арбитражного суда г. Москвы от 6 сентября 2010 г. по делу № А40-80627/10-118-416; постановление ФАС Московского округа от 1 сентября 2011 г. № КА-А40/9419-11 по делу № А40-140882/10-129-522.

[2] Так, особенности правового режима таких соглашений были разъяснены в постановлении Пленума ВС РФ № 5 и Пленума ВАС РФ № 29 от 26 марта 2009 г. «О некоторых вопросах, возникших в связи с введением в действие части четвертой Гражданского кодекса Российской Федерации» (п. 38.2).

[3] Письмо Минфина России от 1 апреля 2008 г. № 03-07-15/44 «О взимании НДС с операций по передаче прав на использование результатов интеллектуальной деятельности».

назвать нельзя. На практике иногда такие отношения оформляются договором купли-продажи[1]. Данный подход представляет собой интерес, поскольку является следствием применения единого подхода к квалификации однородных по сути отношений. Действительно, на первый взгляд странно выглядит различная квалификация отношений по «продаже» одного и того же объекта в зависимости от использованного вида носителя.

Однако такая квалификация не укладывается в классические каноны положений о купле-продаже, объектом которой является товар, в качестве которого могут выступать лишь вещи (ст. 455 ГК РФ). Не очень помогает и п. 4 ст. 454 ГК РФ, устанавливающий возможность применения норм о договоре купли-продажи к продаже имущественных прав, если иное не вытекает из содержания и характера таких прав. Ведь в данном случае речь не идет о продаже имущественных прав в том смысле, о котором здесь идет речь, – договоре цессии имущественного права, в основании которого лежит договор купли-продажи[2]. Да и в доктрине нет единого мнения о том, насколько правомерно интерпретировать п. 4 ст. 454 ГК РФ как допускающий возможность существования договора купли-продажи, в котором в качестве товара выступает не вещь. Так, В.В. Витрянский полагает, что, поскольку имущественные права – самостоятельные объекты гражданских прав, не относящиеся к категории вещей, они не могут признаваться товаром по договору купли-продажи. Смысл п. 4 ст. 454 ГК РФ заключается в распространении действия правил о договоре купли-продажи на иные правоотношения, не относящиеся к этому договору, и такое распространение не может свидетельствовать о признании имущественных прав товаром, а сделки по их отчуждению (продаже) – договором купли-продажи[3]. Так что при всей привлекательности использования конструкции договора купли-продажи для случаев распространения компьютерных программ в электронной форме вряд ли такая конструкция укладывается в рамки действующего законодательства.

С точки зрения существа возникающих отношений «продавец» в данном случае выступает не столько в качестве продавца некоего

[1] В качестве примера можно привести практику интернет-дистрибьютора *Softkey*, согласно которой покупатель может приобрести программы на материальном носителе или в электронной форме с оформлением товарно-транспортной накладной по форме «Торг-12». См.: www.softkey.ru

[2] См., например: *Новоселова Л.А.* Сделки уступки права (требования) в коммерческой практике. Факторинг. М., 2003.

[3] См.: *Брагинский М.И., Витрянский В.В.* Договорное право. Книга вторая: Договоры о передаче имущества. С. 265–266.

материального объекта, сколько в качестве посредника, обеспечивающего возможность приобретения лицензионного (неконтрафактного) экземпляра программного продукта. Таким образом, квалификация указанных отношений в качестве посреднических услуг представляется наиболее адекватной, поскольку она корректно улавливает суть отношений и позволяет учитывать нематериальный характер предоставляемого «блага».

Таким образом, мы приходим к различной квалификации: при наличии материального носителя – купля-продажа, при электронной форме распространения компьютерной программы – посреднические услуги (как представляется, преимущественно агентского характера). *De lege ferenda*, возможно, имело бы смысл подумать о возможности распространения на данные отношения норм о договоре купли-продажи, «растянув» тем самым существующее понимание понятия «товар»[1]. Это позволило бы обеспечить единообразие правового регулирования однородных отношений по распространению программных продуктов и легитимировать существующую практику заключения многими дистрибьюторами договоров купли-продажи в отношении электронных экземпляров программ. Предоставляемый посредником электронный ключ или ссылку можно было бы сравнить с вручением ключей как способом символической передачи (*traditio symbolica*) имущества (ст. 574 ГК РФ): в обоих случаях совершения указанных действий достаточно для того, чтобы получатель смог воспользоваться своим правом. Другое дело, что, для того чтобы иметь возможность осуществлять такую передачу, лицо должно быть должным образом управомоченным, а это в контексте распространения программного обеспечения означает либо наличие лицензионного договора с правообладателем, либо распространение принципа исчерпания права на электронные экземпляры. При этом проблема, обозначенная в последнем варианте, занимает умы многих зарубежных специалистов в области права. Существует и достаточно противоречивая судебная практика по данному вопросу. Поскольку от того, как будет регламентироваться принцип исчерпания права, являющийся краеугольным камнем обеспечения баланса частных и публичных интересов в праве интеллектуальной

[1] Примечательно, что такой подход уже принят на вооружение в Европе. В деле UsedSoft GmbH v Oracle International Corp. Европейский суд указал, что скачивание программы и заключение лицензионного соглашения представляют собой явную передачу права собственности на экземпляр программы в обмен на равноценное экономическое вознаграждение. Способ передачи экземпляра компьютерной программы потребителю (скачивание с сайта, передача *CD*- или *DVD*-диска) при этом не играет роли, и с экономической точки зрения они абсолютно равнозначны (ECJ. Case C-128/11. 3 July 2012).

собственности, будет зависеть дальнейшее развитие правовых форм распространения цифрового контента, необходимо подробнее остановиться на данном вопросе.

§ 5. Исчерпание права и цифровой контент

Положения об исчерпании прав возникли еще на рубеже XIX–XX вв. Обычно в качестве их «родоначальника» указывают Германию, в которой они впервые были разработаны и применены в судебной практике[1]. В США доктрина исчерпания прав, именуемая обычно доктриной первой продажи (*first sale*), является творением судебной практики и окончательно сформировалась после решения Верховного суда США по делу *Bobbs-Merill Co. v. Straus*, рассмотренному в 1908 г. Имеет смысл несколько подробнее остановиться на данном решении, поскольку его логика имеет значение для рассмотрения проблематики распространения цифрового контента. Ведь именно под американское право «заточены» положения большинства используемых зарубежными правообладателями договоров, поэтому понимание мотивов включения тех или иных условий позволит лучше осмыслить их возможную применимость на российской почве.

В деле *Bobbs-Merill Co. v. Straus* истец продал книжному магазину экземпляры книг под условием, что цена перепродажи не будет ниже 1 долл., причем уведомление о данном ограничении было нанесено на каждый экземпляр книги, с указанием, что его несоблюдение будет являться нарушением авторских прав. Впоследствии книжный магазин перепродал данные экземпляры по цене ниже 1 долл. за каждый, что послужило поводом для предъявления иска со стороны правообладателя. Суд отверг доводы истца о нарушении его авторских прав, указав, что авторские права в данном случае ограничены возможностью определения условий первоначальной продажи экземпляров и не дают права контролировать условия, на которых осуществляется дальнейшая перепродажа. В противном случае признание такого права за правообладателем означало бы излишне широкое толкование закона в противоречии с его значением[2]. Год спустя соответствующие положения были внесены в Закон об авторском праве США 1909 г. В настоящее время доктрина первой продажи закреплена в ст. 109 Закона об авторском праве США

[1] *Пирогова В.В.* Исчерпание исключительных прав и параллельный импорт. М., 2008. С. 35. Автор ссылается при этом на работу Йозефа Колера, разработавшего учение об исчерпании патентных прав (*Kohler J.* Deutsches Patentrecht. Mancheim, 1978. S. 100).

[2] Bobbs-Merill Co. v. Straus. 210 U.S. 339, 350–351 (1908).

1976 г. (*U.S. Copyright Act*). Она предусматривает, что собственник (*owner*) копии произведения или фонограммы, правомерно созданной в соответствии с требованиями законодательства об авторском праве, вправе продать или иным образом совершить отчуждение такого экземпляра без согласия правообладателя[1].

В настоящее время нормы об исчерпании прав являются неотъемлемой частью любого современного законодательства в области интеллектуальной собственности[2]. Они выступают одним из важнейших ограничений исключительного права, установленных законом, и имеют своей целью создание условий для свободного обращения товаров. В частности, это достигается путем создания условий для возникновения так называемого вторичного рынка, объектами которого выступают подержанные товары, в том числе книги и аудиозаписи. Нормы об исчерпании права создают необходимые условия и для деятельности публичных библиотек. Таким образом, указанные положения делают результаты интеллектуальной деятельности более доступными для потребителей, выступая важным элементом баланса интересов общества и правообладателей[3].

В контексте распространения цифрового контента в сети Интернет нас будет интересовать вопрос о применимости положений об исчерпании прав на объекты авторских прав. При этом главный вопрос заключается в том, применимы ли данные положения к случаям распространения экземпляров произведений в электронной форме или нет.

В США Конгресс еще в 2001 г. дал отрицательный ответ на данный вопрос, отказавшись вносить изменения в § 109 Закона об авторских правах, которые должны были бы распространить его действие на цифровой контент. Основной причиной послужил негативный отзыв со стороны Бюро по охране авторских прав при Конгрессе США, который высказал опасения о возможных злоупотреблениях со стороны пользователей, особенно актуальных в свете развития пиринговых сетей[4].

---

[1] 17 U.S.C. § 109(a).

[2] В Европе соответствующие положения содержатся в национальном законодательстве государств – членов ЕС, а также нашли свое отражение в ст. 4 Директивы ЕС от 22 мая 2001 г. № 2001/29/ЕС «О гармонизации некоторых аспектов авторского права и смежных прав в информационном обществе» (Directive 2001/29/EC on the harmonisation of certain aspects of copyright and related rights in the information society) // OJ. 2001. L 167/10.

[3] *Reese A.* The First Sale Doctrine in the Era of Digital Networks // Boston College Law Review. No 44. 2003. P. 585.

[4] См. подробнее: *Eurie Hayes Smith IV.* Digital First Sale: Friend of Foe? // Cardozo Arts & Entertainment Law Journal. No 22. 2005. P. 369–370.

Суды также дают отрицательный ответ на вопрос о возможности распространения доктрины исчерпания прав на цифровой контент. Из недавних решений стоит упомянуть решение окружного суда г. Нью-Йорка, в котором суд указал, что доктрина исчерпания прав (первой продажи) по определению затрагивает только право на распространение. Она не распространяется на реализацию права на воспроизведение, которая имеет место при создании новой копии произведения. Если же копия произведения изготовлена неправомерно, то к такой копии указанная доктрина вообще неприменима. С технической точки зрения передать тот же самый экземпляр файла физически невозможно, поскольку запись на жесткий диск всегда ведет к появлению (воспроизведению) нового экземпляра. При этом, по мнению суда, неважно, сохраняется исходный файл у первоначального пользователя или нет. В результате суд признал незаконной деятельность ответчика, организовавшего веб-сайт, посредством которого пользователи могли продать ранее приобретенные ими на легальной основе музыкальные произведения в виде электронных файлов[1].

В Европе ответ на данный вопрос зависит от характера цифрового контента. Если речь идет о музыке, произведениях литературы, фильмах и иных объектах авторского права, которые подпадают под действие Директивы № 2001/29/ЕС «О гармонизации некоторых аспектов авторских и смежных прав в информационном обществе», то ответ отрицательный. В соответствии с п. 28, 29 преамбулы принцип исчерпания права действует только в случае продажи материальных носителей и из-под его действия исключаются случаи предоставления доступа в процессе оказания услуг, особенно онлайн-услуг.

Что же касается компьютерных программ, то здесь подход несколько иной. Компьютерные программы подпадают под особый режим, предусмотренный Директивой № 2009/24/ЕС «О правовой охране компьютерных программ». Статья 4 (2) данной Директивы предусматривает что первая продажа экземпляров компьютерной программы на территории Европейского союза правообладателем или с его согласия влечет исчерпание права на их распространение на всей территории Европейского союза. При этом в п. 7 преамбулы Директивы № 2009/24/ЕС указывается на ее применимость к любым компьютерным программам независимо от их формы.

Толкование данных положений дало Европейскому суду основания для распространения положений об исчерпании права на случаи распространения электронных экземпляров компьютерной программы.

[1] Capitol Records, LLC v. ReDigi, Inc., USDC S.D. N.Y., March 30, 2013.

В данном случае предметом рассмотрения был спор производителя программного обеспечения *Oracle* и компании *UsedSoft*, деятельность которой заключалась в скупке ставших ненужными пользователям лицензий на компьютерные программы и их последующей продаже заинтересованным лицам. По мнению Суда, с экономической точки зрения нет особой разницы между продажей программы на материальном носителе и предоставлением электронного экземпляра, поскольку иной подход предоставил бы правообладателю необоснованную экономическую выгоду, так как стоимость лицензии включает в себя вознаграждение за неограниченный срок использования программы. Таким образом, в данном решении речь идет о распространении принципа исчерпания прав только на те программы, которые не были предоставлены на основе срочного лицензионного договора. Важно подчеркнуть, что Европейский суд прямо указал на то, что данная позиция не распространяется на случаи приобретения лицом лицензий на большее количество пользователей, чем ему необходимо. Такое лицо не вправе, ссылаясь на принцип исчерпания права, разделять такую лицензию, отчуждать экземпляр программы с произвольно определенным им количеством пользовательских лицензий. Исчерпание права распространяется на экземпляр программы, а не на лицензионное соглашение (лицензии)[1].

Таким образом, в европейском праве применение принципа исчерпания прав к цифровому контенту носит весьма ограниченный характер и применяется к некоторым случаям распространения компьютерных программ в электронном виде.

Рассмотрим, как данный вопрос будет решен по российскому законодательству. В соответствии со ст. 1272 ГК РФ если оригинал или экземпляры правомерно опубликованного произведения введены в гражданский оборот на территории Российской Федерации путем их продажи или иного отчуждения, дальнейшее распространение оригинала или экземпляров произведения допускается без согласия правообладателя и без выплаты ему вознаграждения. Буквальное толкование положений ст. 1272 ГК РФ приводит к выводу о ее неприменимости к электронным версиям объектов авторского права. Дело в том, что ст. 1272 ГК РФ связывает наступление указанных в ней последствий не с любыми способами введения произведения в оборот, а лишь с теми, которые осуществлены «путем продажи или иного отчуждения» экземпляров. Продажа экземпляра, а также иное отчуждение всегда подразумевает его передачу от одного лица к другому, причем переданный и полученный

[1] UsedSoft GmbH v Oracle International Corp. ECJ. Case C-128/11. 3 July 2012.

экземпляр должны быть тождественны. Таким образом, в отсутствие факта передачи экземпляра пользователю, без чего невозможна такая продажа или иное отчуждение, отсутствуют и условия для применения ст. 1272 ГК РФ[1]. При электронной дистрибуции произведений пользователь, записывая («загружая») его на свой компьютер, создает новый экземпляр, *отличный от исходного*. На это прямо указывает п. 2 ст. 1270 ГК РФ, закрепляющий, что запись в память ЭВМ считается воспроизведением, а под воспроизведением произведения понимается изготовление экземпляра произведения или его части в любой материальной форме. Экземпляр произведения, который загружается пользователем и который был получен им в результате состоявшейся загрузки являются двумя *различными* экземплярами компьютерной программы. В данном случае следует говорить не столько о распространении в авторско-правовом смысле, сколько о воспроизведении, которое не охватывается ст. 1272 ГК РФ. Следовательно, правообладатель в таких случаях сохраняет за собой в полном объеме возможности по контролю за последующим распространением компьютерной программы в электронной форме. Разумеется, в таких случаях соответствующие ограничения, установленные в лицензионном соглашении, являются правомерными, а их несоблюдение является нарушением авторских прав со всеми вытекающими последствиями.

Если ответ на вопрос о возможности применения положений об исчерпании права к цифровому контенту *de lege lata* является более-менее очевидным, то ответ на вопрос о целесообразности распространения данных положений *de lege ferenda* не так прост, как кажется.

Сторонники распространения положений об исчерпании права на цифровой контент мотивируют это тем, что данный подход повышает доступность, минимизирует контроль правообладателей над частной жизнью пользователей и обеспечивает прозрачность договорных конструкций, подобную той, которая имеет место быть при приобретении традиционных носителей[2]. Некоторые авторы заходят настолько

[1] Конечно, можно попробовать истолковать понятие «иное отчуждение» расширительно и охватить им не только собственно ситуации, когда передается экземпляр, но и случаи, когда предоставляется право по его созданию. Но не следует забывать, что нормы об исчерпании прав являются частным случаем ограничений исключительного права, а всякое исключение не подлежит расширительному толкованию (см.: Комментарий к части четвертой Гражданского кодекса Российской Федерации (поглавный) / Г.Е. Авилов, К.В. Всеволожский, В.О. Калятин и др. / под ред. А.Л. Маковского. М., 2008. С. 412).

[2] *Tobin J.* Licensing as a Means of Providing Affordability and Accessibility in Digital Markets: Alternatives to a Digital First Sale Doctrine // Journal of Patent & Trademark Office Society. No 93. 2011. P. 175.

далеко, что в ультимативной форме заявляют, что отсутствие такой доктрины способствует развитию пиратства, поскольку недовольные потенциальные покупатели цифрового контента на вторичном рынке будут склонны к использованию пиратских продуктов[1].

Главной посылкой, лежащей в основе позиции сторонников данного подхода, является довод об эквивалентности произведения, распространяемого на материальном носителе, тому же самому произведению, распространяемому в электронной форме, что обусловливает схожий характер интересов покупателей. Однако при этом игнорируется весьма важное принципиальное различие между произведением на традиционном материальном носителе и его цифровым эквивалентом. Ранее уже отмечалось, что, для того чтобы создать копию произведения, распространенного на традиционном носителе, нужно приложить немало усилий. Ксерокопирование книги, приобретение чистой кассеты или диска с последующей записью на них музыки или фильма, организация «доставки» полученной копии до получателя – все это немалые издержки. Да и качество полученных аналоговых копий, как правило, значительно ниже оригинала. Все это в течение долгого времени служило достаточно эффективным превентивным фактором, препятствующим широкомасштабному пиратству. Цифровой контент может быть скопирован и распространен в сети Интернет с огромной легкостью, с минимальными затратами времени и средств и без потери качества. Этот очевидный факт является главной причиной, требующей особого отношения со стороны законодателя к регламентации условий осуществления цифровой дистрибуции.

Распространение положений об исчерпании права на цифровой контент потребует одновременного введения мер, которые позволили бы хоть как-то выправить появившийся дисбаланс между интересами правообладателей и пользователей. В Конгрессе США обсуждался вопрос о внедрении в пользовательское оборудование технологий *forward and delete*, которые гарантировали бы удаление с компьютера пользователя того экземпляра произведения, которое он распространяет дальше[2]. Очевидно, что реализация данной идеи на практике является крайне непростой задачей. Получившаяся в итоге система неизбежно будет допускать значительные перегибы в процессе функ-

[1] *Newman J.* Selling the Right to License: Examination of the First Sale Doctrine Through the Lens of UMG Recordings & Quanta Computer // Journal of Corporate Law. No 35. 2010. P. 849, 862.

[2] US Copyright Office, Dmca Section 104 Report 19 (Aug. 2001), available at http://www.copyright.gov/reports/studies/dmca/sec-104-report-vol-1.pdf

ционирования, ограничивая вполне законные права пользователей (на создание архивных копий, копирование произведения на другое устройство, принадлежащее этому же пользователю, и т.п.). Возникнет также вопрос о том, кто будет разработчиком и производителем такой системы и под чьим надзором она будет функционировать.

Поскольку разработка и внедрение такой системы вряд ли произойдут в обозримом будущем, правообладатели в ответ на распространение принципа исчерпания права на цифровой контент усилят использование технических средств защиты авторских прав, что вряд ли будет способствовать интересам потребителей. Ни для кого не секрет, что подобного рода средства весьма назойливы и способны значительно попортить нервы пользователям. Конечно, их можно обойти и устранить, но даже абстрагируясь от правовой квалификации подобных действий в качестве неправомерных, для их осуществления требуется наличие специальных навыков, которых у большинства пользователей просто нет. В результате может возникнуть ситуация, что на бумаге право на свободное распространение электронного экземпляра произведения есть, но реализовать его будет невозможно в силу применяемых технических средств защиты авторских прав (например, в процессе активации устанавливается привязка компьютерной программы к аппаратной части компьютера, изменения в которой влекут ее неработоспособность). Стоит ли бороться за введение того права, которое все равно не получится в большинстве случаев реализовать?

Да и с чисто теоретической точки зрения сложно обосновать целесообразность расширения сферы применения норм об исчерпании права. Если исходить из того, что их основная задача состоит в обеспечении доступности результатов интеллектуальной деятельности широкой общественности, то существующие средства распространения цифрового контента уже в значительной степени ее обеспечили. Если раньше, для того чтобы взять фильм в прокат или даже купить его, необходимо было идти в магазин, надеясь на то, что он имеется там в наличии, сейчас достаточно воспользоваться специализированным сервисом вроде *iTunes* и получить искомый продукт можно быстро и не выходя из дома, нередко по более низкой цене, чем при покупке экземпляра в обычном магазине. Таким образом, распространение контента в цифровой форме уже само по себе подразумевает его повышенную доступность для потребителя, в связи с чем дополнительное применение механизмов вроде положений об исчерпании права будет чрезмерным.

Применение доктрины исчерпания прав к цифровому контенту повлечет ограничение возможности правообладателя выпускать различные версии одного и того же произведения с разными ценами, в зависимости от категории потребителя или способа его использования. Так, например, некоммерческие версии программных продуктов нередко стоят дешевле, чем коммерческие. В то же время подобная ценовая дифференциация возможна лишь в том случае, когда она подкрепляется правовыми и техническими механизмами. Таким правовым механизмом является лицензионный договор, который позволяет правообладателям более адресно подходить к потребностям конечных пользователей, не заставляя их переплачивать за те функции, которые им не нужны. Снятие посредством применения положений об исчерпании права соответствующих ограничений повлечет минимизацию адресного подхода к потребностям отдельных групп потребителей и в итоге сузит их возможности выбора.

Представляется, что вышеизложенные аргументы свидетельствуют о нецелесообразности распространения положений об исчерпании права на цифровой контент. Вместо этого целесообразно продолжение использования лицензирования как основного регулятора отношений в данной области, хотя, возможно, с бóльшим контролем над добросовестностью условий таких договоров. Подобно тому, как распространение норм об исчерпании права на цифровой контент влечет значительный дисбаланс в ущерб правообладателям, абсолютизация их права на определение лицензионных условий влечет аналогичный дисбаланс, но уже в ущерб интересам пользователей. Правообладатель не должен иметь возможности перечеркивания в договорном порядке тех прав, которые предоставлены пользователю в силу закона (случаи свободного использования произведений), а равно использовать договорные условия для того, чтобы иметь возможность в значительной степени лишить пользователя того, на что он рассчитывал, заключая договор. В связи с этим необходимо обеспечить максимальную прозрачность и понятность условий таких лицензионных договоров, в частности перечень ограничений, сопровождающих использование такого цифрового контента. Так, например, если по условиям проката фильм может быть просмотрен в течение 30 дней, но не более 2 дней с момента начала просмотра, то такие условия должны быть в явной форме указаны в момент заключения договора (совершения оплаты, загрузки файла). Представляется, что транспарентность и ясность условий заключаемых в сети Интернет договоров имеют бóльшую практическую ценность для потребителя, чем распространение норм об исчерпании

права на приобретаемый цифровой контент. В таком случае пользователь будет иметь четкое представление о том, что он приобретает, и иметь возможность выбрать наиболее подходящий вариант.

В качестве примера удачного подхода к обеспечению наглядности и понятности условий лицензионного договора можно привести лицензии *Creative Commons*, которые помимо классического многостраничного текста условий лицензионного соглашения предусматривают краткое описание существенных условий лицензии, изложенное максимально доступным языком, а также наглядное отображение основных элементов лицензии в графической форме[1]. Представляется, что данные идеи вполне могли бы быть заимствованы и применительно к коммерческим лицензиям. Примечательно, что новая Директива ЕС № 2011/83/ЕС «О защите прав потребителей»[2] предусматривает дополнительные информационные обязанности предпринимателей, распространяющих цифровой контент на коммерческой основе. В частности, до потребителя должна быть доведена информация о функциональности цифрового контента и применяемых технических средствах защиты авторских прав, а также информация о его совместимости с аппаратным и программным обеспечением (ст. 5 (1) (*g*, *h*)).

§ 6. Предоставление удаленного доступа как особая модель распространения цифрового контента

Предоставление доступа к цифровому контенту в удаленном режиме без его передачи пользователю является одной из наиболее перспективных бизнес-моделей дистрибуции цифрового контента. В самом упрощенном виде суть данных отношений сводится к предоставлению пользователю возможности доступа к цифровому контенту (функционалу компьютерной программы, потоковому аудио или видео[3]) без предоставления его экземпляра. Поскольку в таком случае экземпляр произведения находится под полным контролем провайдера

[1] www.creativecommons.ru/licenses

[2] Directive 2011/83/EU «On consumer rights» // Official Journal of the European Union. L 304/64. 22.11.2011.

[3] Так, вещание интернет-радио производится по технологии потокового радио с вещательных серверов (*stream*-технология). Слушатель, подключаясь программой-клиентом (медиаплеером), получает файл, не имеющий окончания, который несет в себе аудиоинформацию. Данный файл сохраняется в буферной памяти медиаплеера всего несколько секунд для предотвращения «скачков» звука, обрабатывается плеером и исчезает из памяти по мере прослушивания (см.: *Сытенко Г.И.*, *Вилинов А.А.* Актуальные вопросы регулирования отношений по охране авторского и смежных прав в сети Интернет // Культура: управление, экономика, право. 2010. № 2).

(правообладателя или уполномоченного им лица), риск пиратства существенно снижен[1].

В связи с этим не может не интересовать вопрос о правовой природе отношений, складывающихся между провайдером удаленного доступа к информационному ресурсу и его клиентом. В настоящее время данный вопрос особенно актуален применительно к предоставлению удаленного доступа к функционалу компьютерных программ посредством сети Интернет, поэтому имеет смысл подробнее остановиться именно на этом вопросе, имея в виду, что соответствующие выводы *mutatis mutandis* будут применимы и к иным видам цифрового контента.

Предоставление удаленного доступа посредством сети Интернет к функционалу программного обеспечения обычно именуется на практике как *Software-as-a-Service* («программное обеспечение как услуга») или сокращенно: *SaaS*. В качестве синонима *SaaS* иногда используются термины *Software on demand* («программное обеспечение по требованию»), *application hosting* («хостинг приложений») или *cloud computing* («облачные вычисления»). Причем последнее используется все чаще и чаще, хотя понятие облачных вычислений несколько шире, чем понятие *SaaS*. Под облаком принято понимать обобщенное название совокупности сервисов и моделей развертывания, которые в свою очередь опираются на такие элементы, как стандартизация, автоматизация и оптимизация, с целью эффективной и согласованной доставки потребителю *IT*-сервисов по сети[2]. В соответствии с общепринятой классификацией, предложенной Национальным институтом стандартизации США (*NIST*), различают три модели облачных сервисов: *IaaS* (*Infrastructure as a Service* – инфраструктура как сервис), *PaaS* (*Platform as a Service* – платформа как сервис) и *SaaS* (*Software as a Service* – программное обеспечение как сервис)[3]. Частое употребление понятия «облачные вычисления

[1] Хотя и не исключен в принципе. Известная организация «*Business Software Alliance*» провела исследование, по результатам которого пришла к выводу, что существуют определенные формы пиратства и при распространении контента посредством облачных сервисов. К ним относятся, в частности, неправомерное предоставление идентификационных данных эккаунта третьим лицам; предоставление удаленного доступа к программному обеспечению в нарушение условий лицензионного соглашения с его правообладателем или при отсутствии оного. *Holleyman R.* Piracy in the Cloud: A Picture Is Starting to Emerge. July 19, 2012 // http://blog.bsa.org/2012/07/19/piracy-in-the-cloud-a-picture-is-starting-to-emerge/#sthash.8P6ugD8N.dpuf

[2] Путешествие в «облако»: практическое руководство по созданию и воплощению успешной облачной стратегии. Statecast. Frost & Sullivan. Август 2012. С. 2 // http://www.ibm.com/ru/services/vds/sce/stepping-into-the-cloud-ibm-ru.pdf

[3] The NIST Definition of Cloud Computing. Special publication 800-145. September 2011 // http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf

(сервисы)» применительно к *SaaS* необходимо учитывать, поскольку многие правовые вопросы, актуальные именно для *SaaS*, рассматриваются в работах, посвященных облачным вычислениям[1], а договоры *SaaS* могут именоваться договорами на предоставление «облачных» услуг, особенно если это договоры с иностранными провайдерами.

На первый взгляд особых проблем в квалификации данных отношений быть не должно: само название данного явления содержит недвусмысленный намек на его правовую природу. Однако не следует забывать, что обозначения тех или иных продуктов или бизнес-моделей в *IT*-сфере нередко носят маркетинговый характер и в связи с этим не обязаны точно передавать правовую суть явления.

Существует два основных типа договора, которые могут быть использованы для оформления *SaaS*-отношений: лицензионный договор и договор возмездного оказания услуг[2]. Рассмотрим подробнее аргументы за и против соответствующей квалификации.

В обоснование использования лицензионного договора можно высказать следующие аргументы.

1. Неисчерпывающий перечень правомочий, составляющих исключительное право обладателя авторского права на компьютерную программу. Статья 1270 ГК РФ сформулирована предельно широко и позволяет вводить иные способы использования программы с учетом развития технологий[3]. Использование компьютерной программы посредством получения удаленного доступа к ней через сеть Интернет вполне может подпасть под понятие особого способа использования, не поименованного в п. 2 ст. 1270 ГК РФ. Соответствующее правомо-

---

[1] См., например: *Marchini R.* Cloud Computing: A Practical Introduction to the Legal Issues. BSI. London, 2010; Cloud Computing Law / ed. by Christopher Millard. Oxford University Press. 2013.

[2] На практике также иногда встречается обозначение таких отношений в качестве «аренды ПО» (см., например: http://arenda1c.ru) или «аренды приложений» (http://cloud.croc.ru/services/saas.php). Учитывая, что объектом договора аренды по российскому праву могут быть только непотребляемые вещи (ст. 607 ГК РФ), говорить об аренде в юридическом смысле применительно к отношениям *SaaS* нельзя, впрочем, как и применительно к компьютерным программам в целом. Хотя, учитывая экономическое сходство отношений *SaaS* с арендой (временное пользование за плату), для маркетинговых и пояснительных целей вполне можно говорить об аренде ПО, главное, чтобы это потом не проникало в юридические документы. В зарубежной практике (преимущественно немецкой и австрийской) встречаются случаи квалификации отношений по удаленному предоставлению временного доступа к программе за плату в качестве аренды (см.: BGH 15.11.2006. XII ZR 120/04; *Sandra Manhardt.* Der «Software as a Service» –Vertrag: Vertragsrechtliche Aspekte neuer Formen der Softwareüberlassung. LexisNexis ARD ORAC. 2012).

[3] См.: Комментарий к части четвертой Гражданского кодекса Российской Федерации / под ред. А.Л. Маковского.

чие можно было бы условно обозначить как «предоставление доступа к программе посредством сети Интернет». В данном случае не следует путать данный способ использования программы с правомочием доведения до всеобщего сведения (подп. 11 п. 2 ст. 1270 ГК РФ), которое тоже относится к использованию произведения в сети Интернет. Применительно к отношениям *SaaS* доведение до всеобщего сведения (даже если его и можно толковать настолько широко, чтобы охватить ситуации доведения программы только до сведения заранее определенных, зарегистрированных пользователей) осуществляет *SaaS*-провайдер, пользователь не доводит программу ни до чьего сведения, напротив, он пользуется результатами такого доведения.

Помимо указанных соображений в обоснование лицензионной природы отношений *SaaS* можно привести мнение, согласно которому, «получая доступ к программе, размещенной на удаленно находящемся сервере, пользователь воспроизводит ее на экране своего монитора, т.е. начинает использовать программу для ЭВМ»[1].

2. Аргументы из разряда «здравого смысла». Можно говорить о том, что принципиального различия с точки зрения пользователя между использованием, скажем, текстового редактора, установленного на жесткий диск пользователя, и использованием той же самой программы в удаленном режиме нет. С функциональной точки зрения это одна и та же программа. Было бы глупо называть работу с ней использованием для целей законодательства об интеллектуальной собственности, требующим наличия лицензионного договора, а во втором случае – нет.

3. Налоговые соображения. Появление в налоговом законодательстве известной льготы по НДС применительно к реализации прав на компьютерные программы по лицензионным договорам (подп. 26 п. 2 ст. 149 НК РФ) в значительной степени деформировало сложившуюся практику распространения программного обеспечения в России. В погоне за указанной льготой участники оборота стараются представить в виде лицензионных договоров те соглашения, права и обязанности по которым должны регулироваться иными соглашениями (поставки, агентским договором и пр.). Отношения по предоставлению удаленного доступа к программе посредством сети Интернет также нередко становятся предметом налоговой оптимизации и оформляются лицензионным договором. Хотя справедливости ради надо отметить, что в данном случае есть хоть какие-то формальные основания для этого в отличие от ситуаций, когда речь идет о заключении лицензионных

[1] *Разуваев В.Э.* Софт как услуга // эж-Юрист. 2010. № 5.

и сублицензионных договоров при распространении экземпляров программ через цепочку посредников[1].

В обоснование применения договора возмездного оказания услуг можно привести следующие соображения.

1. Отмечается, что основные действия совершаются на стороне провайдера облачных услуг: «информация хранится и обрабатывается на оборудовании исполнителя. Логические операции также производятся на оборудовании исполнителя»[2]. Иными словами, взаимодействие пользователя с программным обеспечением осуществляется опосредованно, через действия провайдера облачных услуг, который должен обеспечить возможность осуществления такого взаимодействия в пределах, установленных договором. В связи с этим А. Серов задается вопросом: «как можно лично использовать то, к чему нет непосредственного доступа?»[3] Действительно, пользователь *SaaS* не имеет *технической* возможности использования программы без непосредственного и *постоянного* участия провайдера. Данный факт позволяет говорить о том, что характер связи между сторонами отношений *SaaS* носит характер, который более адекватно отражается в договоре оказания услуг, нежели в лицензионном договоре, который предполагает самостоятельное использование результата интеллектуальной деятельности лицензиатом в установленных пределах.

2. Аргументы из разряда «здравого смысла». Если следовать позиции сторонников квалификации отношений *SaaS* как лицензионных, получается, что любое посещение пользователем более-менее современного веб-сайта будет требовать заключения лицензионного договора. Такие сайты содержат множество компонентов, обычно написанных на *Javascript*, которые могут быть квалифицированы в качестве компьютерной программы и которые воспроизводятся на экране монитора. Однако вряд ли кто-то будет утверждать, что посещение таких сайтов и использование их функционала (например, кредитных калькуляторов

[1] Этот момент не учитывает А. Серов, который, придя к правильному по существу выводу о недоступности пользователю *SaaS* перечисленных в ст. 1270 ГК РФ способов использования программы, приходит к выводу о ничтожности оформляемых посредством лицензионного договора отношений *SaaS* по причине отсутствия в таком договоре предмета, являющегося его существенным условием. См.: *Серов А.* SaaS: программное обеспечение или услуга? // эж-Юрист. 2011. № 17. Оставляя в стороне допущенную автором неточность в квалификации последствий отсутствия существенного условия в виде ничтожности договора, в то время как это обычно влечет незаключенность договора, следует отметить, что столь категоричный вывод автора противоречит открытому перечню способов использования объекта авторского права, закрепленному в ст. 1270 ГК РФ.

[2] *Серов А.* SaaS: программное обеспечение или услуга?

[3] Там же.

или калькуляторов страховой премии) влекут возникновение лицензионных отношений. А если учесть, что в доктрине ведется серьезная дискуссия относительно возможности отнесения самих веб-сайтов к базам данных или компьютерным программам, «масштабы бедствия» становятся еще больше.

Попробуем ответить на вопрос о том, какой тип договора является наиболее адекватным применительно к *SaaS* с точки зрения существа возникающих отношений.

Одним из основных критерием «правильности» квалификации того или иного договора является возможность распространения на возникающие из него права и обязанности сторон того правового режима, который предусмотрен для соответствующего договора. Какой смысл, скажем, в квалификации договора, который является по существу куплей-продажей, в качестве договора поручения, если к нему все равно малоприменимы нормы о договоре поручения.

Если руководствоваться данным, достаточно очевидным критерием, то квалификация *SaaS* в качестве лицензионного договора с применением норм авторского права к данным отношениям становится весьма сомнительной. Дело в том, что авторское право и лицензионный договор на предоставление права пользования объектом авторского права тесно связаны с экземпляром произведения. Это проявляется в описании правомочий, входящих в состав авторского права (п. 2 ст. 1270 ГК РФ), среди которых из числа применимых к компьютерным программам следует указать воспроизведение, распространение путем продажи или иного отчуждения оригинала или экземпляров, импорт экземпляров в целях распространения, прокат, публичное исполнение, переработка, доведение до всеобщего сведения. Это проявляется и в регулировании случаев свободного использования компьютерной программы правомерным владельцем ее экземпляра (ст. 1280 ГК РФ): праве внести в компьютерную программу изменения и осуществить исправление явных ошибок в целях ее функционирования на технических средствах пользователя; праве изготовить копию для архивных целей или для замены правомерно приобретенного экземпляра; праве декомпилировать программу для ЭВМ. Применение норм об исчерпании права на компьютерную программу (ст. 1272 ГК РФ) также неразрывно связано с конкретным ее экземпляром.

Не трудно увидеть, что все приведенные выше положения предполагают в той или иной мере взаимодействие лицензиата с экземпляром компьютерной программы[1]. Ключевой чертой *SaaS* является

[1] *Серов А.* Указ. соч.

отсутствие факта передачи экземпляра во владение пользователя, контроль над программой сохраняется за правообладателем (уполномоченным лицом) в полном объеме. Именно *SaaS*-провайдер осуществляет использование программы в авторско-правовом смысле этого слова и если он не является правообладателем, должен получить необходимые правомочия, которые предоставляются на основании лицензионного договора. Но пользователь не осуществляет использование экземпляра программы каким бы то ни было способом, требующим вмешательства авторского права. Он получал результат использования программы другим лицом, подобно тому, как зритель в кинотеатре не является лицом, «использующим» произведение, он лишь потребляет ту услугу, которую предоставляет ему то лицо, которое действительно его использует.

Сложно согласиться с доводом о том, что, «получая доступ к программе, размещенной на удаленно находящемся сервере, пользователь воспроизводит ее на экране своего монитора, то есть начинает использовать программу для ЭВМ»[1]. Как известно, под воспроизведением в соответствии со ст. 1270 ГК РФ понимается «изготовление одного и более экземпляров произведения», а также «запись произведения на электронном носителе, в том числе запись в память ЭВМ». Как отмечалось ранее, в рамках *SaaS* программа не копируется (устанавливается) на компьютер пользователя. Тот факт, что некие ее фрагменты отображаются на экране монитора, не может считаться воспроизведением, поскольку такое отображение является следствием записи в память ЭВМ временного характера, составляющей неотъемлемую и существенную часть технологического процесса, и тем самым подпадает под исключение, указанное в подп. 1 п. 2 ст. 1270 ГК РФ.

Таким образом, большинство норм, составляющих правовой режим лицензионного договора, оказываются просто неприменимыми к *SaaS*. И такая несовместимость правового режима должна наталкивать на мысль о неправильности произведенной квалификации. В контексте *SaaS* утрачивает смысл даже применение норм о технических средствах защиты авторского права, поскольку они имеют смысл только «в связке» с конкретным экземпляром программного продукта, который выходит из-под контроля правообладателя.

В связи с вышеизложенным представляет интерес то, как подходят к решению вопроса о природе *SaaS* американские юристы.

В американской доктрине высказывается мнение, что *SaaS* может быть квалифицирован и в качестве услуги, и в качестве лицензионного

[1] *Разуваев В.Э.* Указ. соч.

договора. При этом решение о том, по какой модели конструировать отношения, принимает провайдер. Так, квалификация отношений в качестве услуги может быть выгодна из маркетинговых соображений и позволяет подчеркнуть новизну *SaaS*, тем самым сильнее противопоставив данный продукт традиционным лицензиям. Выбор модели также может иметь значение с точки зрения налогов, применяемых в соответствующих штатах[1]. Иногда квалификация отношений в качестве лицензии имеет преимущества и с точки зрения законодательства о банкротстве, поскольку позволяет лицензиату при определенных условиях сохранить право использования программы при возбуждении дела о банкротстве *SaaS*-провайдера[2].

Некоторые американские юристы более категорично подходят к квалификации *SaaS*. Поскольку американское авторское право тесно связано с понятием копии, то, по их мнению, об отношениях, регулируемых авторским правом, можно говорить только тогда, когда имеет место создание копии произведения; при отсутствии факта копирования произведения нет и необходимости в выдаче лицензии на его использование[3]. Да и те юристы, которые говорят о возможности квалификации отношений *SaaS* как лицензионных, руководствуются при этом преимущественно сиюминутно прагматичными соображениями, а не доводом о наибольшей адекватности такого типа договора применительно к *SaaS*. Примечательно, что большинство зарубежных провайдеров облачных сервисов (к числу которых относится и *SaaS*) квалифицируют возникающие отношения в качестве услуги[4].

В условиях существующей парадигмы авторского права, «зацикленного» на вопросах использования экземпляра произведения, отношения по предоставлению к ним удаленного доступа посредством сети Интернет наиболее адекватно регулируются в рамках договора на оказание услуг.

---

[1] *Landy G., Mastrobattista A.* The IT/Digital Legal Companion: A Comprehensive Business Guide to Software, IT, Internet, Media and IP Law. 2008. P. 367.

[2] См. § 365 (n) U.S. Bankruptcy Code. См.: *Guth S.* Contract Negotiation Handbook: Software as a Service. Virginia, 2013. P. 20–21.

[3] *Tollen D.* Don't Use License Agreements for Software as a Service. 12 September 2011. http://blog.techcontracts.com/2011/09/12/dont-use-license-agreements-for-software-as-a-service/; *Wolf C.* SaaS on a EULA? Get Some New Pants. 20 May 2013. http://www.cloudtweaks.com/2013/05/saas-on-a-eula-get-some-new-pants-2/

[4] См. подробный обзор предлагаемых соглашений 27 провайдеров *SaaS* (в частности, *Apple*, *Amazon*, *Google*, *IBM*, *Microsoft*, *Salesforce*): *Bradshaw S., Millard C., Walden I.* Contracts for Clouds: Comparison and Analysis of the Terms and Conditions of Cloud Computing Services // Queen Mary University of London, School of Law Legal Studies Research Paper. No 63/2010.

Однако здесь необходимо сделать несколько оговорок. Во-первых, конструкция договора оказания услуг, предусмотренная в гл. 39 ГК РФ, предусматривает именно *возмездное* оказание услуг. Многие облачные сервисы, в том числе и *SaaS*, могут являться безвозмездными в контексте положений ст. 423 ГК РФ, предусматривающей, что возмездным признается договор, по которому сторона должна получить плату или иное встречное предоставление. Конечно, компании, предоставляющие подобного рода бесплатные сервисы, не занимаются благотворительностью и имеют определенную выгоду от них: либо размещая рекламу и получая доход от рекламодателей, либо получая данные пользователей, либо «приучая» пользователей к продуктам своей компании, повышая узнаваемость бренда, и т.д. Так или иначе, подобного рода бизнес-выгода, не подпадая ни под один из объектов гражданских прав, указанных в ст. 128 ГК РФ, не может быть квалифицирована в качестве встречного предоставления с точки зрения ст. 423 ГК РФ. Учитывая, что возмездный характер договора оказания услуг является конститутивным признаком договора, указанного в гл. 39 ГК РФ, и Кодекс не содержит специальных норм, посвященных безвозмездному оказанию услуг, не остается ничего иного, как квалифицировать подобные договоры в качестве непоименованных с применением к ним общих положений об обязательствах и договорах, а положений гл. 39 ГК РФ – лишь по аналогии закона[1].

Во-вторых, квалификация *SaaS* в качестве договора оказания услуг (возмездного или непоименованного безвозмездного) не исключает возможность присутствия в нем определенной лицензионной составляющей. Это может быть связано с условиями таких договоров, предоставляющими провайдеру определенные права на информацию, размещаемую пользователями в облаке в процессе исполнения договора. В связи с тем что данная информация хранится на оборудовании провайдера, для юридической чистоты подобного рода отношений целесообразно иметь условия, регламентирующие статус такой информации. Другой пример – так называемое вспомогательное программное обеспечение (*enabling software*), которое клиент должен установить локально для того, чтобы иметь возможность воспользоваться услугой *SaaS*. Не всегда одного только браузера может быть достаточно для полноценного использования фукционала программы, предоставляемой

[1] Подробнее о правовом регулировании непоименованных договоров см.: *Савельев А.И.* Отдельные вопросы правового регулирования смешанных договоров в российском и зарубежном гражданском праве. С. 230; *Карапетов А.Г., Савельев А.И.* Свобода заключения непоименованных договоров и ее пределы // Вестник ВАС РФ. 2012. № 4.

в рамках *SaaS*. Разумеется, в таких случаях заключается отдельный лицензионный договор на использование таких вспомогательных программ и он может являться составной частью договора облачных услуг. Но в любом случае данные аспекты не составляют «ядра» возникающих отношений и не означают, что право, предоставляемое пользователю на использование программы, установленной на сервере *SaaS*-провайдера, является лицензионным.

Квалификация отношений *SaaS* в качестве договора оказания услуг имеет ряд практических последствий. Во-первых, она позволяет оптимизировать условия платежей. Если в лицензионном договоре вознаграждение подлежит уплате за сам факт предоставления права – фактическое использование программы не имеет значения[1], то посредством договора оказания услуг можно в полной мере реализовать схемы взимания платежей, характерных для *SaaS*, в соответствии с которыми оплате подлежит только период фактического использования программы.

Во-вторых, договор оказания услуг в большей степени приспособлен к регулированию вопросов качества сервиса. По мнению некоторых судов, ставить вопрос о качестве применительно к лицензионным договорам некорректно, поскольку «неисключительное право, не являясь вещью, не может быть некачественным»[2]. В отсутствие в части четвертой ГК РФ специальных положений о качестве объекта авторских прав такой подход имеет право на существование. Не исключено, что на него повлиял закрепленный в п. 1 ст. 1259 ГК РФ постулат авторского права о том, что «объектами авторских прав являются произведения науки, литературы и искусства *независимо от достоинств* (выделено мной. – *А.С.*)». Поэтому, каким бы ни было качество («достоинство») программного продукта, он все равно является охраноспособным, а следовательно, может выступать объектом лицензионного договора. Напротив, договоры на оказание услуг *SaaS* нередко содержат так называемые соглашения об уровне сервиса (*SLA*), которые детально регулируют вопросы доступности сервиса и иных условий, регламентирующих его качество. В их числе могут быть и вопросы функциональных характеристик программы, доступ к которой предоставляется в рамках *SaaS*[3].

---

[1] См.: постановление Пленума ВС РФ и Пленума ВАС РФ от 26 марта 2009 г. № 5/29 «О некоторых вопросах, возникших в связи с введением в действие части четвертой Гражданского кодекса Российской Федерации» (п. 13.7).

[2] Постановление ФАС Московского округа от 30 сентября 2009 г. № КГ-А40/9849-09, оставленное в силе Определением ВАС РФ от 25 января 2010 г. № ВАС-17883/09.

[3] См.: *Guth S.* Op. cit. P. 25 ff.

В-третьих, поскольку пользователь не приобретает экземпляр компьютерной программы, его нельзя привлечь к ответственности за нарушение авторских прав третьих лиц в случае, если программное обеспечение включает в себя компоненты, принадлежащие таким лицам[1]. В случае оценки ситуации в системе координат авторского права правообладатель может предъявить соответствующее требование любому пользователю. В случае с *SaaS* главным кандидатом на статус нарушителя является провайдер услуги подобно тому, как в случае несанкционированного показа фильма в кинотеатре правообладатель будет предъявлять требования не к зрителям, а к кинотеатру.

Наконец, наличие в законе специальных оснований для расторжения договора возмездного оказания услуг в виде императивной нормы ст. 782 ГК РФ также отличает правовой режим данного договора от лицензионного, в котором за неимением специальных императивных положений на сей счет в части четвертой ГК РФ данный вопрос будет регламентироваться в договорном порядке

Таким образом, можно сделать вывод о том, что, несмотря на наличие формальных оснований для квалификации отношений по предоставлению удаленного доступа к компьютерной программе посредством сети Интернет в качестве лицензионного договора, такая квалификация является нецелесообразной с практической точки зрения по причине неприменимости большей части положений, составляющих правовой режим такого договора. Квалификация таких отношений в качестве договора возмездного оказания услуг либо непоименованного договора при отсутствии встречного предоставления, предусмотренного ст. 423 ГК РФ, является наиболее целесообразной. Представляется, что указанные соображения применимы *mutatis mutandis* и к отношениям по предоставлению удаленного доступа и к иным объектам авторских прав.

Подобное положение вещей вызвано тем фактом, что вся система правомочий, входящих в состав авторского права субъекта, рассчитана на распространение копий (экземпляров) произведений и воспринимается их как основной способ реализации авторского права. Тем самым не учитываются современные бизнес-модели распространения цифрового контента, при которых экземпляры не распространяются, а предоставляется лишь некое право доступа к объектам авторского права. По мере роста популярности таких моделей может оказаться так, что авторское право окажется «за бортом» и регламентация доступа к объектам авторского права будет осуществляться средствами

[1] *Tollen D.* Op. cit.

договорного права без учета интересов общества. Представляется, что в эпоху Интернета право интеллектуальной собственности все же должно регламентировать вопросы, связанные с предоставлением доступа к произведениям в цифровой форме безотносительно к форме их «доставки» потребителю. Однако для этого необходим пересмотр принципов авторского права и переориентация его направленности на регламентацию правового режима использования экземпляров произведения на регламентацию прав доступа к таким произведениям. Но рассмотрение данного вопроса определенно уже выходит за рамки данной работы и вполне может претендовать на отдельное исследование больших размеров.

§ 7. Виртуальная «собственность»

Рынок цифрового контента не ограничивается лишь предоставлением электронных экземпляров традиционных объектов авторских и смежных прав, а также предоставлением удаленного доступа к ним. Существует еще один сегмент, который пока находится в тени и не получает особого внимания со стороны юристов. Речь идет как о различного рода персонажах (аватарах) онлайновых игр и внутриигровых объектах, так и о виртуальных аналогах реальных объектов, реализуемых в виртуальных мирах вроде *Second Life*, которые приобретаются прямо или косвенно за реальные деньги.

Многие онлайн-игры и виртуальные миры обладают развитой виртуальной экономикой с собственной валютой, выступая источником доходов для правообладателей. Некоторые разработчики виртуальных миров даже приглашают экономистов, которые работают над моделями таких виртуальных экономик[1]. Так, в 2009 г. суммарная стоимость рынка виртуальной экономики проекта *Second Life* составила 567 млн долл.[2] Есть все основания полагать, что она будет с каждым годом только расти.

Вместе с тем правовой режим такого рода объектов, которые для целей данной главы можно обозначить как «объекты виртуальной собственности», остается неопределенным. В подавляющем большинстве случаев их статус регламентируется правообладателем того программного продукта, в рамках которого осуществляется циркуляция таких

[1] В качестве примера можно привести обширную литературу, посвященную тому, как можно делать деньги и вести предпринимательскую деятельность в виртуальном мире *Second Life*. *Freedman R.* How to Make Real Money in Second Life: Boost Your Business, Market Your Services, and Sell Your Products in the World's Hottest Virtual Community. McGraw-Hill. N.Y., 2008; *Terdiman D.* The Entrepreneur's Guide to Second Life. Indiana. 2008.

[2] http://venturebeat.com/2010/01/19/second-lifes-economy-grows-65-to-567m/

объектов. В качестве инструмента регламентации используются уже знакомые соглашения с конечным пользователем (*End User License Agreement, Terms of Service, Terms of Use*)[1].

Для того чтобы продемонстрировать, к чему может привести такой подход на практике, имеет смысл привести пару реальных судебных споров, где рассматривались вопросы принадлежности объектов виртуальной собственности.

В первом из них в качестве истца выступал Марк Брэг (*Marc Bragg*), юрист из штата Пенсильвания, который являлся активным пользователем *Second Life*. Иск касался неправомерного лишения его «права собственности» на виртуальные земельные участки ответчиком – компанией *Linden Lab*, выступающей правообладателем программного продукта *Second Life*. В процессе использования данной программы истец приобрел ряд земельных участков за валюту, принятую в данном виртуальном пространстве (так называемые линдены), которая может быть приобретена за реальные деньги. Стоимость аккаунта истца (его виртуального «я» в виртуальном мире *Second Life*) составляла порядка 2000 долл. Один из виртуальных земельных участков был приобретен Брэгом с использованием уязвимости программного кода *Second Life*, которая позволила ему приобрести его достаточно дешево. Данное действие являлось нарушением Правил оказания услуги, и как следствие *Linden Lab* заморозила аккаунт истца и стерла его имя из реестра «прав» на все земельные участки, в том числе и те, которые были приобретены им без каких-либо нарушений. Впоследствии данные участки были перепроданы *Linden Lab* другим пользователям без выплаты какой-либо компенсации истцу. Истец ссылался на то, что подобные действия ответчика составляют деликт, именуемый «конверсия» (*conversion*), суть которого сводится к неправомерному присвоению чужого имущества[2]. К сожалению, суду не была предоставлена возможность вплотную заняться вопросами квалификации существующих отношений, поскольку, после того как он признал недействительной арбитражную оговорку в Правилах оказания услуги, дело завершилось мировым соглашением[3].

Другой пример также связан с проектом *Second Life*, но касается уже нарушения интеллектуальных прав на виртуальные объекты посредством действий, совершенных другим пользователем в виртуальном

[1] *Fairfield J.* Virtual Property // Boston University Law Review. No 85. 2005. P. 1050; *Benjamin Tyson Duranske*. Virtual Law: Navigating the Legal Landscape of Virtual Worlds. Chicago: ABA Publishing, 2008. P. 27.

[2] Restatement (second) of Torts. § 222A (1965).

[3] Bragg v. Linden Research, Inc. 487 F. Supp. 2d 593, 603 (E.D. Pa. 2007).

мире. В данном деле истец выступал в качестве продавца различного рода виртуальных товаров эротического характера, которые обладали оригинальным дизайном и пользовались популярностью среди других пользователей. Ответчик также являлся продавцом, только иного рода: вместо разработки собственных оригинальных продуктов он копировал продукты других лиц и продавал их по меньшей цене. Получался своего рода виртуальный контрафакт. Истец обратился в суд с иском о нарушении его авторских прав и прав на товарный знак. Ответчик не стал возражать по существу предъявленных требований, ограничившись заявлением о том, что «истцы могут говорить что угодно. Но это всего лишь видеоигра». Суд счел иначе и вынес решение против ответчика, обязав его выплатить 525 долл., а также предоставить истцам информацию о всех сделках, совершенных им в *Second Life*[1].

Как видно из указанных примеров, отношения, возникающие в виртуальных мирах, весьма схожи с теми, которые имеют место в реальном мире: соответствущие объекты приобретаются или могут быть приобретены за реальные деньги, для их идентификации используются средства индивидуализации, аналогичные товарным знакам, и т.д. То, что их отличает от классических отношений, регулируемых правом, – так это их виртуальный характер.

В связи с этим один из первых вопросов, требующих своего разрешения, – это определение виртуального мира и его соотношения с обычной компьютерной игрой. Специалистами в области виртуальных технологий приводится две основных черты виртуального мира: 1) стабильность и 2) динамичность[2]. Стабильность проявляется в том, что виртуальный мир не прекращает своего существования с выключением пользователем своего компьютера. Динамичность проявляется в постоянных изменениях, происходящих в данном мире.

Все виртуальные миры принято делить на скриптовые и нескриптовые. В скриптовых виртуальных мирах пользователи лишены возможности создания виртуальных объектов и получают доступ к новым объектам по мере прохождения игры. Типичный пример такого виртуального мира – *World of Warcraft*. Нескриптовый виртуальный мир позволяет пользователям создавать собственный контент и объекты. Здесь наиболее ярким примером является *Second Life*.

Указанные различия во многом предопределяют подходы правообладателей к вопросам регламентации прав пользователей на вирту-

[1] Eros, LLC v. Simon. 1:07-cv-04447-SLT-JMA (E.D.N.Y. 2008).

[2] *Benjamin Tyson Duranske.* Op. cit. P. 3; *Lipson A., Brain R.* Computer and Video Game Law: Cases, Statutes, Forms, Problems & Materials. 2009. P. 505–506.

альные объекты. Поскольку в нескриптовых мирах основной интерес пользователей заключается в прогрессе персонажа, правообладатели запрещают продажу виртуальных объектов и аккаунтов[1]. В противном случае получался бы существенный дисбаланс: игрок, который только что присоединился к игре, мог бы сравняться по своим показателям с опытными игроками лишь за счет значительных финансовых вливаний в игру, что отпугнуло бы многих пользователей.

Напротив, в нескриптовых виртуальных мирах пользователи имеют возможность создания своего контента и распоряжения им. Такой контент может быть создан из текстур и «строительных блоков», предоставленных правообладателем, что требует немалых затрат времени и сил подобно тому, как это имеет место в реальном мире. Другой вариант – пользователь может купить готовый продукт и заняться в виртуальном мире тем, к чему лежит его душа. В связи с этим интерес представляет то, как регламентируется статус таких объектов не во внутриигровых инструкциях, а в соглашении между правообладателем и пользователем, которое является основным документом, регулирующим правовой статус пользователя в виртуальном мире. И здесь открывается удивительная картина. Максимум, что обычно предоставляется пользователю, – это некое неисключительное право использования соответствующей компьютерной программы. При этом указывается на отсутствие у пользователей каких-либо прав на контент[2]. Что же касается виртуальной валюты, то ее нельзя обменять на реальные деньги в случае удаления аккаунта, предъявив соответствующие требования правообладателю. Можно только продать ее другим заинтересованным пользователям.

Во многом это объясняется тем, что правообладатели заинтересованы в защите произведенных инвестиций в разработку виртуального мира, а также в осуществлении контроля над тем, что там происходит[3]. Признание виртуальной собственности собственностью в правовом смысле повлечет возможную ответственность правообладателей за внесение изменений в виртуальный мир, которые могут повлечь ущерб или снижение стоимости таких объектов[4]. Например, в результате

[1] В правилах *World of Warcraft* установлен запрет на продажу аккаунтов игроков и указано, что пользователи не приобретают прав или титула на виртуальные товары или валюту (см.: World of Warcraft, Terms of Use Agreement // http://www.worldofwarcraft.com/legal/termsofuse.html).

[2] Second Life, Terms of Service // http://secondlife.com/corporate/tos.php, 1.3

[3] *Westbrook T.* Owned: Finding a Place for Virtual World Property Rights // Michigan State Law Review. No 2006. 2006. P. 788–789.

[4] *Bartle R.*, Bartle of Virtual Property. The Themis Group. April 2004, available at: http://www.themis-group.com/uploads/Bartle%20of3/o20Virtual%20Property.pdf

создания новых объектов виртуальной недвижимости рядом с теми, которые были ранее приобретены пользователями, их стоимость может существенно снизиться и инвестиции, сделанные пользователями, обесценятся. Или другой пример. Если ценность какого-либо виртуального объекта неразрывно связана с его редкостью, введение правообладателем в игру дополнительных подобных объектов для целей корректировки баланса игры может быть расценено как нарушение права «виртуальной собственности» пользователя. Иными словами, создание правообладателем определенного виртуального объекта будет равнозначно признанию за ним определенного долга по отношению к пользователю – владельцу такого объекта, к чему вряд ли готово большинство правообладателей[1].

Возникает вопрос, насколько право в принципе должно вмешиваться в процессы, происходящие в виртуальном мире, и защищать пользователей от односторонних действий правообладателей и (или) других пользователей, посягающих на объекты виртуальной собственности. С одной стороны, речь идет об отношениях, возникающих в виртуальном, а не реальном мире, речь идет об игре, сама суть которой заключается в предоставлении игроку возможности действовать так, как он не стал бы действовать в реальном мире[2]. С другой стороны, речь идет об объектах, пусть и виртуальных, но обладающих реальной рыночной ценностью, а также об отношениях, которые составляют часть реальной жизни реальных людей. Представляется, что здесь необходимо некое компромиссное решение, которое позволило бы оградить игровой процесс от необоснованного вмешательства права, с одной стороны, и пресечь возможные злоупотребления, совершаемые под прикрытием такого игрового процесса, – с другой. Такое решение было предложено в концепции «волшебного круга» (*The Magic Circle Test*). Ее суть заключается в том, что виртуальные отношения подпадают под действие права в том случае, когда их участник предвидел или должен был предвидеть, что такие виртуальные отношения будут иметь определенные последствия в реальном мире[3]. Например, если речь идет о совершении кражи в игре, условия которой допускают возможность существования персонажей, которые крадут, как это имеет место во многих многопользовательских онлайновых играх[4], то факт

[1] *Duranske B.* Virtual Law. ABA Publishing. 2008. P. 96.

[2] *Duranske B.* Op. cit. P. 60.

[3] Ibid. P. 75.

[4] Например, в известной многопользовательской игре *Ultima Online* есть специальный класс персонажей – «Вор» (*Thief*), существуют гильдии воров и прочие атрибуты, свойственные данному виду деятельности.

совершения кражи в рамках игрового процесса является проявлением игры и не выходит за рамки «волшебного круга». Если же пользователь специально взламывает аккаунт и совершает кражу виртуального персонажа или иных объектов, то это уже действие, имеющее последствия в реальном мире и подпадающее под правовые нормы, в частности под ст. 272 УК РФ (неправомерный доступ к компьютерной информации). Или другой пример. Правообладатель виртуального мира, организовавший продажу виртуальных объектов за реальные деньги, не может не осознавать, что такие действия имеют определенные последствия в реальном мире: начиная от вопросов совершения платежа и заканчивая налоговыми последствиями.

Некоторые правопорядки уже приступили к активному правовому регулированию виртуальных отношений. Так, Китай уже начал предпринимать действия по разработке собственного виртуального права как составной части программы по построению конкурентоспособной индустрии продажи объектов виртуальной собственности[1]. Так, в решении *Li Hongchen v. Beijing Arctic Ice Technology Development Co*, Второй кассационный суд г. Бейджинг рассмотрел спор между пользователем онлайн-игры и правообладателем. Аккаунт истца был взломан и украден третьим лицом. Суд обязал правообладателя восстановить аккаунт, восстановив тем самым право на виртуальную собственность за ее первоначальным владельцем[2]. Это далеко не единичное решение, касающееся виртуальной собственности. Так, 17-летний подросток был осужден за кражу виртуального контента. Проводятся расследования по факту кражи виртуальной валюты. Существуют даже специальные инструкции по вопросам расследования подобного рода дел.

Тайвань идет в том же направлении. Министерство юстиции Тайваня издало постановление от 23 ноября 2011 г, в котором было указано, что объекты виртуальной собственности являются собственностью в правовом смысле, являются отчуждаемыми и передаваемыми, а кража таких объектов является наказуемой по нормам уголовного права[3]. С тех пор тайваньская юриспруденция насчитывает сотни дел, связанных с кражей и мошенничеством с виртуальной собственностью. Аналогичные тенденции имеют место и в Южной Корее, где за один

[1] *Fairfield J.* Op. cit. P. 1085.

[2] *Will Knight*, *Gamer Wins Back Virtual Booty in Court Battle,* newscientist.com. Dec. 23, 2003 // http://www.newscientist.com/article.ns?id=dn4510

[3] Taiwan Ministry of Justice Official Notation No. 039030 (90). Цит. по: *Fairfield J.* Op. cit. P. 1086.

только год было рассмотрено около 22 000 заявлений по поводу кражи объектов виртуальной собственности[1].

Однако, если абстрагироваться от практики азиатских стран, пока оборот виртуальных объектов является «относительно неурегулированным в законодательстве большинства стран»[2]. Правоприменителям обычно достаточно сложно провести параллели между реальной собственностью и математическими алгоритмами, эмулирующими внешний вид и функционал объектов реального мира[3].

В России отношения, возникающие в связи с объектами виртуальной собственности, в большинстве случаев не находят судебной защиты. Одной из причин является квалификация судами отношений, возникающих в связи с многопользовательскими онлайн-играми, в качестве игр и пари (гл. 58 ГК РФ). Согласно п. 1 ст. 1062 ГК РФ требования граждан и юридических лиц, связанных с организацией игр и пари или с участием в них, не подлежат судебной защите, за исключением требований лиц, принявших участие в играх или пари под влиянием обмана, насилия, угрозы или злонамеренного соглашения из представителя с организатором игр или пари, а также требований, указанных в п. 5 ст. 1063 ГК РФ[4]. Рассмотрим подробнее, насколько корректна такая квалификация.

ГК РФ не содержит определения понятий «игра» и «пари». В настоящее время дефиниции указанных понятий содержатся в Федеральном законе от 29 декабря 2006 г. № 244-ФЗ «О государственном регулировании деятельности по организации и проведению азартных игр и о внесении изменений в некоторые законодательные акты Российской Федерации». Под азартной игрой понимается основанное на риске соглашение о выигрыше, заключенное двумя или несколькими участниками такого соглашения между собой либо с организатором азартной игры по правилам, установленным организатором азартной игры; под пари понимается азартная игра, при которой исход осно-

---

[1] *Mark Ward*. Does Virtual Crime Need Real Justice? BBC NEWS, Sept. 29, 2003 // http://news.bbc.co.uk/2/hi/technology/3138456.stm

[2] *Steinberg A*. For Sale – One Level 5 Barbarian for 94,800 Won: The International Effects of Virtual Property and the Legality of its Ownership // The Georgia Journal of International and Comparative Law. No 37. 2009. P. 384.

[3] *Westbrook T*. Op. cit. P. 779–780.

[4] См., например: постановление президиума Московского городского суда от 24 мая 2013 г. по делу № 44г-45; определения Костромского областного суда от 12 мая 2010 г. по делу № 33-562; от 31 мая 2010 г. по делу № 33-672; решение Басманного районного суда от 17 августа 2010 г. по делу № 2-2360/10; решение Лефортовского районного суда г. Москвы от 5 октября 2010 г., решение мирового суда судебного участка № 352 Басманного района г. Москвы от 1 февраля 2011 г. № 2-01/11.

ванного на риске соглашения о выигрыше, заключаемого двумя или несколькими участниками пари между собой либо с организатором данного вида азартной игры, зависит от события, относительно которого неизвестно, наступит оно или нет.

Насколько отношения, возникающие в связи с приобретением и распоряжением виртуальными объектами за реальные деньги в многопользовательских играх, подпадают под указанные определения и признаки?

Во-первых, в данных отношениях достаточно сложно найти то самое соглашение о выигрыше, которое является краеугольным камнем во всем регулировании игр и пари. Пользователя интересует сам процесс пребывания, общения с другими игроками и прогресс его статуса в виртуальном мире. Причем достижение персонажем максимальных уровней не влечет остановки игры с последующей выплатой каких-либо призов или дивидендов. Все, что обычно получает пользователь по достижении определенного уровня, так это облегчение игрового процесса, но никак не некий выигрыш из призового фонда игры. В многопользовательских играх в отличие от карточных игр или спортивных соревнований отсутствует само понятие выигравшего. Ведь *нельзя считать игроком такого участника игры, который не может проиграть.* В отсутствие соглашения о выигрыше, заключенного с другими участниками или хотя бы правообладателем (организатором игры), нельзя говорить об игре или пари в юридическом смысле.

Конечно, можно говорить о том, что прогресс в многопользовательской игре, в том числе возможность получения обладания виртуальным объектом, зависит от случая, способностей и ловкости участника. Но данных признаков самих по себе еще недостаточно для того, чтобы говорить об игре в *юридическом* смысле. В равной степени все вышеуказанные обстоятельства определяют успех и при ведении предпринимательской деятельности.

Но самое главное заключается в том, что при таком «механическом» применении положений гл. 58 ГК РФ к отношениям, возникающим в виртуальной среде, происходит отождествление самого игрового процесса с теми правами и обязанностями, которые могут быть связаны с ним. Никто не утверждает, что право должно регулировать то, как игрок должен убивать монстров в игре, подобно тому, как право не должно регулировать то, как надо играть в шахматы. Но отношения, связанные с организацией игрового процесса, которые носят явно выраженный экономический характер, вполне могут охватываться предметом правового регулирования. Ничто ведь не препятствует

обязательствам из договора купли-продажи шахматной доски или колоды карт иметь исковую защиту, несмотря на их возможную связь с играми и пари.

Таким образом, отношения, возникающие в многопользовательских играх и прочих виртуальных мирах по поводу виртуальных объектов, имеющих реальную денежную оценку, не охватываются существующей законодательной дефиницией игр и пари. Следовательно, отсутствуют и формальные основания для применения к ним положений гл. 58 ГК РФ.

Для того чтобы в полной мере убедиться в справедливости данного вывода, целесообразно рассмотреть вопрос не только с формально-догматической, но и с политико-правовой точки зрения, а именно проанализировать мотивы, по которым законодатель ввел ограничения на признание юридической силы обязательств из игр и пари, и определить, насколько они применимы к виртуальным мирам.

Как известно, гражданское право еще со времен римского права достаточно настороженно относится к обязательствам, возникающим из игр и пари. Дигесты Юстиниана упоминают о сенатусконсультах и законах, которые запрещают играть (заключать пари) на деньги, за исключением состязаний в метании копья, беге, прыжках, борьбе, кулачном бое и других случаев состязаний «ради доблести» (D. 11.5.2.1). Не облеченный в форму стипуляции долг из игры не мог быть истребован посредством иска, однако, будучи уплаченным, не подлежал возврату. Пари на деньги по поводу игр, не связанных с «навыками тела», не дозволялись, и уплаченный по ним долг не только мог быть истребован (возвращен) посредством иска, но и при определенных обстоятельствах мог повлечь санкции со стороны государства[1]. Впоследствии подобный подход был реципирован средневековым правом и оттуда попал во многие современные европейские правопорядки[2].

Разумеется, сразу же возникает вопрос: по какой причине данного рода отношения были лишены исковой защиты? Достаточно распространена точка зрения, что такое решение принято законодателем по причине аморальности игр и пари или по крайней мере их непо-

[1] *Федотов А.Г.* Игры и пари в гражданском праве // Вестник гражданского права. 2011. № 2.

[2] См., например: § 762 Германского гражданского уложения («Обязательство из игры или пари не устанавливается. Предоставленное на основании игры или пари не может быть истребовано к возврату», ст. 1965–1967 Французского гражданского кодекса («Закон не предоставляет никакого права на иск ввиду долга, вытекающего из игорного договора, или из платежного обязательства по договору пари... То что проигравший уплатил добровольно, он не может истребовать обратно»).

лезности для общества[1]. Однако данное объяснение вряд ли может считаться удовлетворительным. Во-первых, право, как известно, – это минимум морали[2]. Наличие азарта, а равно посвящение своего времени тому, что не приводит к увеличению валового внутреннего продукта, вряд ли может быть квалифицировано как аморальное, особенно в современных условиях, когда представления о морали носят весьма плюралистический характер. Во-вторых, гражданское право допускает исковую защиту требований из игр и пари, которые организованы государством, что говорит не столько о нравоучительной ориентации права в данном вопросе, сколько а о его прагматизме: соответствующие платежи имеют немалое фискальное значение. Так что есть основания полагать, что причина может крыться в чем-то ином.

А.Г. Федотов, автор одного из наиболее интересных исследований по тематике игр и пари, высказывает мнение, что отнесение игр и пари к натуральным обязательствам (и соответственно невозможность их судебной защиты и оспаривания) является особой формой правовой защиты пари, при которой признание отношений юридически существующими неразрывно соединено с невозможностью предъявления иска, что неизбежно привело бы к признанию сделки пари недействи-

[1] Весьма ярко эта мысль была отражена в одном средневековом трактате: «Азартная игра есть игра, порожденная дьяволом из его стремления обманывать людей и тем искушать естество и губить души» (см.: Tractatus diversi super maleficiis. Lugduni: Apud haeredes Jacobi Iuntae. 1555. P. 581. Цит. по: *Федотов А.Г.* Игры и пари в гражданском праве). Представляется, что в такой интерпретации данный аргумент все же может иметь определенное значение применительно к многопользовательским компьютерным играм, которые зачастую вызывают у игроков сильные формы зависимости. Однако вряд ли отказ в исковой защите требований, связанных с оборотом виртуальных объектов, будет как-то способствовать излечению от данного недуга или предотвращать его. Напротив, существуют прецеденты, когда отказ государственных органов от вмешательства в подобные отношения приводил к весьма трагическим случаям. Так, в 2005 г. некто *Qui Chengwei*, пользователь онлайн-игры «*Legends of Mir III*», предоставил в пользование своему другу уникальный меч, который тот не возвратил, а перепродал на аукционе *eBay* за сумму порядка 820 евро. Поскольку, по мнению полиции, в данном случае не было совершено кражи аккаунта или какого-либо еще противоправного действия, она отказалась вмешиваться. Не найдя помощи со стороны правоохранительных органов, *Qui Chengwei* взял правосудие в свои руки и убил своего бывшего друга (см.: Cao Li. Death sentence for online gamer // China Daily. 06.08.2005 // http://www.chinadaily.com.cn/english/doc/2005-06/08/content_449494.htm). Конечно, данный случай является экстраординарным и столь трагичные последствия, к счастью, не являются распространенными. Но форумы различных онлайновых игр содержат немало сообщений, свидетельствующих о вынесении неразрешенных виртуальных конфликтов в реальную жизнь, что нередко оканчивалось насилием.

[2] *Брагинский М.И., Витрянский В.В.* Договорное право. Общие положения. 3-е изд., стереотип. М., 2001.

тельной либо незаключенной, поскольку она заведомо для сторон была совершена под влиянием заблуждения. Игры и пари являются сделками, при заключении которых один или некоторые из участников сделки неизбежно заблуждаются касательно некоторых (а при широком толковании предмета – существенных) условий этой сделки. Без этого пари и игра невозможны, это лежит в их природе и составляет их суть. Поэтому признавая в виде исключения некоторые основания для правовой защиты требований из игр и пари, закон тем самым позволяет обеспечить их участников хоть какой-то правовой защитой.

Нетрудно убедиться в том, что данные соображения неприменимы по отношению к сделкам, опосредующим оборот виртуальных объектов. Участники виртуальных пространств обычно отдают себе отчет в том, какие функции выполняет тот или иной объект или какими параметрами обладает тот или иной персонаж. Заблуждение как таковое может и иметь место, но будет носить факультативный характер, а не являться неизбежным атрибутом действий, совершаемых в связи с оборотом таких объектов. Не может участие в многопользовательской игре или виртуальном мире рассматриваться в качестве аморального поступка в условиях всеобщей распущенности.

При таких обстоятельствах отсутствуют веские политико-правовые основания для отказа в признании юридической силы сделок, связанных с виртуальными объектами, по крайней мере со ссылкой на положения гл. 58 ГК РФ.

В отсутствие возможности применения положений гл. 58 ГК РФ, которые можно было бы хоть как-то квалифицировать в качестве «специальных» (все же они посвящены играм, хотя и качественно иного характера), остается вопрос о том, какие правовые нормы могут быть использованы для защиты интересов субъектов таких сделок.

В американской доктрине высказываются предложения о распространении на объекты виртуальной собственности норм *common law* о праве собственности. Данный подход весьма логичен, поскольку если стоит цель защитить подобного рода объекты от неправомерных посягательств на них, для начала необходимо придать им соответствующий статус: нельзя украсть (продать) то, что не принадлежит потерпевшему (продавцу). Виртуальные объекты являются, с точки зрения сторонников данной позиции, нематериальными объектами особого рода, занимая промежуточное положение между объектами интеллектуальной собственности и классическими объектами права собственности. Последними они не являются, поскольку существуют лишь на экране компьютера, а к первым не относятся, поскольку в ряде случаев они

не являются предметом творческого труда пользователя[1]. В качестве аргументов в пользу своей позиции сторонники распространения на виртуальные объекы норм о праве собственности ссылаются на то, что такие объекты могут приобретаться и отчуждаться и обладают явно выраженной потребительской ценностью[2]. К тому же «определенные виды виртуальной собственности обладают многими характеристиками, свойственными традиционным объектам права собственности и не должны быть исключены из-под правовой охраны только потому, что первоначально выглядят незнакомыми»[3]. Тем не менее американские суды пока не решились на открытое признание прав на виртуальные объекты собственностью пользователя во многом из-за того, что индустрия многопользовательских игр не заинтересована во внесении ясности в правовой статус таких объектов, так как это может пошатнуть ее монополию на регулирование отношений, возникающих в рамках виртуальных пространств и возложить дополнительные обременения (более детально аргументы представителей индустрии были изложены чуть ранее). Конечно, ни один американский суд пока не изложил данные соображения в явной форме, но она находят свое отражение в их позиции о регулировании соответствующих вопросов в договорном порядке посредством *End User License Agreement, Terms of Use* и прочих подобных документов.

Если даже американское право, достаточно гибко подходящее к определению собственности, не готово признать виртуальные объекты в качестве объектов права собственности, то что уж можно говорить о российском праве. Как известно, объектом права собственности в системе координат российского вещного права могут быть только вещи, причем индивидуально определенные[4], поэтому виртуальные объекты не могут быть регламентированы нормами о праве собственности ввиду их явно выраженного нематериального характера[5].

---

[1] *Duranske B.* Op. cit. P. 80.

[2] *Lastowka G., Hunter D.* The Laws of the Virtual Worlds // California Law Review. No 92. 2004. P. 49.

[3] *Hunt K.* This Land is not Your Land: Second Life, Copybot and the Looming Question of Virtual Property Right // Texas Review of Entertainment and Sports Law. No 9. 2007. P. 172.

[4] См., например: *Суханов Е.А.* О понятии и видах вещных прав в российском гражданском праве // Журнал российского права. 2006. № 12.

[5] Даже если и признать, что право собственности на виртуальные объекты возможно, здесь возникает немало проблем, связанных с тем, что его реализация неразрывно связана с правом на доступ к программному продукту, в рамках которого он существует. Здесь возникает ситуация, схожая с земельным участком, к которому невозможен доступ без использования чужого земельного участка. В вещном праве данный конфликт решается посредством ограниченных вещных прав вроде сервитутов. Вопрос в том, как

Другим возможным кандидатом на регулирование отношений по поводу виртуальных объектов являются нормы договорного права. В условиях отсутствия специального регулирования и невозможности по тем или иным причинам использования традиционных положений о праве собственности можно использовать регулятивный материал, содержащийся в договоре.

Фактически сейчас это и происходит на практике, когда соответствующие отношения рассматриваются в контексте лицензионных отношений между правообладателем (администратором) и лицензиатом (пользователем). Приобретение виртуальные объектов (экипировка персонажей, виртуальная валюта или иные внутриигровые объекты) за реальные деньги можно рассматривать как своего рода лицензионный платеж, в обмен на который правообладатель «активирует» определенные компоненты программы и пользователь получает возможность использования ее дополнительных функциональных характеристик. Ведь с технической точки зрения все эти виртуальные объекты представляют собой определенный программный код, являющийся составной частью основной программы и не представляющий особой ценности в отрыве от нее. Данный подход не может не импонировать тем, кто не хотел бы уплачивать НДС с хозяйственных операций, связанных с реализацией виртуальных объектов, поскольку такая реализация подпадала бы под льготу подп. 26 п. 2 ст. 149 НК РФ. Другое дело, что в таком случае, сказав «а», надо говорить и «б», квалифицируя отношения по передаче таких внутриигровых объектов другому пользователю в качестве сублицензионного договора. А такое усложнение картины с трудом принимается даже сторонниками рассматриваемого подхода.

Однако основным недостатком данного подхода является тот факт, что условия пользовательских соглашений не могут в полной мере восполнить регуляторный вакуум по причине того, что они направлены преимущественно на регламентацию отношений между правообладателем и пользователем, а не между пользователями[1]. Да и интерпретация условий таких соглашений может быть непростым делом и иметь противоположные толкования. К тому же все равно остается вопрос: каков правовой статус такого рода объектов в случае, когда пользовательское

быть с виртуальными земельными участками, доступ к которым невозможен без согласия правообладателя программного продукта.

[1] *Duranske B.* Op. cit. P. 129. Конечно, правообладатель может отреагировать на жалобу одного пользователя по поводу нарушения условий пользовательского соглашения другим пользователем, но такая реакция является бизнес-решением правообладателя, а не вопросом обязательственного права.

соглашение никак не регламентирует его или такого соглашения просто нет, в том числе по причине признания его недействительным?

В условиях, когда существующие экономические отношения в виртуальных мирах не могут быть в полной мере урегулированы нормами пользовательских соглашений, а признание виртуальных предметов объектами права собственности с распространением на них всех соответствующих гарантий выглядит слишком революционным решением, могут пригодиться положения гражданского законодательства о неосновательном обогащении. Как известно, применение норм о неосновательном обогащении носит субсидиарный характер[1] и имеет своей целью восстановление нарушенного имущественного права, если это не может быть достигнуто путем предъявления иска из других оснований – закона, договора, деликта и пр. Как отмечает А.Л. Маковский, кондикционное обязательство является родовым по отношению ко всем способам возврата имущества[2]. Поэтому нормы о неосновательном обогащении потенциально вполне могут быть применены к отношениям, связанным с виртуальными объектами. Правда, при условии, что такие объекты или права на них будут признаны имуществом в юридическом смысле.

Несмотря на то что термин «имущество» достаточно часто употребляется в законодательстве, он не имеет четкой дефиниции. Напротив, в действующем ГК РФ, как отмечает А.Н. Лысенко, данный термин используется в различных значениях. Так, под имуществом понимаются отдельные вещи и их совокупность (п. 2 ст. 15, п. 2 ст. 46, ст. 211, п. 4 ст. 218, ст. 301, п. 2 ст. 561, п. 3 ст. 564, п. 2 ст. 690, п. 1 ст. 705, п. 2 ст. 947, ст. 1064 ГК РФ). Во-вторых, понятием «имущество» могут охватываться вещи, деньги и ценные бумаги (п. 1 ст. 302, п. 1 ст. 307 ГК РФ). В-третьих, имуществом называются не только перечисленные выше объекты, но и имущественные права (ст. 18, ст. 24, п. 1 ст. 56, п. 1 ст. 126, ст. 209, 336, п. 3–6 ст. 582 ГК РФ). В-четвертых, понятие «имущество» может обозначать всю совокупность наличных вещей, денег, ценных бумаг, имущественных прав, а также обязанностей субъекта (п. 2 ст. 63, п. 2 ст. 132, ст. 217, 1112 ГК РФ). И в-пятых, в ряде случаев в состав имущества включаются: предприятия и другие имущественные комплексы, отдельные объекты, относящиеся к недвижимому

[1] Комментарий к Гражданскому кодексу Российской Федерации, части второй / под ред. Т.Е. Абовой, А.Ю. Кабалкина. М., 2004. С. 1008.

[2] Гражданский кодекс Российской Федерации. Часть вторая. Текст, комментарии, алфавитно-предметный указатель / под ред. О.М. Козыря, А.Л. Маковского, С.А. Хохлова. М., 1996. С. 599.

имуществу, ценные бумаги, права, удостоверенные бездокументарными ценными бумагами, исключительные права и другое имущество, причем деньги (в подобном понимании) в состав имущества не входят (п. 1, 2 ст. 1013 ГК РФ)[1].

Европейский суд по правам человека демонстрирует чрезвычайно широкое понимание понятия «имущество», нередко отождествляя его со всеми закрепленными правами, которые способен доказать заявитель (в том числе денежными требованиями, основанными на договоре или деликте, социальными льготами, лицензиями и т.д.)[2]. В столь же широком смысле предлагают понимать имущество и некоторые отечественные юристы[3].

Существующий в законодательстве и доктрине плюрализм в понимании имущества наталкивает на вывод, что оно носит конъюктурный характер и его содержание может варьироваться в зависимости от конкретных потребностей и специфики отношений. Иными словами, включение какого-либо нового явления под «зонтик» понятия «имущество» не нарушит стройности гражданско-правовых конструкций и связанных с ними догматических построений, как это может иметь место при неосторожном обращении с иными гражданско-правовыми понятиями[4]. Так что категорию «имущество» можно использовать максимально гибко и включать в нее новые объекты, которые так или иначе вовлекаются в имущественный оборот. Вряд ли можно оспаривать тот факт, что объекты, обладающие качеством товара, т.е. те, которые могут приобретаться за деньги, заслуживают того, чтобы быть причисленными к объектам гражданских прав, хотя бы в качестве «иного имущества».

Отнесение виртуальных объектов к категории имущества открывает возможность для защиты прав их владельцев посредством инструментария норм о неосновательном обогащении. Так, неосновательное присвоение таких объектов другими лицами вполне может быть квалифицировано в качестве неосновательно приобретенного имущества с возникновением правового обязательства по его возврату в натуре либо при невозможности такого возврата – возмещении его стоимости (ст. 1102, 1104, 1005 ГК РФ). Таким образом, кража чужого аккаунта

---

[1] *Лысенко А.Н.* Имущество в гражданском праве России. М., 2010.

[2] См.: *Лапач Л.В.* Понятие «имущество» в российском праве и в Конвенции о защите прав человека и основных свобод // Российская юстиция. 2003. № 1.

[3] См.: Гражданское право России. Общая часть: курс лекций / отв. ред. О.Н. Садиков. М., 2001. С. 262.

[4] См., например: *Суханов Е.А.* Осторожно: гражданско-правовые конструкции // Законодательство. 2003. № 9.

с персонажем многопользовательской игры, кража виртуальной валюты или объектов виртуальной инфраструктуры (вроде земельных участков из *Second Life*) может породить возникновение юридически значимого обязательства лица, которое приобрело их, по возврату такого объекта в натуре или в стоимостном выражении. Аналогичным образом необоснованное лишение пользователя приобретенных им объектов виртуальной собственности правообладателем может быть квалифицировано в качестве неосновательного обогащения. В данном случае обогащение будет выражено в тех средствах, которые правообладатель получил за такие объекты. В случае *Braggs v. Linden Lab* правообладатель лишил пользователя не только того объекта, который был получен с нарушением установленных норм, но и всех остальных, к характеру приобретения которых у него не было претензий. Причем такие конфискованные объекты впоследствии перепродавались правообладателем другим лицам, в результате чего он получал необоснованную выгоду. Представляется, что иск из неосновательного обогащения вполне мог бы быть применен в случае рассмотрения данного спора по российскому праву, поскольку присвоение чужого имущества в данном случае привлекло к обогащению другого лица[1].

В качестве некоторого обобщения вопросов, рассмотренных в данной главе, можно указать следующее. Цифровой контент постепенно становится одним из наиболее популярных видов товара в сфере электронной коммерции. При этом под широко распространенным в настоящее время понятием «цифровой контент» скрываются различные способы коммерциализации объектов авторских и смежных прав посредством сети Интернет. Такая коммерциализация может иметь две основные формы: распространение электронных экземпляров таких объектов и предоставление к ним удаленного доступа.

В первом случае коммерциализация объектов опосредуется лицензионным договором, заключаемым в виде договора присоединения (*click-wrap-* или гораздо реже – *browse-wrap*-соглашения). Объекты интеллектуальной собственности, распространяемые в электронной форме посредством сети Интернет, обладают существенной спецификой по сравнению с аналогичными объектами, распространяемыми на материальных носителях, которая проявляется в беспрецедентных

[1] См.: п. 2 информационного письма Президиума ВАС РФ от 11 января 2000 г. № 49 «Обзор практики рассмотрения споров, связанных с применением норм о неосновательном обогащении». При этом сам по себе факт наличия договорных отношений между потерпевшим и неосновательно обогатившимся лицом не препятствует применению норм о неосновательном обогащении. См.: п. 1 Информационного письма Президиума ВАС РФ от 11 января 2000 г. № 49.

возможностях копирования и распространения цифрового контента без потери качества. Указанная специфика предопределяет нецелесообразность механического распространения традиционных механизмов, обеспечивающих баланс интересов общества и правообладателя, на случаи распространения цифрового контента, в частности положений об исчерпании права. Цифровой контент не является товаром для целей применения положений о договоре купли-продажи (гл. 30 ГК РФ), а является имущественным правом, предоставляемым в рамках лицензионного договора. Регулирование отношений посредством лицензионных договоров позволяет максимально адаптировать условия и цену цифрового продукта применительно к различным интересам пользователей, что в итоге способствует бóльшей доступности произведений для общества. В то же время во избежание возможных злоупотреблений правообладателей при формулировании условий таких соглашений целесообразно введение дополнительных мер, обеспечивающих возможность непосредственного восприятия в доступной форме их наиболее существенных условий в момент совершения юридически значимых действий пользователем (оформление заказа, его оплата, загрузка контента), а также осуществления последующего судебного контроля над справедливостью лицензионных условий.

При коммерциализации цифрового контента посредством предоставления удаленного доступа к нему пользователь не получает экземпляра произведения. Поскольку контроль над экземпляром произведения сохраняется за правообладателем (провайдером), большинство положений законодательства об авторском праве и лицензионных договорах неприменимы, что обусловливает целесообразность квалификации возникающих отношений в качестве договора возмездного оказания услуг или непоименованного договора при безвозмездном характере предоставляемого сервиса.

Новые виды социального взаимодействия, доступные посредством сети Интернет, породили ряд виртуальных миров, обладающих развитой экономической подсистемой. Виртуальные объекты, существующие в рамках данных миров, нередко обладают немалой экономической ценностью и могут приобретаться за реальные деньги, что обусловливает целесообразность их охраны с помощью права. В то время как некоторые азиатские правопорядки распространяют на такие объекты положения о праве собственности, представляется, что применительно к России на данном этапе целесообразно использовать для защиты таких объектов инструментарий гл. 60 «Неосновательное обогащение» ГК РФ, рассматривая их в качестве «иного

имущества» в контексте ст. 128 ГК РФ. Тем не менее следует признать, что в силу существующей тенденции к дематериализации и виртуализации имущества отношения, возникающие в виртуальных мирах, все хуже и хуже поддаются интерпретации на языке, унаследованном от римского права. Со временем неизбежно возникнет необходимость переосмысления традиционных представлений о праве собственности, его объектах и порядке их защиты с целью причисления к ним виртуальных объектов. Как справедливо указывает М.А. Федотов, «... он [законодатель] должен корректно включить киберпространство в сферу текущего правового регулирования, не противопоставляя реальный и виртуальный миры, а понимая, что эти миры существуют совместно, и то, что происходит в одном, может иметь серьезные последствия в другом»[1]. В любом случае существующий *status quo* в отношении виртуальных объектов не продлится долго. Ситуация, когда существует черный рынок таких объектов, а их регулирование осуществляется соглашениями, составленными в одностороннем порядке правообладателями без учета интересов пользователей и третьих лиц, является ненормальной. Эксперты сходятся во мнении, что рано или поздно суды, а вслед за ними и законодатели будут вынуждены признать реальность виртуальной собственности[2].

[1] *Федотов М.А.* Проблемы доктрины информационного права // Труды по интеллектуальной собственности. М., 2012. Т. 10. С. 42.

[2] См.: *Duranske B.* Op. cit. P. 114.

Глава 7. Электронные платежи в сфере электронной коммерции

§ 1. Виды электронных средств платежа

Развитие компьютерных технологий и сети Интернет не могло не повлечь появление новых платежных инструментов, среди которых следует особо выделить инструменты электронного доступа к банковским счетам (*access products*) и электронные деньги. Их появление является одной из наиболее значимых инноваций в сфере денежного обращения и отражает устойчивую тенденцию к дематериализации денег, т.е. процессу, при котором деньги получают существование лишь в виде записей по счетам в отсутствие физической формы воплощения владения ими. По меткому выражению известного банкира Уолтера Ристона, «информация о деньгах приобрела такое же значение, как и сами деньги».

Различия между инструментами электронного доступа к банковским счетам (*access products*) и электронными деньгами основываются на двух ключевых характеристиках: 1) местонахождении денежной стоимости и 2) используемом механизме для перевода такой стоимости[1].

Инструменты электронного доступа позволяют осуществлять в удаленном режиме распоряжение средствами, размещенными в традиционных кредитных учреждениях (дебетовые и кредитные карты, инструменты мобильного банкинга, электронные чеки). Механизм совершения платежа носит трехсторонний характер: помимо плательщика и получателя в нем участвует платежный посредник (кредитное учреждение). Таким образом, инструменты электронного доступа хотя

[1] Иногда в качестве отдельной категории упоминается так называемый мобильный банкинг, в котором основную роль в проведении платежа играет мобильный телефон. Однако различные его формы можно так или иначе отнести к двум описанным выше. В случае когда мобильный телефон используется в качестве средства доступа и управления банковским счетом – это не что иное, как *access product*, в том случае, когда в качестве средства платежа используется остаток на лицевом счете абонента сети сотовой связи, данная форма платежного инструмента может охватываться понятием электронных денег.

и носят электронный характер, но суть денег, распоряжение которыми осуществляется, они не меняют – это все те же безналичные денежные средства, только со значительно облегченным порядком доступа к ним.

Понимание термина «электронные деньги» претерпевало изменения с момента его появления. Поначалу он использовался для обозначения систем электронных переводов, систем платежей с использованием банковских карт. Впоследствии, со второй половины 90-х гг. прошлого века, термин «электронные деньги» стал обозначать новые электронные средства платежа, при которых используется эмиссия электронного скрипа (*e-scrip*)[1], представляющего собой денежное требование к эмитенту, которое выражено в электронной форме и передается при платеже от плательщика к получателю[2]. В качестве эмитента электронных денег могут выступать как кредитные учреждения, так и иные учреждения. При этом денежная стоимость хранится не на банковском счете, а на информационном носителе и не требует обязательного участия эмитента для ее перевода получателю.

Следует особо подчеркнуть, что ни один из существующих платежных механизмов не является идеальным и подходящим для всех типов платежей[3]. Например, многие из них не очень подходят для так называемых микроплатежей или для осуществления расчетов между физическими лицами в сети Интернет. Все это обусловливает сосуществование и конвергенцию различных платежных инструментов.

§ 2. Инструменты электронного доступа к банковским счетам

В настоящее время пластиковые карты (дебетовые и кредитовые) получили наибольшее распространение в интернет-коммерции[4].

Под пластиковой картой понимается персонифицированный платежный инструмент, используемый для автоматизации безналичных расчетов, а также для обналичивания имеющихся на банковском счете средств. При выдаче карты клиенту осуществляется ее персонализация – на нее заносятся данные, позволяющие идентифицировать карту и ее держателя, а также осуществлять проверку платежеспособности карты при приеме ее к оплате или выдаче наличных денег (процесс

[1] Под электронным скрипом понимается специальный информационный файл, содержащий уникальный идентификационный номер и указывающий на объем денежной стоимости, принадлежащий его владельцу. Именно он и выступает в качестве средства платежа при осуществлении расчетов посредством использования электронных денег.

[2] *Кочергин Д.А.* Электронные деньги: учебник. М., 2011. С. 20.

[3] *Graham Smith*. Op. cit. P. 874.

[4] *Юрасов А.В.* Указ. соч. С. 218.

аутентификации). Технология аутентификации зависит от схемы функционирования платежной системы и типа карты. Обычно аутентификация в торговой точке при физическом присутствии ее владельца осуществляется посредством введения секретного ПИН-кода или, что встречается все реже и реже, – посредством сличения фактической подписи на слипе с подписью на карте, иногда с предъявлением документа, удостоверяющего личность.

Отличительной особенностью использования пластиковых карт в сети интернет является тот факт, что традиционные способы аутентификации, описанные выше, не работают, что обусловливает необходимость особого подхода к данному процессу, в том числе с точки зрения обеспечения сохранности сведений о платежной карте и транзакции.

В качестве средства аутентификации при совершении покупки через интернет-магазин выступают данные карты: номер, срок действия, имя владельца карты и особый код на обороте карты: *CVV2* (*card verification value*) – для *Visa*, *CVC2* (*card verification code*) – для *MasterCard*. Данный код расположен на обороте карты и представляет собой трехзначное число, получаемое с помощью специального алгоритма с использованием номера карты и срока его действия. Данный алгоритм использует пару секретных ключей, известных эмитенту карты, поэтому, даже зная номер карты и срок ее действия, вычислить секретный код без знания данного ключа невозможно. В последнее время все большее распространение получает технология *MasterCard SecureCode* и *Verified by Visa*. Суть ее сводится к привлечению для целей аутентификации плательщика дополнительных средств из «реальной жизни», таких как мобильный телефон. Каждый раз когда клиент совершает покупки в интернет-магазинах, происходит запрос на ввод пароля. Пароль является одноразовым (действующий только для одной покупки) и сообщается посредством *sms*-сообщения, отправленного на номер мобильного телефона, либо получается клиентом в банкоматах (терминалах) его банка-эмитента. После успешного ввода пароля платеж будет одобрен. Подобно ПИН-коду банковской карты, такой пароль является «иным аналогом собственноручной подписи», о котором говорится в п. 3 ст. 847 ГК РФ: «...договором может быть предусмотрено удостоверение прав распоряжения денежными суммами, находящимися на счете, электронными средствами платежа и другими документами с использованием в них аналогов собственноручной подписи (пункт 2 статьи 160), кодов, паролей и иных средств, подтверждающих, что распоряжение дано уполномоченным на это лицом».

В самом общем виде последовательность совершения действий оплаты в интернет-магазине посредством банковской карты выглядит следующим образом:

Участники процесса:

– интернет-магазин;

– покупатель (держатель банковской карты);

– банк-эмитент (банк, выпустивший карту покупателя);

– банк-эквайер (банк, принимающий оплату от лица продавца);

– платежная система (например, *MasterCard*, *Visa*).

Процедура прохождения платежа (рисунок).

1. Покупатель формирует заказ и выбирает в качестве способа оплаты банковскую карту.

2. Интернет-магазин отправляет запрос банку-эквайеру.

3. Банк-эквайер пересылает запрос на авторизацию операции в платежную систему.

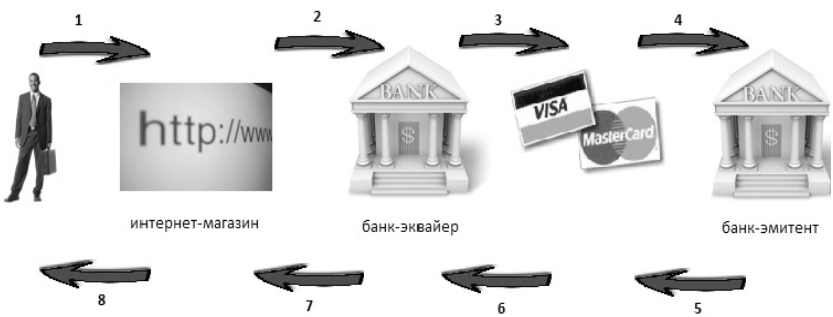
4. Платежная система передает запрос банку-эмитенту.

5. Банк-эмитент проверяет наличие средств на карте и возвращает платежной системе положительный ответ на запрос.

6. Платежная система транслирует ответ банку-эквайеру.

7. Банк-эквайер сообщает результат интернет-магазину и производит с ним расчеты.

8. Интернет-магазин доставляет товар (оказывает услугу).



Одним из основных недостатков использования платежных карт являются риски, связанные с мошенничеством. Данные платежные карты могут быть перехвачены хакерами в процессе пересылки, поскольку пакеты данных, пересылаемые в сети Интернет, распространяются в незашифрованном виде. Для минимизации данной угрозы был разработан специальный протокол *SSL*, который шифрует данные о платежах

перед их отправкой. Правда, этот механизм не может в полной мере устранить указанные риски. Широкое распространение получили так называемые фишинговые сайты (*phishing sites*), которые представляют собой зеркальные копии сайтов известных интернет-магазинов и осуществляют сбор данных о пользователях. К тому же нередки ситуации, когда хакерам удавалось взломать сервер интернет-магазинов и получить доступ к платежным данным покупателей[1].

В качестве альтернативы пластиковым картам все большее распространение получают технологии удаленного управления счетом (например, системы «Банк – Клиент»). Они предполагают использование для доступа к счету специальной программы-клиента, установленной на компьютере или смартфоне пользователя, а также применение технологий защиты данных в процессе передачи и идентификации пользователя с использованием средств электронной подписи. Следует отметить, что, несмотря на связь данных технологий с «деньгами» и применение электронных средств связи, они не являются электронными деньгами в том понимании, которое в настоящее время является превалирующим. Технологии удаленного управления счетом являются техническим продолжением традиционных правоотношений, возникающих в связи с заключением договора банковского счета. Основным вопросом, который может возникнуть в связи с правовой оценкой возникающих отношений, является авторизация пользователя и связанное с ней правовое регулирование электронной подписи.

§ 3. Электронные деньги. Общие положения

В зависимости от того, какое техническое устройство используется для хранения денежной стоимости, может выделить следующие виды систем электронных денег: системы на базе микропроцессорных карт (*Card-Based Systems*); системы на базе программно-сетевых продуктов (*Software/Network-Based Systems*) и системы, использующие удаленный доступ к серверам (*Server-Based Systems*).

В системах, построенных на базе микропроцессорных карт в качестве устройства хранения электронных денег выступает микрочип, который встроен в микрокарту и на котором хранится информация о денежной стоимости, обновляющаяся в результате совершения операций с картой. В качестве примера системы электронных денег, построенной на базе микропроцессорных карт, можно привести *GeldKarte* (Германия), *Quick* (Австрия), *Moneo* (Франция), *Edy* (Япония) и ряд

[1] *Graham Smith*. Op. cit. P. 884.

других. В России в настоящее время нет успешно функционирующих систем электронных денег на основе многоцелевых предоплаченных карт, что, по мнению Д.А. Кочергина, свидетельствует о низкой заинтересованности кредитных и других финансовых институтов в предложении электронных денег, а также о низком потребительском спросе на данный тип финансовых продуктов[1].

Следует отметить, что в качестве электронных денег не могут рассматриваться различного рода предоплаченные карты, эмитированные предприятием, предназначенные для оплаты товаров или услуг, произведенных *данным* предприятием (телефонные карты, карты оплаты проезда и пр.). Такие карты не имеют нейтральной покупательной способности, выраженной в определенной валюте, их покупательная способность выражается в единицах потребления *конкретного* блага. В связи с этим электронные «деньги», выпущенные предприятием, являются признанием существования долга в рамках заключенного договора на передачу товара или оказание услуги. Полученные в момент реализации карты средства являются собственностью предприятия, которыми он может распоряжаться по собственному усмотрению, а держатель карты путем приобретения карты исполняет свою обязанность по оплате товара (услуги), а не размещает временно свободные средства для их сохранения и получения процента.

Системы электронных денег, построенные на базе программно-сетевых продуктов, используют в качестве устройства хранения электронных денег не микрочип, а специальную компьютерную программу, размещенную на жестком диске компьютера или ином носителе. В России наиболее известными представителями данного вида системы являются *WebMoney* и до недавнего времени «Яндекс.Деньги»[2], которые ориентированы на осуществление платежей в сети Интернет.

В системах электронных денег, построенных на базе удаленного доступа к серверам, денежная стоимость хранится на удаленном сервере, к которому осуществляется подключение при совершении платежа. Наиболее известными примерами данной системы являются *PayPal*, *Moneybookers*. В данном случае денежная стоимость приобретается посредством оплаты традиционной пластиковой картой и зачисляется на счет пользователя в системе *PayPal*. Впоследствии данная стоимость

[1] *Кочергин Д.А.* Указ. соч. С. 61.

[2] С 2011 г. система «Яндекс.Деньги» прекратила поддержку пользования системой посредством программы Интернет.Кошелек, устанавливаемой на компьютер пользователя. В настоящее время использование кошелька возможно посредством веб-браузера. Таким образом, в настоящее время «Яндекс.Деньги» относится скорее к третьей группе – системе электронных денег, построенных на базе удаленного доступа к серверу эмитента.

может использоваться для осуществления покупок в интернет-магазинах, принимающих платежи через *PayPal*, либо для перечисления на счет другого пользователя *PayPal*, что является особенно актуально для *C2C*-сегмента электронной коммерции (вроде *eBay*)[1].

Преимущества электронных денег

Электронные деньги имеют ряд преимуществ по сравнению с платежами посредством банковских карт.

Во-первых, лежащая в основе электронных денег технология позволяет обеспечить *анонимность* совершаемых транзакций. Анонимность в современных условиях тотальной информатизации является весьма ценным ресурсом. Дело в том, что невозможность оплатить что-либо анонимно означает и невозможность купить что-либо анонимно. Вследствие автоматизации технологий продаж, а также развития инструментария *Big Data* аналитики-продавцы могут составить полную картину совершенных продаж, в том числе по покупателям. Данная информация представляет собой большую ценность, о чем свидетельствует широкое распространение различных программ лояльности (скидочных карт), которые предоставляются, по существу, в обмен на персональные данные покупателя и возможность отслеживания информации о сделанных им покупках. По мере объединения баз данных, составленных различными продавцами, появляется возможность составления всеобъемлющего портфолио на каждого покупателя, из которого можно сделать выводы не только о его предпочтениях, но и о состоянии здоровья, политических и религиозных взглядах и прочих персональных характеристиках. Полученные данные могут быть использованы страховыми компаниями (для оценки страховых рисков) и кредитными компаниями (для принятия решений о выдаче кредита и его условиях), потенциальными работодателями и много кем еще. Использование безналичных средств платежа с привлечением банков в силу существа процесса платежа не может оставаться без следов. В связи с этим электронные деньги, по крайней мере некоторые их виды, имеют значительный потенциал анонимности и ближе к наличным деньгам, использование которых также не влечет следов в виде записей по счету[2].

---

[1] В 2002 г. платежная система *PayPal* была приобретена интернет-аукционом *eBay*.

[2] *Graham Smith*. Op. cit. P. 908. Несмотря на то что данные вопросы более относятся к сфере законодательства о персональных данных, не вызывает сомнений тот факт, что на практике многие его положения не выполняются интернет-магазинами и иными участниками оборота и привлечение их к ответственности является весьма проблематич-

Использование технологии слепой подписи, предложенной Д. Чаумом, позволяет выпускать электронные деньги, дальнейшее использование которых эмитент не может проследить. Под слепой подписью понимается технология, позволяющая идентифицировать полученную информацию, т.е. убедиться в том, что она пришла от авторизованного лица, и удостоверить ее, не зная ее содержания. Применение технологии слепой подписи позволяет сделать платежи электронными деньгами полностью анонимными[1]. В настоящее время технология «слепой подписи» используется, в частности, в платежной системе «Яндекс.Деньги»[2].

Вместе с тем возможность совершения анонимных платежей может быть использована с целью отмывания денежных средств, полученных преступным путем, с целью уклонения от уплаты налогов или приобретения объектов, ограниченных в обороте или исключенных из оборота. Как следствие, законодатели пытаются минимизировать данные риски, устанавливая максимальные размеры денежной стоимости, которая может принимать форму электронных денег, а также накладывая ограничения по сфере их использования[3].

Во-вторых, использование электронных денег позволяет существенно снизить транзакционные издержки, связанные с совершением платежа, открыв тем самым широкие возможности для осуществления *микроплатежей*, под которыми понимаются незначительные платежи, осуществление которых традиционными платежными средствами невыгодно с точки зрения соотношения «размер платежа – стоимость его обработки»[4]. Реализация микроплатежей посредством платежных

ным. Так что любые иные механизмы, позволяющие минимизировать распространение персональных данных в сети Интернет, являются весьма востребованными.

[1] В качестве аналогии можно привести процесс выдачи ПИН-кода пользователю банковской карты. После его генерации компьютером он распечатывается на специальном принтере на бланке, помещенном в запечатанный конверт вместе с копировальной бумагой. Принтер формирует оттиск ПИН-кода непосредственно в запечатанном конверте, обеспечивая тем самым его конфиденциальность и неизвестность сотрудникам банка.

[2] См.: *Мартынов В.Г., Андреев А.Ф., Кузнецов В.А., Шамраев А.В и др.* Электронные деньги. Интернет-платежи. М., 2010. С. 58–59.

[3] См. подробнее далее.

[4] Себестоимость розничного платежа для кредитного учреждения составляет в среднем около 1 долл. См.: Технологии *CyberPlat*® («КиберПлаТ»): Основа глобальной инфраструктуры новой экономики. 2003. С. 10. К тому же не следует забывать, что существующие риски, связанные с использованием банковских карт (риск непогашения кредитной задолженности клиентом, оспаривания совершенного платежа клиентом с последующим его возвратом на карту (*chargeback*) и пр.), закладываются в стоимость договора между банком и интернет-магазином.

карт неэффективна, так как транзакционные издержки на обслуживание такого платежа сопоставимы или даже превышают его размер, что делает произведенные микроплатежи убыточными для получателя.

Как отмечается, потенциально высокий спрос на микроплатежи в интернет-коммерции способен оказать значительное влияние на развитие электронных денег[1]. Особенно ценной возможность осуществления микроплатежей является при распространении цифрового контента: нередко пользователь не заинтересован в приобретении полноценной подписки на соответствующий ресурс, а желает получить конкретный материал или выдержку из него (например, конкретную страницу или статью). Обеспечивая такую возможность, владелец ресурса может существенно увеличить клиентскую базу. Микроплатежи могут иметь немалое значение и в области интернет-маркетинга. Некоторые предприятия, занимающиеся интернет-рекламой, готовы платить по несколько центов пользователям за каждое письмо, которое при иных условиях будет воспринято пользователем как спам и с ожесточением удалено.

В-третьих, электронные деньги являются привлекательным инструментом для осуществления расчетов между физическими лицами, что особенно важно для различного рода интернет-аукционов и электронных площадок для *C2C*-коммерции. Далеко не каждое физическое лицо готово связываться с громоздкими процедурами организации и осуществления банковских платежей, особенно при незначительной сумме договора. Платеж электронными деньгами является гораздо более удобным вариантом.

Механизм расчетов посредством электронных денег

Для понимания процессов, возникающих при расчетах электронными деньгами, необходимо разграничить два основных типа электронных денег: электронные деньги, выпущенные в рамках закрыто циркулирующих систем, и электронные деньги, выпущенные в рамках открыто циркулирующих систем[2].

Под закрыто циркулирующей системой (*closed circulation system*) понимается система, в которой не допускаются многократные переводы (или обращение) одной и той же денежной стоимости между участниками системы. Для осуществления окончательного расчета получатель электронных денег должен возвратить их для проверки

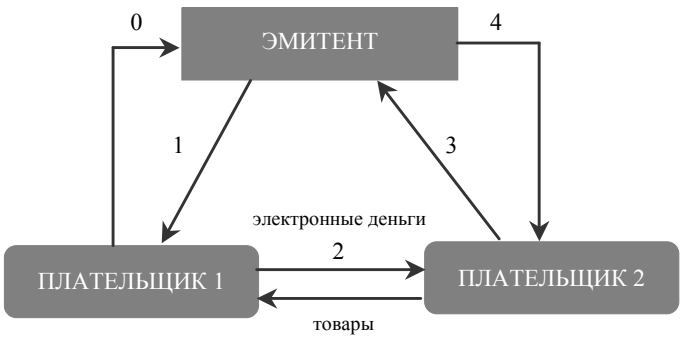
[1] *Юрасов А.В.* Указ. соч. С. 266.

[2] Указанная классификация впервые была предложена в работе: *Pauli R., Koponen R.* Toward Electronic Money // Bank of Finland Bulletin. 1997. Vol. 71. No 4. P. 9–12.

и уничтожения. Примером таких систем являются построенные на базе программно-сетевых продуктов системы *eCash*, *Magex*, *PayCash*, а также бóльшая часть электронных денег, функционирующих с использованием электронных кошельков.

Открыто циркулирующая система (*open circulation system*) представляет собой систему, в которой предусматривается возможность многократного обращения одной и той же денежной стоимости между хозяйствующими субъектами. В качестве примера можно привести международную систему *Mondex*, сингапурскую систему *CashCard*, виртуальную валюту *Bitcoin* и др.

Одна из главных особенностей большинства видов систем электронных денег[1], вытекающих из необходимости обеспечения безопасности и целостности платежей, состоит во вмешательстве эмитента в каждую транзакцию. Это вызвано тем фактом, что свободное движение электронных денег не гарантирует в достаточной мере защиту от их двойного расходования. Дело в том, что, поскольку электронные деньги представляют собой файл, он без особых проблем может быть скопирован: в отсутствие специальных механизмов, предотвращающих возможность повторного использования электронных денег, их обладатель может неограниченно богатеть при помощи их копирования с последующей рассылкой в различные платежные точки. Для предотвращения такой ситуации совершаемый платеж проходит несколько потоков (рисунок):



1) появление электронных денег предваряет их предоплата традиционными деньгами, которая является основанием для их эмиссии (поток 0);

[1] Кроме децентрализованных электронных валют вроде *Bitcoin*, особенности которой будут рассмотрены далее.

2) электронные деньги выпускаются эмитентом в пользу плательщика 1 исключительно для совершения конкретного платежа плательщику 2 (поток 1);

3) плательщик 1 совершает платеж плательщику 2 (поток 2);

4) после получения электронных денег плательщик 2 должен их вернуть эмитенту (поток 3) и получить окончательный расчет (поток 4).

Выделяется пять основных характеристик электронных денег, выпущенных в закрыто циркулирующей системе:

1) единственной целью выпуска электронных денег является осуществление платежа;

2) каждый платеж предполагает возникновение отношений между тремя лицами: плательщиком, получателем и эмитентом;

3) для окончательного проведения платежа получатель электронных денег должен вернуть их эмитенту для уничтожения, что означает ограниченный период существования электронных денег. Каждая купюра живет только один цикл оплаты. После предъявления ее эмитенту она заносится им в базу данных использованных купюр и тем самым предотвращается возможность ее последующего обращения. При попытке плательщика заплатить той же купюрой еще раз получатель информируется о недействительности платежа;

4) электронные деньги не могут свободно обращаться между хозяйствующими субъектами;

5) каждый эмитент выпускает свою «версию» электронных денег, т.е. они не являются однородными[1].

Приведенный механизм совершения платежей электронными деньгами в закрыто циркулирующей системе демонстрирует, что деньги не покидают такую систему, а являются «депонированными» у эмитента. В связи с этим возникающие отношения иногда трактуются как особая форма депозита. Как отметила Рабочая группа по платежным системам, «с экономической точки зрения очевидно, что деньги, полученные эмитентом, являются банковским депозитом. В действительности это требование, которое держатель электронных денег имеет на третье лицо (эмитента)»[2]. В качестве возможного стимула для эмитентов (банков) предлагать цифровую валюту выступает отсутствие необходимости уплаты процента, который традиционно платится по остаткам средств на банковских счетах: банк в таких случаях

[1] *Кочергин Д.А.* Указ. соч. С. 99.

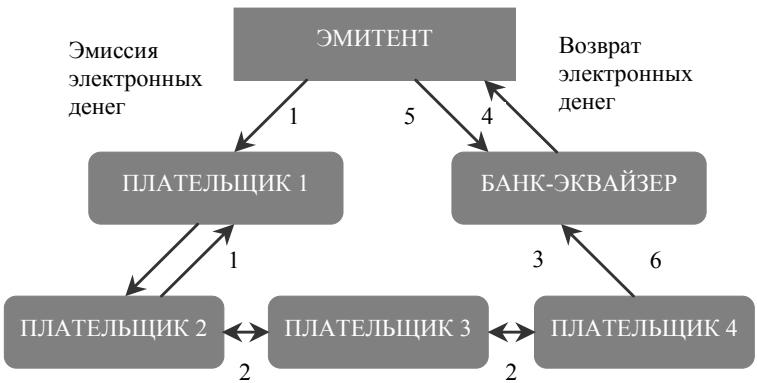
[2] Working Group on EU Payment Systems. Report to the Council of the European Monetary Institute on Prepaid Cards. Brussels: European Monetary Institute. May 1994.

получает беспроцентную ссуду от клиентов, хранящих свои денежные остатки в цифровой валюте.

Однако данная точка зрения не разделяется рядом экономистов и законодателей. Не оспаривая факт наличия определенного момента времени между приобретением электронных денег (поток 0) и получением окончательного расчета (поток 4), данный момент в закрыто функционирующих системах весьма непродолжителен по времени. При таких обстоятельствах средства, предоставленные эмитенту, не могут выполнять функцию средства сбережения. Этот довод нашел свое отражение в Директиве ЕС № 2009/110/ЕС об электронных деньгах: «выпуск электронных денег не относится к депозитной деятельности... в силу специфического характера электронных денег как электронного суррогата банкнот и монет, которые используются для совершения платежей, как правило, на лимитированные суммы и не являются средством сбережения». В соответствии с п. 6 ст. 7 Федерального закона от 27 июня 2011 г. № 161-ФЗ «О национальной платежной системе» (далее – Закон о НПС) оператор электронных денежных средств не вправе осуществлять начисление процентов на их остаток или выплату любого вознаграждения клиенту.

Таким образом, электронные деньги с точки зрения европейского и российского законодательства не являются средством сбережения, а являются предоплаченным финансовым продуктом, предназначенным для совершения платежей на небольшие суммы.

Схема платежей в открыто циркулирующей системе электронных денег представлена на рисунке.



Как видно из указанной схемы, электронные деньги выпускаются эмитентом в адрес плательщика 1, после чего имеет место ряд пос-

ледовательных платежей (потоки 2) между плательщиками 1, 2, 3, 4 (на самом деле их может быть сколько угодно), последний из которых помещает электронные деньги в банк – агент эмитента (поток 3), который отправляет их эмитенту для проверки и уничтожения (технический клиринг – поток 4, 5). Завершается цепочка кредитованием счета плательщика 4 (поток 6).

Д.А. Кочергин выделяет следующие основные характеристики электронных денег в открыто циркулирующих системах: 1) выпускаются для осуществления последовательных платежей между хозяйствующими субъектами; 2) не требуют обязательного участия третьей стороны – эмитента в процессе совершения платежа; 3) существуют в пределах всей последовательности платежей, пока не возвращены эмитенту; 4) могут свободно обращаться между хозяйствующими субъектами; 5) не являются однородными.

Несмотря на то что большинство свойств электронных денег в открыто циркулирующих системах совпадает с характеристиками наличных денег, пятое свойство указывает на существующее различие между наличными и электронными деньгами. Однородность последних будет достигаться лишь в том случае, если они будут выпускаться единственным эмитентом, например центральным банком.

§ 4. Правовое регулирование электронных денег в США и Европейском союзе

Правовое регулирование электронных денег в США

Президент США Билл Клинтон и вице-президент США Альберт Гор 1 июля 1997 г. изложили свое видение развития электронной коммерции в документе под названием «*Framework for Global Electronic Commerce*». Основная идея данного документа заключалась в политике наименьшего вмешательства государства в процессы, связанные с развитием электронной коммерции, и предоставляла рынку возможность расставить все на свои места. Электронные платежные средства были обозначены в данном документе в качестве ключевого компонента складывающегося электронного рынка. При этом отмечалось, что развитие электронных платежных средств носит настолько динамичный характер, что весьма сложно обеспечить своевременную разработку адекватной политики в отношении них. В связи с этим предлагалось осуществлять вмешательство в процесс развития электронных платежей в индивидуальном порядке («*on a case by case basis*»).

Последующая политика регуляторов США по отношению к электронным деньгам во многом соответствовала данным подходам. Так, Совет управляющих Федеральной резервной системы (ФРС) пришел к выводу о нецелесообразности распространения на эмитентов электронных денег «правила Е» (*Regulation «E»*), устанавливающего порядок осуществления электронных переводов[1]. Данное правило предписывает, в частности, необходимость выдачи чека по факту проведения каждой транзакции, а также возложение на организацию, осуществляющую такие расчеты, рисков, связанных с совершением транзакции неавторизованным лицом.

Как отмечал бывший на тот момент председателем ФРС Алан Гринспан, «в нынешний момент рыночных перемен и неопределенности может возникнуть естественное искушение для нас и естественное желание для участников оборота воззвать к правительству с требованием вмешаться и устранить существующую неопределенность путем введения законодательных норм или стандартов, либо путем проведения иных видов государственной политики. Применительно к электронным деньгам уроки прошлого учат нас тому, что потребители и предприниматели в конечном счете сами определят, какие продукты являются успешными на рынке. Государственное вмешательство в данном случае может затормозить прогресс и уж абсолютно точно не может его обеспечить»[2].

Отсутствие текущей опасности со стороны систем электронных денег для национального денежного обращения, а также традиционно либеральная политика в отношении регулирования финансовых услуг являются основными причинами, по которым федеральные регуляторы США не осуществляли долгое время жесткого *централизованного* регулирования эмитентов электронных денег, что, однако, не означало отсутствия какого-либо регулирования вообще.

Уже в 2006 г. более чем в 45 штатах выпуск электронных денег на базе физических носителей являлся объектом регулирования (в части резервных требований к размеру капитала, требований по лицензированию указанного вида деятельности и ряда других). Законодательство о защите прав потребителей в ряде штатов (например, штатов Калифорния, Коннектикут, Массачусетс) также оказывало и продол-

[1] Report to the Congress on the Application of the Electronic Fund Transfer Act to Electronic Stored-Value Products (1997).

[2] Remarks by Chairman Alan Greenspan at the Conference on Privacy in the Information Age, Salt Lake City, Utah March 7, 1997. Цит. по: *Grigg I.* Critique on the 1994 EU Report on Prepaid Cards // http://www.iang.org/papers/1994_critique.html

жает оказывать непосредственное влияние на эмитентов электронных денег, регламентируя договорно-правовой аспект пользования их услугами и т.д.[1]

В целях унификации публично-правовых аспектов оказания финансовых услуг небанковскими организациями был разработан Модельный закон о денежных услугах США, рекомендованный для имплементации в отдельных штатах. Он имеет целью создание «единообразного подхода к регламентации финансовых инструментов с хранимой стоимостью (*stored value*) и электронной валюты»[2]. Его основные положения сводятся к определению оснований и порядка лицензирования небанковских организаций, предоставляющих финансовые услуги *(Money services businesses*), а также порядка размещения средств, полученных от потребителей за реализованные платежные инструменты. Данный Закон не регламентирует частноправовых аспектов взаимоотношений между такими организациями и их клиентами.

В целом Модельный закон не содержит революционных положений с точки зрения существовавшего на момент его разработки регулирования, а является скорее обобщением принятых в различных штатах подходов. В связи с этим применительно к электронным платежам в сети Интернет было принято решение не создавать специальное регулирование, а распространить уже имеющиеся с некоторыми корректировками. Такие платежи рассматривались в качестве функционального аналога обычных денежных переводов[3]. Согласно данному Закону эмиссия электронных денег подпадает под понятие «денежный перевод» (*money transmission*).

При этом электронные деньги сами по себе не получили признания в качестве денег в строгом смысле этого слова, под которыми в соответствии с определением, данным еще в ЕТК,[4] понимается лишь «средство платежа, допущенное или принятое отечественным или иностранным правительством и включающее денежную единицу расчета, установленную межправительственной организацией или путем соглашения между двумя и более странами»[5].

Таким образом, в США отсутствует единая правовая база по вопросам регулирования отношений, возникающих в связи с электронными деньгами. Данные вопросы в большинстве своем регламентируются

---

[1] *Кочергин Д.А.* Указ. соч. С. 310.
[2] Uniform Money Services Act. With Prefatory Note and Comments. 2000.
[3] Uniform Money Services Act. With Prefatory Note and Comments. 2000. P. IX.
[4] Аналогичное определение содержится в ст. 1-201 (24) ЕТК США.
[5] Section 102 (12) Uniform Money Services Act.

в законодательстве отдельных штатов. Наличие специального закона, посвященного электронным деньгам или платежам в сети Интернет, в целом нетипично для отдельных штатов. Инновационные виды платежей обычно рассматриваются ими под «зонтиком» уже сложившихся норм, сформированных применительно к традиционным видам денежных переводов, с некоторой адаптацией их к специфике новых видов платежей. Отношения, возникающие в связи с эмиссией электронных денег, при этом воспринимаются скорее как разновидность услуг, чем как разновидность банковской деятельности.

Либеральный подход США к регулированию электронных денег, о котором так часто говорится в литературе, претерпел существенные изменения с принятием после терактов 11 сентября 2001 г. *Patriot Act* 2001 г. Данный Закон содержит в том числе и нормы, направленные на противодействие финансированию терроризма и возлагает на финансовые учреждения ряд обязанностей, в числе которых реализация политики «знай своего клиента» (*know your customer*). Как отмечается, с момента принятия данного Закона осуществление в США деятельности в сфере переводов электронных денег превратилось в кошмар[1].

Для иллюстрации данного тезиса можно привести следующий пример. Существует множество различных определений, которые могут быть применимы к «организации, осуществляющей переводы денежных средств» (*money transmitter*). В соответствии с § 1960 (*b*) (2)[2] понятие перевода денег (*money transmitting*) включает в себя «перевод средств (*transfer of funds*), осуществляемый в отношении каждого, кто обратился (*on behalf of the public*), любым способом, включая, но не ограничиваясь переводами как внутри страны, так и международными, осуществляемыми средствами проводной связи, чеками, траттами, средствами факсимильной связи или курьером». Организация, чья деятельность подпадает под данную дефиницию, подпадает под действие положений § 5330[3], который в свою очередь содержит уже иное понятие *money transmitter'a*: «бизнес, осуществляющий обналичивание чеков, обмен валюты, денежный перевод, выпуск или оплату почтовых ордеров на денежный перевод, дорожных чеков или иных подобных инструментов, а также любое иное лицо, которое осуществляет деятельность, связанную с переводом средств, в том числе любое лицо, которое осуществляет деятельность в неформальной системе перевода

[1] *Генкин А., Суворова Е.* Электронные платежи: будущее наступает сегодня. М., 2011. С. 194.

[2] 18 U.S.C. § 1960 (b) (2).

[3] 31 U.S.C. § 5330.

денег, а также сообщество лиц, которые осуществляют деятельность по внутренним и международным переводам средств за рамками общепринятых систем финансовых учреждений»[1].

Для целей применения положений об обязательной имплементации программы контроля над подозрительными операциями (*anti-money laundering program*), указанными в § 5318 (*h*), организация должна подпадать под понятие финансового учреждения в соответствии с дефиницией, содержащейся в § 5312 (*a*) (2), подразделяющей их на 26 категорий. Одной из таких категорий является «лицензированный отправитель денег или иное лицо, которое осуществляет деятельность в рамках неформальной системы денежных переводов, а также сообщество лиц, которые осуществляют деятельность по внутренним и международным переводам средств за рамками общепринятых систем финансовых учреждений».

Кроме того, видимо, в целях большей «ясности» в § 5318 (*h*) содержится ссылка на то, что подпадающее под ее действие финансовое учреждение также является организацией, оказывающей денежные услуги (*Money Services Businesses*). Положения, регулирующие деятельность таких организаций, содержат свое понятие *money transmitter'a*: «любое лицо, вне зависимости от наличия лицензии или необходимости ее получения, которое осуществляет деятельность по принятию валюты или средств, номинированных в валюте, и переводит валюту или средства либо стоимость, содержащуюся в валюте или средствах любыми способами посредством финансовых учреждений, Федерального резервного банка или его подразделений, или электронной системы перевода средств; или любое иное лицо, осуществляющее деятельность по переводу средств[2]. Правда, видимо, осознавая всю широту приведенных дефиниций, делается оговорка о том, что вопрос о том, является ли лицо *money transmitter*'ом, должен решаться с учетом конкретных фактов и обстоятельств дела. Кроме того, под понятие *money transmitter*'а не подпадает физическое лицо, которое осуществляет соответствующую деятельность на несистематической основе и без намерения извлечения прибыли[3].

Очевидно, что при наличии столь запутанного федерального регулирования, усугубляемого обширным нормотворчеством штатов, никогда нельзя быть уверенным в том, что вновь разработанная бизнес-модель или инновационное средство совершения платежей полностью

[1] 31 U.S.C. § 5330 (*d*) (1).
[2] 31 C.F.R. § 103.11 (*uu*) (5) (*i*).
[3] 31 C.F.R. § 1010.100 (*ff*) (5) (*ii*); § 1010.100 (*ff*) (8) (*iii*).

ему соответствуют. В литературе отмечаются существенные сложности в юридическом консультировании клиентов, которые хотят внедрить новые платежные механизмы[1]. Вряд ли в связи с этим американский подход может представлять собой большую ценность с точки зрения его возможного заимствования иными правопорядками.

Для полноты картины необходимо указать, что несоблюдение со стороны *money transmitters* положений, связанных с имплементацией программ по противодействию легализации доходов, полученных преступным путем, влечет достаточно серьезную ответственность: штраф до 25 000 долл. в день (за умышленное нарушение) за несоблюдение существующей программы или штраф до 500 000 долл. за отсутствие такой программы в организации[2]. Также за осуществление незаконной деятельности по переводу денежных средств предусмотрена уголовная ответственность в виде лишения свободы сроком до 5 лет[3].

Столь часто упоминаемая либеральность существующего в США подхода к регулированию электронных денег[4] была уже протестирована на себе некоторыми эмитентами электронных денег. Широкий резонанс получил процесс, инициированный в отношении известной в сети Интернет платежной системы *e-gold*[5]. Данная система представляла собой платежи в альтернативной валюте, номинированной в граммах золота. При этом золото в объеме, покрывавшем соответствующие требования, находилось на хранении в репозиториях *E-gold Ltd*, сертифицированных Лондонской ассоциацией торговцев слитками в виде особого траста в пользу владельцев счетов в системе *e-gold*. Счета таких владельцев, равно как и операции по ним, были анонимны, один пользователь мог иметь множество счетов[6].

В отношении владельцев системы *e-gold* 24 апреля 2007 г. был инициирован судебный процесс, в котором помимо всего прочего они были обвинены в 1) сговоре, направленном на использование финансовых инструментов в целях легализации доходов, полученных преступным путем, а также в 2) осуществлении деятельности по переводу средств в отсутствие лицензии. В качестве общего обоснования

---

[1] *Hughes S., Middlebrook S., Peterson B.* Developments in the Law Concerning Stored-Value Cards and Other Electronic Payments Products // The Business Lawyer. 2007. No 63. P. 260.

[2] http://www.irs.gov/irm/part4/irm 04-026-007.html

[3] 18 U.S.C. § 1960 (*a*) (Supp. V 2005).

[4] См., например: *Кочергин Д.А.* Указ. соч. С. 20; *Akindemowo O.* Electronic Money Regulation: A Comparative Survey of Policy Influences in Australia, European Union and US // Journal of Law and Information Science. No 11. 2001. P. 68–70.

[5] US v E-Gold, Ltd. 550 F Supp 2d 82, (2008).

[6] См.: *Мартынов В.Г., Андреев А.Ф., Кузнецов В.А., Шамраев А.В и др.* Указ. соч. С. 31.

вины владельцев системы было заявлено, что вопреки требованиям законодательства они не предпринимали должных усилий по идентификации своих пользователей, позволяя им заводить аккаунты под именами вроде «Микки Маус» или «Аноним». Применительно к обвинениям по п. 1 были также заявления о том, что переводы в системе *e-gold* нередко использовались для осуществления незаконной деятельности (оплата детской порнографии, незаконные инвестиционные схемы и финансовые пирамиды). В основе п. 2 обвинений лежала квалификация стороной обвинения деятельности системы *e-gold* как организации, осуществляющей перевод средств (*money transmitter)*, что требовало получения лицензии. По мнению представителей *e-gold*, их деятельность не подпадала под понятие *money transmitter*, поскольку переводов денежных средств как таковых не осуществлялось, а имела место *продажа прав* на драгоценные металлы. Данный аргумент не показался убедительным суду, поскольку, как можно судить из приведенных ранее определений данного понятия, они сформулированы таким образом, что под них можно подвести практически любую систематическую деятельность по переводу чего-либо ценного в качестве средства платежа. В итоге обвинения были признаны обоснованными и суд обязал владельцев *e-gold* получить необходимые лицензии во всех штатах, где он осуществлял деятельность (т.е. практически во всех), а также имплементировать программу, направленную на противодействие легализации доходов, полученных преступным путем, что в конечном счете оказалось неподъемным бременем для компании, через некоторое время прекратившей свою деятельность[1].

Правовое регулирование электронных денег в Европейском союзе

Органы денежно-кредитного регулирования Европейского союза заняли достаточно противоречивую позицию по отношению к электронным деньгам. Европейский центральный банк и Европейская комиссия подчеркивали необходимость подвергнуть эмитентов электронных денег ясному и строгому регулированию, гарантирующему техническую и финансовую безопасность, защиту потребителей и взаимную совместимость различных видов электронных платежных инструментов.

В 1994 г. Европейский валютный институт (предшественник Европейского центрального банка) опубликовал первый отчет по элек-

[1] *Kim Zetter*. Bullion and Bandits: The Improbable Rise and Fall of E-Gold // http://www.wired.com/threatlevel/2009/06/e-gold

тронным деньгам, одна из основных идей которого сводилась к тому, что их эмиссия должна быть позволена только банкам[1].

Со своей стороны Европейская комиссия допускала выпуск электронных денег небанковскими организациями и введение упрощенного порядка регулирования их деятельности[2]. В итоге победила точка зрения Европейской комиссии, поскольку считалось, что более либеральный подход в данном вопросе будет стимулировать конкуренцию между эмитентами. Нетрудно заметить здесь определенное влияние и со стороны США с их рыночно-ориентированным, либеральным подходом к данному вопросу.

Одним из основных документов, направленных на регулирование вопросов, связанных с эмиссией и использованием электронных денег, стала Директива № 2000/46/ЕС «Об учреждении, деятельности и пруденциальном надзоре над деятельностью институтов, осуществляющих эмиссию электронных денег» (далее – Директива об электронных деньгах 2000 г.»[3]. Данная Директива ввела понятие института, осуществляющего эмиссию электронных денег (*Electronic Money Institute, ELMI*), под которым понимается юридическое лицо, осуществляющее эмиссию средств платежа в виде электронных денег.

Под электронными деньгами понимается денежная стоимость, которая представлена в виде требования к эмитенту и которая: а) хранится на электронном устройстве; б) выпускается по получении эмитентом средств в размере не менее внесенной в качестве предоплаты денежной суммы; в) принимается в качестве средства платежа иными учреждениями, чем эмитент. Данная дефиниция позволяет отграничить электронные деньги от различного рода предоплаченных карт, используемых отдельными предприятиями, которые предоставляют право скидок или приобретения товаров у данной организации: в данном случае не выполняется условие «в», так как такие электронные деньги представляют собой средство платежа, существующее лишь в отношениях с эмитентом. Кроме этого, условие «а» позволяет отграничить электронные деньги от средств электронного доступа к банковским счетам, поскольку в последнем случае денежная стоимость расположена не на электронном устройстве, а на банковском

[1] Working Group on EU Payment Systems. Report to the Council of the European Monetary Institute on Prepaid Cards. Brussels: European Monetary Institute. May 1994.

[2] Parliament Resolution on Electronic Money and Economic and Monetary Union // Bulletin EU 1/2. 03.10.1998.

[3] Directive 2000/46/EC of 18.09.2000 «On the Taking up, Pursuit of and Prudential Supervision of the Business of Electronic Money Institutions» // Official Journal of the European Communities. 2000. L. 275.

счете. Правда, данная дефиниция не позволяет дать однозначный ответ на вопрос о том, подпадают ли под сферу действия Директивы системы электронных денег, использующие удаленный доступ к серверам (*Server-Based Systems*)[1]. Фактически данный вопрос был оставлен на усмотрение национального законодательства государств – членов ЕС.

Директива об электронных деньгах содержит ряд требований к эмитентам электронных денег:

1) установление специальной правоспособности эмитентов электронных денег. Несмотря на то что такие организации могут и не являться банками, они не могут осуществлять иную деятельность, кроме как связанную с эмиссией электронных денег и оказанием сопутствующих услуг (администрирование электронных денег, включая их учет, сохранение финансовой информации на электронных носителях, полученной от других организаций). Такие эмитенты не должны иметь долей в других организациях, за исключением тех, которые связаны с эмиссией электронных денег. При этом сами кредитные институты не ограничены в праве на эмиссию электронных денег, поскольку считается, что они уже находятся под достаточным контролем, обеспечивающим безопасность такого рода деятельности[2];

2) требования к размеру собственного капитала. Первоначальный размер такого капитала должен быть не менее 1 млн евро. Впоследствии он должен быть не менее 2% текущих обязательств по эмитированным электронным деньгам;

3) требования к объектам инвестирования привлеченных средств. Эмитенты имеют право инвестировать полученные в оплату за электронные деньги средства только в активы с нулевым риском или иные высоколиквидные инструменты, отвечающие установленным требованиям;

4) подотчетность контрольным органам. В частности, эмитенты должны сообщать информацию об объеме собственного капитала, объеме эмитированных электронных денег и информацию об активах, в которые были осуществлены инвестиции.

Как показало время, Директива об электронных деньгах 2000 г. не оправдала возложенных на нее надежд. Расчет на возникновение высококонкурентного рынка в сфере эмиссии электронных денег не оправдался[3]. Создать новую организацию –эмитента электронных денег

[1] *Graham Smith*. Op. cit. P. 903–904.

[2] Понятие кредитного института для данных целей содержится в Директиве № 2006/48/ЕС (ст. 4 (1)).

[3] *Graham Smith*. Op. cit. P. 906.

на практике было ненамного легче, чем создать новый банк. К тому же та модель, которая закладывалась при разработке Директивы (специализированный эмитент электронных денег, который не занимается никакими иными видами деятельности), не оправдалась на практике. Ограничения, установленные на инвестирование средств, поступивших в обмен на электронные деньги, не позволяли получить доход, который бы окупил те многочисленные затраты, которые необходимо было понести для обеспечения соответствия условиям Директивы. А те бизнес-модели, которые сформировались после принятия Директивы и характеризуются выпуском электронных денег организациями, аккумулировавшими средства от оказания иных услуг (например, операторы сотовой связи, эмитенты дорожных чеков), не очень укладывались в формат Директивы[1]. В итоге лицензию на выпуск электронных денег в рамках данной Директивы получили шесть европейских операторов, из которых реально работали по ней лишь три[2].

Как следствие, после многочисленных консультаций и дискуссий в сентябре 2009 г. была принята новая Директива об электронных деньгах[3].

Директива № 2009/110/ЕС содержит новое, более технологически нейтральное определение электронных денег: «электронно- в том числе магнитно хранимая денежная стоимость, представленная в виде требования на эмитента, которое выпускается при получении денежных средств эмитентом для совершения платежей и которое принимается в качестве средства платежа иными учреждениями, нежели эмитент электронных денег». Исключение из дефиниции электронных денег ссылки на электронное устройство, на котором должна размещаться денежная стоимость, позволило снять вопрос о статусе систем электронных денег, использующих удаленный доступ к серверам.

Из-под сферы действия новой Директивы исключены:

1) предоплаченные инструменты одноцелевого или ограниченного целевого использования (ваучеры на питание, топливные карты, карты супермаркетов), поскольку они предназначены для приобретения товаров и услуг у эмитента или в пределах ограниченной сети поставщиков услуг, с которыми у эмитента установлены прямые торговые отношения. Однако при этом сделана оговорка о том, что если такие инструменты

---

[1] *Reed C.* Internet Law. Text and Materials. Cambridge University Press, 2004. P. 284.

[2] *Генкин А., Суворова Е.* Указ. соч. С. 184.

[3] Directive 2009/110/EC of 16.09.2009 «On the Taking up, Pursuit of and Prudential Supervision of the Business of Electronic Money Institutions Amending Directives 2005/60/EC and 2006/48/EC and Repealing Directive 200/46/EC» // Official Journal of the European Communities. 2009. L. 267.

превращаются в многоцелевые или универсальные, то на них начинают распространяться требования Директивы (п. 5 преамбулы);

2) денежная стоимость, использующаяся для приобретения цифрового контента при условии, что оператор телекомуникационных услуг, посредством которых осуществляется транзакция, не выполняет функцию исключительно посредника в совершении платежа (п. 6 преамбулы). В качестве примера, когда оператор является исключительно платежным посредником между продавцом контента и потребителем, можно привести ситуации, когда абонент сотовой сети связи платит напрямую оператору связи в отсутствие непосредственных договорных отношений между поставщиком контента и таким абонентом. В таких случаях средства, используемые для оплаты такого контента, подпадают под понятие электронных денег.

Важно отметить, что данные исключения применяются автоматически в отличие от ранее действовавшей Директивы, требовавшей предварительного согласования с регулятором возможности их применения.

Новая Директива снизила требования к размеру собственного капитала с 1 000 000 евро до 350 000 евро, расширила перечень допустимых видов деятельности, которыми могут заниматься эмитенты электронных денег, разрешила привлечение дистрибьюторов и агентов. Кроме того, был расширен перечень институтов, которые могут эмитировать электронные деньги, включив в него помимо *ELMI* и кредитных институтов Европейский центральный банк и центральные банки государств – членов ЕС, почтовые отделения и органы власти государств – членов ЕС (в пределах, установленных национальным законодательством).

Для того чтобы деятельность эмитентов электронных денег не подпадала под понятие привлечения средств на депозит, им запрещено выдавать кредиты из средств, полученных в качестве оплаты за электронные деньги, а также выплачивать проценты или иные формы дохода на денежные средства, лежащие в основе эмиссии электронных денег.

Наконец, более четко прописаны отдельные аспекты регулирования отношений между эмитентом электронных денег и их держателями. Так, по требованию держателя электронных денег эмитент обязан осуществить возмещение их стоимости в любой момент по их номинальной стоимости. Условия соглашения должны предусматривать условия выкупа и возможных комиссионных платежей. В целях противодействия использованию электронных денег в целях отмывания доходов, полученных преступным путем, установлен максималь-

ный размер денежных средств, при котором могут не применяться специальные меры контроля: 250 евро при отсутствии возможности пополнения такого носителя либо 2500 евро в течение календарного года – при наличии такой возможности. При определенных условиях в национальном законодательстве сумма в 250 евро может быть увеличена до 500 евро, правда, только в отношении внутригосударственных транзакций (ст. 19 (2) Директивы № 2009/110/ЕС).

§ 5. Правовое регулирование электронных денег в России

До недавнего времени электронные деньги в России не могли похвастаться наличием специального правового регулирования, по крайней мере на уровне законов и иных нормативных правовых актов.

Основным правовым подспорьем обращению электронных денег в российской экономике долгое время являлся п. 3 ст. 847 ГК РФ, который предусматривает возможность удостоверения прав распоряжением денежными суммами, находящимися на счете, электронными средствами платежа и дргуими документами с использованием в них аналогов собственноручной подписи, кодов, паролей и иных средств, подтверждающих, что распоряжение дано уполномоченным на это лицом[1].

Что касается подзаконных актов, регламентировавших данную сферу, то из таковых можно было назвать лишь не действующее ныне указание ЦБ РФ от 3 июля 1998 г. № 277-У «О порядке выдачи регистрационных свидетельств кредитным организациям-резидентам на осуществление эмиссии предоплаченных финансовых продуктов»[2]. Данный документ был в течение долгого времени практически единственным источником правовых норм об электронных деньгах в России[3]. Он предусматривал уведомительный порядок регистрации кредитных организаций-резидентов с выдачей им регистрационного свидетельства на осуществление эмиссии предоплаченных финансовых продуктов. Данный документ не предполагал возможности отзыва выданного свидетельства и был направлен преимущественно на предоставление Банку России информации о будущем эмитенте, его технологиях и до-

[1] См.: *Мартынов В.Г., Андреев А.Ф., Кузнецов В.А., Шамраев А.В и др.* Указ. соч. С. 5.

[2] Отменено в связи с принятием Положения Банка России от 24 декабря 2004 г. № 266-П «Об эмиссии банковских карт и об операциях, совершаемых с использованием платежных карт».

[3] См. подробнее: *Башкатов М.* Правовая природа «электронных денег» // Хозяйство и право. 2003. № 8. С. 85.

говорной модели. В период действия данного Указания регистрационное свидетельство было выдано лишь одному эмитенту электронных денег – Банку «Таврический».

Учитывая ограниченную сферу действия данного Указания по субъектному составу (адресат – кредитные организации) и по предмету, можно утверждать, что отношения, возникающие в связи с использованием электронных денег в России, регулировались преимущественно в договорном порядке, а также обычаями делового оборота.

Ситуация в значительной степени изменилась с принятием Закона о НПС. Данный Закон устанавливает правовые и организационные основы национальной платежной системы, регулирует порядок оказания платежных услуг, в том числе порядок осуществления перевода денежных средств, использования электронных средств платежа, деятельность субъектов национальной платежной системы, а также определяет требования к организации и функционированию платежных систем, порядок осуществления надзора и наблюдения в национальной платежной системе. Следует отметить, что одновременно с ним был принят Федеральный закон от 27 июня 2011 г. № 162-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации в связи с принятием Федерального закона «О национальной платежной системе»», в котором также содержится ряд важных положений, имеющих отношение к использованию электронных денег. Не случайно в доктрине данные законы рассматриваются как единое целое под обобщенным названием *законов* о НПС[1].

Закон о НПС впервые ввел в российское законодательство дефиницию электронных денежных средств, под которыми понимаются «денежные средства, которые предварительно предоставлены одним лицом (лицом, предоставившим денежные средства) другому лицу, учитывающему информацию о размере предоставленных денежных средств без открытия банковского счета (обязанному лицу), для исполнения денежных обязательств лица, предоставившего денежные средства, перед третьими лицами, и в отношении которых лицо, предоставившее денежные средства, имеет право передавать распоряжения исключительно с использованием электронных средств платежа» (п. 18 ст. 3)[2].

---

[1] См., например: *Лисицын А.Ю.* Систематизация в эмиссионном праве // Реформы и право. 2012. № 4.

[2] Термин «электронные деньги» в законе не используется, однако в рамках данной работы термины «электронные деньги» и «электронные денежные средства» будут использоваться как синонимы по причине того, что термин «электронные деньги»

Как видно, в данном случае отечественный законодатель предпочел пойти своим путем и не заимствовать дословно дефиницию электронных денег, закрепленную в Директиве № 2009/110/ЕС. Главным отличием от последней помимо громоздкости является отсутствие понятия «денежная стоимость» и указания на то, что она хранится в электронной форме. Тем не менее основная цель, которую преследовали европейские законодатели при введении указанных понятий (отграничение электронных денег от продуктов удаленного доступа к банковским счетам), достигается за счет оговорки о том, что денежные средства предоставляются без открытия банковского счета. Так что можно говорить о том, что дефиниции электронных денег, содержащиеся в европейском и российском законодательстве, являются схожими.

Расчеты электронными деньгами были причислены Законом о НПС к иной форме безналичных расчетов, что допустимо в силу п. 1 ст. 862 ГК РФ. Как отмечается, это позволило «уйти от вопроса о денежных суррогатах и частной эмиссии денег. Кроме того, это позволило распространить на электронные денежные средства те правовые механизмы, которые применяются в рамках налоговых и иных публично-правовых отношений к денежным средствам на банковских счетах (взыскание, приостановление операций, запрос остатка)»[1].

В Законе о НПС отсутствует понятие эмитента электронных денег, его функцию выполняет понятие «оператор электронных денежных средств», которое раскрывается в п. 3 ст. 3 как «оператор по переводу денежных средств, осуществляющий перевод денежных средств без открытия банковского счета»; таким лицом может быть *только кредитная организация*, в том числе небанковская кредитная организация, имеющая право на осуществление переводов денежных средств без открытия банковских счетов и связанных с ними иных банковских операций (НКО)[2]. В отношении таких небанковских кредитных организаций Законом о внесении изменений установлен упрощенный порядок лицензирования и упрощенные пруденциальные требования. Минимальный уставный капитал для регистрации вновь создаваемой НКО составляет 18 млн руб.

является широко распространенным в юридических и экономических кругах в России и за рубежом.

[1] *Шамраев А.В.* Законодательство о национальной платежной системе и его влияние на развитие платежных инноваций // Банковское право. 2011. № 5.

[2] Подробнее о статусе НКО в контексте Закона о НПС см.: *Тарасенко О.А.* Платежные небанковские кредитные организации – новый субъект предпринимательской деятельности в банковской системе России // Законы России: опыт, анализ, практика. 2012. № 1.

Осуществление лицом, не являющимся кредитной организацией, на основании передаваемых ему физическими лицами распоряжений в электронном виде, деятельности по исполнению денежных обязательств указанных физических лиц перед поставщиками услуг (товаров, работ) за счет предварительно предоставленных денежных средств является нарушением законодательства Российской Федерации. В соответствии с разъяснениями ЦБ РФ это относится и к случаям выпуска лицами, не являющимися кредитными организациями, различного рода «подарочных», «накопительных», «дисконтных», «бонусных» карт в целях их использования физическими лицами для расчетов с поставщиками услуг (товаров, работ), отличными от эмитентов карт[1]. То же самое справедливо и в отношении операторов мобильной связи, которые допускают использование авансов физических лиц по оплате услуг мобильной связи для расчетов с поставщиками услуг (товаров, работ).

Закон о НПС выделяет целый ряд лиц, осуществляющих деятельность в сфере обращения электронных денег, закрепляя требования к ним и соответствующие обязанности. Помимо уже упомянутого оператора по переводу денежных средств к таким лицам относятся:

– оператор платежной системы, основной функцией которого является определение правил платежной системы;

– оператор услуг платежной инфраструктуры – организация, обеспечивающая для участников платежной системы и их клиентов доступ к услугам по переводу денежных средств, в том числе с использованием электронных средств платежа, а также обмен электронными сообщениями (операционный, клиринговый и расчетный центры);

– банковские платежные агенты (субагенты), которые вправе на основании договора с кредитной организацией (банковским платежным агентом) принимать наличные денежные средства в целях увеличения остатков электронных денежных средств[2], выдавать наличные денежные средства при возврате остатков электронных денежных средств, предоставлять клиентам электронные средства платежа (например, карты или иные электронные носители) и обеспечивать возможность их использования для переводов электронных денежных средств. Кроме того, банковские платежные агенты могут привлекаться для проведения идентификации клиента – физического лица, его представителя

[1] См.: разъяснения ЦБ РФ по вопросам применения отдельных положений Федерального закона от 27 июня 2011 г. № 161-ФЗ «О национальной платежной системе» от 28 февраля 2013 г. // http://cbr.ru/press/Archive_get_blob.aspx?doc_id=130228_1809533.htm

[2] См.: Федеральный закон от 3 июня 2009 г. № 103-ФЗ «О деятельности по приему платежей физических лиц, осуществляемой платежными агентами».

и (или) выгодоприобретателя в целях осуществления перевода электронных денежных средств. Последнее особенно важно, учитывая дистанционную сущность электронных денег. В качестве банковских платежных агентов могут выступать операторы связи[1].

Надзорные функции в отношении платежных систем осуществляет ЦБ РФ. В случае выявления нарушения требований Закона о НПС или принятых в соответствии с ним нормативных актов Банка России поднадзорной организацией, которые влияют на бесперебойность функционирования платежной системы либо на услуги, оказываемые участникам платежной системы и их клиентам, ЦБ РФ может приостановить оказание операционных услуг (п. 2 ч. 2 ст. 34 Закона о НПС).

Закон о НПС устанавливает ряд ограничений, связанных с использованием электронных денег в обороте.

1. *Запрет на электронное кредитование*. В Законе нашел свое отражение взгляд на электронные деньги как на предоплаченный финансовый продукт. Оператор электронных денежных платежей вправе присвоить клиенту только то количество электронных денег, которое было предварительно оплачено им в наличном или безналичном порядке. Электронное кредитование (предоставление оператором электронных денежных средств клиенту собственных денежных средств для увеличения остатка его электронных средств) не допускается. Данное ограничение направлено на обеспечение контроля над объемом денежной массы в стране и предотвращение появления «новых денег»[2].

При этом предусмотрена возможность взаимодействия операторов электронных денежных средств и операторов связи. Так, оператор электронных денежных средств вправе заключить с оператором связи договор, по условиям которого оператор электронных денежных средств вправе увеличивать остаток электронных денежных средств физического лица – абонента такого оператора связи за счет его денежных средств, являющихся авансом за услуги связи (ст. 13 Закона о НПС). Но в этом случае суть электронных денег как предоплаченного финансового продукта не меняется. Установлен запрет на предоставление оператором связи физическому лицу – абоненту денежных средств

[1] *Шамраев А.В.* Указ. соч.

[2] Примечательно, что некоторые специалисты придают настолько важное значение электронному кредиту, что связывают с его распространением возможности возникновения наднациональных денег, неотличимых по функциям от обычных банкнот, которые смогут существовать и без их конвертируемости в национальную валюту. *Operkent A.* The Problems of Electronic Money and EC Banking & Tax Law // Journal of Monetary Economics. 1994. No 6. P. 59–60.

в целях увеличения оператором электронных денежных средств остатка электронных денежных средств.

2. *Установление ограничений в использовании электронных денег по субъектному составу*. Электронные деньги представляют собой платежный инструмент, ориентированный исключительно на отношения с участием физических лиц (*B2C*- и *C2C*- сегменты электронной коммерции). Осуществление расчетов электронными деньгами между юридическими лицами и индивидуальными предпринимателями недопустимо. Во многом это связано с нежеланием законодателя подрывать традиционные формы безналичных расчетов и связанные с ними возможности контроля допущением возможности совершения анонимных платежей электронными деньгами между хозяйствующими субъектами. Юридическое лицо или индивидуальный предприниматель могут выступать плательщиком электронными деньгами только в случае, если получателем является физическое лицо. Перечень возможных операций с остатком электронных денежных средств у юридических лиц и индивидуальных предпринимателей существенно ограничен: он может быть только зачислен на их банковский счет и не может быть выдан наличными деньгами или переведен без открытия банковского счета (п. 9, 20 ст. 7 Закона о НПС).

3. *Распространение на расчеты электронными деньгами норм законодательства о валютном контроле*. В соответствии с п. 25 ст. 7 Закона о НПС на переводы электронных денежных средств в иностранной валюте между резидентами, на переводы электронных денежных средств в иностранной валюте и валюте Российской Федерации между резидентами и нерезидентами, а также на переводы электронных денежных средств в иностранной валюте и валюте Российской Федерации между нерезидентами распространяются требования валютного законодательства Российской Федерации. Правда, само валютное законодательство пока об этом не очень догадывается. Дело в том, что под иностранной валютой и под валютой Российской Федерации понимаются лишь денежные знаки в виде соответствующих банкнот и монет, а также средства на банковских счетах и банковских вкладах (ст. 1 Федерального закона от 10 декабря 2003 г. № 173-ФЗ «О валютном регулировании и валютном контроле» (далее – Закон о валютном регулировании и валютном контроле)[1]). Электронные деньги не являются ни банкнотами, ни монетами, ни средствами на банковских счетах, ни средствами на банковских вкладах. Не являются они и ценными бумагами (еще

[1] РГ. 2003. 17 дек.

одним объектом регулирования законодательства о валютном контроле), хотя бы потому, что они не поименованы законом в качестве таковых, что требуется в силу ст. 143 ГК РФ. Электронные денежные средства являются по правовой сути имущественными правами, но такого объекта валютного регулирования в ст. 1 Закона не указано, равно как в нем не содержится понятия «денежные средства». Поскольку электронные денежные средства не охватываются понятием валюты (иностранной или отечественной), операции с ними не могут быть охарактеризованы в качестве валютных операций. А поскольку существующие ограничения касаются именно совершения отдельных валютных операций, получается, что они не распространяются на операции с электронными денежными средствами.

Аргумент о том, что Закон о НПС является более поздним и специальным, в силу чего должен применяться в приоритетном порядке, имеет сомнительную нормативную базу, поскольку ч. 1 ст. 4 Закона о валютном регулировании и валютном контроле закрепляет приоритет данного Закона: «Валютное законодательство Российской Федерации состоит из настоящего Федерального закона и принятых в соответствии с ним федеральных законов». Как следует из данного положения, все остальные законы, безотносительно к времени их принятия, должны соответствовать ему, в том числе и его основополагающим дефинициям. Примечательно, что в связи с принятием Закона о НПС были внесены изменения в ряд законодательных актов, в том числе и в Закон о валютном регулировании и валютном контроле, однако данные изменения не устранили вышеуказанного противоречия. По-видимому, считая самим собой разумеющимся факт отнесения электронных денежных средств к валюте, законодатель внес некоторые изменения в порядок осуществления операций с ними.

В частности, ст. 10 Закона о валютном регулировании и валютном контроле была дополнена ч. 1^1 следующего содержания: «Нерезиденты вправе без ограничений осуществлять между собой на территории Российской Федерации переводы иностранной валюты и валюты Российской Федерации без открытия банковских счетов, а также осуществлять переводы иностранной валюты и валюты Российской Федерации без открытия банковских счетов с территории Российской Федерации и получать на территории Российской Федерации переводы иностранной валюты и валюты Российской Федерации без открытия банковских счетов».

Другие две нормы ккасаются *расчетов* при осуществлении валютных операций. Во-первых, юридические лица получили возможность

осуществлять такие расчеты путем перевода электронных денежных средств (абз. 1 ч. 2 ст. 14). Во-вторых, физические лица-резиденты теперь могут проводить расчеты при осуществлении валютных операций путем перевода без открытия банковских счетов (п. 9 ч. 3 ст. 14).

Таким образом, как можно увидеть, внесенные в Закон о валютном регулировании и валютном контроле изменения в целом направлены на либерализацию данного Закона применительно к случаям осуществления платежей электронными деньгами. Но в отсутствие четкого отнесения электронных денежных средств к категории «валюта» сохраняется неопределенность относительно возможности применения ряда положений данного Закона, устанавливающих ограничения на совершение валютных операций. Представляется, что до внесения соответствующих изменений должно применяться положение ч. 6 ст. 4 Закона о валютном регулировании и валютном контроле: «Все неустранимые сомнения, противоречия и неясности актов валютного законодательства Российской Федерации, актов органов валютного регулирования и актов органов валютного контроля толкуются в пользу резидентов и нерезидентов» и тем самым данный Закон должен толковаться максимально либерально по отношению к платежам, совершенным электронными деньгами, если они номинированы в иностранной валюте или совершаются с участием нерезидентов.

4. *Установлен максимальный лимит на размер остатка электронных денежных средств.* При этом указанный лимит различается в зависимости от того, является электронный кошелек персонифицированным или анонимным (неперсонифицированным). При наличии идентификации клиента в соответствии с Федеральным законом от 7 августа 2001 г. № 115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма» максимальный лимит остатка электронных денег может составлять 100 000 руб. (или эквивалентную по размеру сумму в иностранной валюте по официальному курсу ЦБ РФ без учета возможных колебаний курса). В случае превышения установленного размера остатка электронных денег организаций и индивидуальных предпринимателей оператор электронных денежных средств обязан без распоряжения осуществить зачисление или перевод денежных средств в размере превышения указанного ограничения на банковский счет, а в отношении физических лиц – по распоряжению осуществить перевод на банковский счет, перевод без открытия банковского счета или выдать наличными денежными средствами. Остаток электронных денежных средств на корпоративном электронном кошельке не должен превы-

шать 100 000 рублей на конец рабочего дня оператора электронных денежных средств. При этом ограничений на объем операций, совершаемых при помощи корпоративного кошелька, не предусмотрено.

Анонимные электронные кошельки и анонимные переводы электронных денег хотя и не запрещены *per se*, но имеют весьма ограниченную платежную способность: их лимит остатка не может превышать 15 000 руб. При этом общая сумма переводимых электронных денежных средств с использованием одного неперсонифицированного электронного средства платежа не может превышать 40 000 руб. в течение календарного месяца (лимитов для перевода средств со счета на счет в отношении персонализированных кошельков не установлено). Данные ограничения установлены в целях противодействия возможному использованию электронных денежных средств для целей отмывания преступных доходов и противодействию терроризму. Несмотря на то что ограничения на размер суммы остатка электронных денежных средств на носителе существуют и в зарубежном законодательстве, в России они реализованы с некоторым своеобразием. Если, скажем, в Европе указанные суммы являются критерием для освобождения от обязанности осуществления мер по контролю сделок в рамках «антиотмывочного» законодательства, а размер сумм зависит от возможности пополнения остатка электронных денежных средств на техническом устройстве, являющемся их носителем, то в России соответствующие ограничения превращены в жесткие запреты, а максимальный размер остатка денежных средств зависит от персонализированности такого устройства. При этом не очень ясно, как данные ограничения будут сочетаться с формально не ограниченной законом возможности лица заводить неограниченное количество электронных кошельков.

Анализ приведенных ограничений (запрет на электронное кредитование, запрет на использование электронных денег в *B2B*-секторе, установление максимальных лимитов на размеры остатков электронных денежных средств) свидетельствует о желании законодателя и регуляторов придать электронным деньгам характер нишевого финансового продукта, ориентированного на отношения с физическими лицами. При этом электронные деньги, будучи разновидностью электронного платежного средства, могут выполнять лишь функцию средства платежа и не могут быть средством тезаврации, т.е. выступать тем активом, который можно хранить и использовать в качестве инструмента накопления богатства, что существенно отличает электронные деньги в российском понимании от классических денег.

Закон о НПС содержит также положения, направленные на регулирование договорных отношений между оператором электронных денежных средств и клиентом.

В соответствии с ч. 1 ст. 9 Закона о НПС между клиентом и оператором заключается договор об использовании электронного средства платежа. Возникает вопрос о правовой природе данного договора. С одной стороны, его вроде бы смело можно рассматривать в качестве самостоятельного поименованного договора, поскольку он не только прямо упомянут в Законе, но имеет место и определенная позитивно-правовая регламентация отношений сторон, возникающих в рамках данного договора[1]. Вместе с тем достаточно часто встречается квалификация рассматриваемых отношений в качестве агентских, причем не только до введения в действие Закона о НПС[2], но и после[3]. Если отталкиваться от дефиниции электронных денежных средств, согласно которой основное их назначение – исполнение денежных обязательств перед третьими лицами, которое осуществляется оператором, то вполне можно квалифицировать данные отношения в качестве посреднических. Такая квалификация вполне имела право на существование в условиях правового вакуума, существовавшего до принятия Закона о НПС. После принятия данного Закона пространства для применения норм ГК РФ об агентском договоре даже с учетом субсидиарного применения норм о договоре поручения (поскольку именно модель договора поручения является наиболее близкой к существу отношений при платежах электронными деньгами) не осталось. Все соответствующие аспекты, упомянутые в гл. 52 «Агентский договор» ГК РФ, так или иначе нашли свое отражение в Законе о НПС (полномочия оператора денежных средств, регламентация вопросов вознаграждения, отчеты, прекращение договора, возможность привлечения третьих лиц к процессу исполнения обязательства). Некоторые статьи вроде ст. 1007 ГК РФ, посвященной возможности ограничения сферы действия агента по территории, кругу субъектов и т.п., неприменимы в принципе *as is* к отношениям, возникающим в связи с платежом электронными деньгами. Так что не отрицая посреднический характер рассматриваемых отношений, их юридическая квалификация в качестве агентского договора в настоящее время невозможна.

---

[1] См. подробнее: *Карапетов А.Г., Савельев А.И.* Свобода заключения непоименованных договоров и ее пределы.

[2] См., например: *Левашов С.* Электронные деньги – фикция? // эж-Юрист. 2005. № 48; *Генкин А., Суворова Е.* Указ. соч. С. 247; *Шахунян М.* Кошелек или веб-суррогат? // эж-Юрист. 2010. № 24.

[3] *Балкаров А.* Реальный оборот виртуальных денег // эж-Юрист. 2012. № 38.

Особенностью договора об использовании электронного средства платежа является право оператора отказать клиенту в его заключении (ч. 2 ст. 9 Закона о НПС), что однозначно выводит данный договор из категории публичных договоров (ст. 426 ГК РФ), конститутивным признаком которого является обязанность коммерческой организации заключить соответствующий договор с каждым, кто обратился (при наличии возможности исполнения такого договора). К сожалению, Закон о НПС не приводит перечня оснований для такого отказа, что вряд ли можно отнести к его достоинствам. Также неясно, как на практике оператором электронных денежных средств будет реализовано такое право на отказ, принимая во внимание, что большинство соглашений, опосредующих платежи электронными деньгами, заключаются посредством сети Интернет и представляют собой договоры присоединения в виде *click-wrap*-соглашений, процесс заключения которых автоматизирован.

Закон о НПС предусматривает обширные информационные обязанности операторов электронных денежных средств. До заключения с клиентом договора об использовании электронного средства платежа он обязан информировать клиента о своем наименовании и местонахождении, об условиях использования электронного средства платежа, в частности о любых ограничениях способов и мест использования, случаях повышенного риска использования электронного средства платежа, а также о размере и порядке взимания вознаграждения (при его наличии), способах подачи претензий и порядке их рассмотрения.

Оператор по переводу денежных средств также обязан информировать клиента о совершении каждой операции с использованием электронного средства платежа путем направления клиенту соответствующего уведомления в порядке, установленном договором с клиентом, и в соответствии с имеющейся у оператора контактной информацией клиента. При этом обязанностью клиента является предоставление достоверной информации для связи с ним и своевременное уведомление о ее изменении.

Данные правила имеют не только важное значение с точки зрения обеспечения информированного выбора клиентом соответствующего электронного средства платежа. К исполнению сторонами своих информационных обязанностей привязано и распределение рисков между оператором электронных денежных средств и клиентом на случай совершения несанкционированных операций. Распределение рисков построено на основе принципа «Рискует тот, кто не уведомляет». В случае обнаружения факта несанкционированного исполь-

зования электронных денег, в том числе на основании полученного от оператора уведомления о совершенной операции, клиент должен незамедлительно сообщить об этом оператору. После получения такого уведомления риск совершения последующих несанкционированных операций возлагается на оператора и он обязан возместить соответствующие суммы операций (ч. 12 ст. 9 Закона о НПС). Если оператор не исполнил свою обязанность по информированию клиента о каждой операции, то на него возлагается обязанность возмещения сумм операций, которые были совершены без согласия клиента и о которых он не был проинформирован. Если же уведомление об операции все же было направлено клиенту, но тот не отреагировал, то риск неблагоприятных последствий такой операции возлагается на клиента[1].

Рассмотрев наиболее важные положения Закона о НПС в части, касающейся регламентации понятия электронных денег и процесса совершения платежей ими, имеет смысл коснуться того, насколько нормы данного Закона нашли свое отражение в наиболее популярных российских системах электронных денег: Яндекс.Деньги и *Webmoney*. Сопоставление данных систем тем более интересно, если учесть различия в их подходах к адаптации своих бизнес-моделей к требованиям Закона о НПС.

Система «Яндекс.Деньги» провела немалую работу по приведению своей платежной системы в соответствие с требованиями Закона о НПС. В качестве компании – оператора электронных денежных средства выступает ООО НКО «Яндекс.Деньги», получившая статус небанковской кредитной организации. Отношения с пользователями регламентируются Соглашением об осуществлении переводов денежных средств без открытия счета с использованием сервиса «Яндекс. Деньги», которое является весьма объемным документом (порядка 24 страниц формата А4) и в целом отражает основные идеи и терминологию Закона о НПС[2].

В соответствии с требованиям Закона о НПС были введены ограничения на лимит остатка анонимных и персонализированных электронных кошельков. Правда, представители системы «Яндекс.Деньги» проявили завидную смекалку в адаптации данных ограничений к сложившимся привычкам пользователей. Общий баланс пользователя разделен на две части: доступный остаток, соответствующий требованиям Закона, и средства, находящиеся в очереди пополнения счета, в отно-

[1] Положения ч. 4–8 ст. 9 Закона о НПС, посвященные распределению рисков совершения несанкционированных операций, вступили в силу с 1 января 2014 г.

[2] http://money.yandex.ru/doc.xml?id=522764

шении которых никаких ограничений не установлено. Таким образом, к примеру, на анонимном кошельке может быть сумма в виде 50 000, из которой 15 000 фигурируют непосредственно на балансе, а остальные 35 000 – в очереди. По мере уменьшения баланса средства из очереди автоматически прибавляются к доступному остатку. Иными словами, средства, превышающие установленный Законом лимит, вытесняются в очередь и поступают на счет по мере траты денег на балансе[1].

Идентификация пользователей для целей приобретения персонализированных электронных кошельков может производиться различными способами, в частности в офисе компании, заказным письмом с нотариально заверенным заявлением внутри, через бюро кредитных историй *Equifax*, через салоны «Евросеть» и некоторыми иными способами.

В целом можно говорить о системе «Яндекс.Деньги» как о примере игры в соответствии с правилами, установленными Законом о НПС, возможно, за исключением хитрости с размерами электронных кошельков.

Несколько иное впечатление оставляют подходы, принятые в системе *Webmoney*.

Во-первых, статус оператора системы *Webmoney* является менее определенным. Как следует из данных официального сайта, ключевые субъекты, вовлеченные в процесс функционирования данной системы, не обладают статусом банка или НКО: ни представитель на территории Российской Федерации (ООО «ВебМани.Ру»), ни гарант по рублевым электронным кошелькам (ООО «*BMP*»)[2]. Тем не менее в процессе функционирования данной платежной системы задействованы организации, обладающие соответствующим статусом: НКО «Сетевая расчетная палата» и ОАО «Консервативный коммерческий банк» (для осуществления оплаты налогов и сборов). Во многом это связано с тем, что система *Webmoney* особым образом позиционирует существо отношений, возникающих в связи с использованием сервиса, что накладывает отпечаток на те правовые схемы, которые используются при ее функционировании.

Представители *Webmoney* заявляют, что данная система не является эмитентом электронных денежных средств, а осуществляет выпуск так называемых титульных знаков[3]. Данные титульные знаки различаются

[1] См.: *Грачева М.* Новые условия использования Яндекс.Денег — FAQ. 12 сентября 2012 // http://habrahabr.ru/company/yandex/blog/151290/

[2] http://www.webmoney.ru/rus/about/contacts/guarantors.shtml

[3] Как указано в Соглашении о трансфере имущественных прав цифровыми титульными знаками, *Webmoney* – универсальный титульный знак (*WM*) в цифровом виде; единица исчисления количества (объема) имущественных прав. Цена титульного знака

объектами, находящимися в их обеспечении: национальные валюты (*WMZ* – доллар США, *WME* – евро, *WMR* – российский рубль, *WMB* – белорусский рубль, *WMU* – украинская гривна), золото (*WMG*), криптовалюта *Bitcoin* (*WMX*). Иными словами, *Webmoney* – это не платежная система, поскольку в ней не осуществляется перевод денежных средств, это система учета имущественных прав.

Эмиссию титульных знаков определенного типа осуществляет так называемый гарант – организация, которая управляет обеспечением эмиссии, устанавливает эквивалент обмена на заявленные имущественные права, опубликовывает на веб-сайте системы оферту по куплепродаже титульных знаков гарантируемого типа.

Характеристика соглашений, заключаемых с гарантом в отношении тех или иных титульных знаков, варьируется в зависимости от их типа. Данные соглашения могут принимать форму соглашения об использовании чеков в электронной форме (*WMR*, *WME*), купли-продажи электронных денег (*WMB*), договора о предоставлении сервиса для осуществления покупок с использованием *WMZ*-сертификатов, договора уступки прав требования (*WMU*), договора хранения (*WMG*) и внимание: договора хранения имущественных прав (*WMX*)[1]. Очевидно, что в творческом подходе к квалификации возникающих отношений отказать юристам системы *Webmoney* никак нельзя. К сожалению, в связи с отсутствием в стандартных соглашениях *Webmoney* оговорок о применимом праве и связанной с этим неопределенностью в решении вопроса о том, насколько соответствуют предложенные соглашения требованиям применимого законодательства (хотя бы в частноправовой плоскости), ответить на вопрос об их жизнеспособности достаточно проблематично. Однако такого рода юридическая «акробатика», когда расчетные по своему существу отношения выдаются за все что угодно, но только не за электронные деньги, весьма смахивает на то, что называется обходом закона. Не случайно, на Украине уже возникли претензии к законности осуществления деятельности *Webmoney* без получения разрешения НБУ[2].

В литературе уже отмечалось, что вследствие данного подхода получается своего рода раздвоение, когда пользователи считают систему учета имущественных прав электронной платежной системой,

(условная сетевая стоимость) устанавливается его держателями, а порядок передачи и учета соответствует процедурам обращения сообщений формата «Титульные знаки» в *Webmoney Transfer* // http://www.webmoney.ru/rus/cooperation/legal/syagreement1.shtml

[1] http://www.webmoney.ru/rus/cooperation/legal/index.shtml

[2] *Марчак Д.* В чем налоговики обвиняют *WebMoney* // http://forbes.ua/business/1353859-v-chem-nalogoviki-obvinyayut-webmoney (дата обращения – 12 июня 2013 г.).

а ее титульные знаки – электронной наличностью, в то же время сама система представляет собой некую технологию, а не платежную систему или кредитную организацию[1]. К слову сказать, на своем официальном сайте *Webmoney* позиционирует себя как «международную систему расчетов и среду для ведения бизнеса в сети».

С точки зрения российского законодательства правовая природа сервисов *Webmoney* должна оцениваться через призму Закона о НПС. Формулировка электронного средства платежа, данная в Законе, является весьма широкой и специально была сформулирована таковой, чтобы охватить все многообразие существующих и перспективных технологий в этой области. Под электронным средством платежа понимается электронное средство платежа – средство и (или) способ, позволяющие клиенту оператора по переводу денежных средств составлять, удостоверять и передавать распоряжения в целях осуществления перевода денежных средств в рамках применяемых форм безналичных расчетов с использованием информационно-коммуникационных технологий, электронных носителей информации, в том числе платежных карт, а также иных технических устройств (п. 19 ст. 3). Основной вопрос состоит в том, являются ли титульные знаки электронными денежными средствами в понимании Закона о НПС?

Как отмечалось ранее, электронные денежные средства – денежные средства, которые предварительно предоставлены одним лицом (лицом, предоставившим денежные средства) другому лицу, учитывающему информацию о размере предоставленных денежных средств без открытия банковского счета (обязанному лицу), для исполнения денежных обязательств лица, предоставившего денежные средства, перед третьими лицами, и в отношении которых лицо, предоставившее денежные средства, имеет право передавать распоряжения исключительно с использованием электронных средств платежа.

В случае с *Webmoney* одно лицо (пользователь) предоставляет денежные средства гаранту в оплату «титульных знаков», размер которых учитывается на специальном счете без открытия банковского счета. Данные титульные знаки используются для исполнения денежных обязательств, возникающих у плательщика. Даже если назвать возникающие отношения иным образом, вроде «услуги по передаче *WMZ*-сертификата третьим лицам», их суть от этого не меняется, в чем можно убедиться, посмотрев внимательнее, что же представляет собой такой сертификат. Исходя из дефиниции, данной в соглашении с *Webmoney*, это «электронный документ учета, удостоверяющий права

[1] *Иванов И.* Виртуальные деньги теперь в законе // эж-Юрист. 2011. № 37.

Покупателей на определенный объем приобретенных ими товаров или услуг Поставщика и предоставляющий право требования на получение товаров или услуг у Поставщиков против предоставления *WMZ*-Сертификата». При этом номинал сертификата исчисляется в условных единицах, эквивалентных долларам США. Учитывая огромный массив потенциальных участников системы, где могут быть совершены соответствующие транзакции, а также открытый характер участия потенциальных поставщиков в ней, становятся очевидными его отличия от различного рода предоплаченных карт, эмитируемых предприятиями и используемых только в рамках предприятий, которые выведены из-под сферы действия Закона о НПС. Ведь в данном случае действительно нельзя говорить об электронных деньгах, так как они представляют собой предоплату по заключаемому договору купли-продажи (услуг) с данным предприятием. *Webmoney* же открыто заявляет о своей непричастности к отношениям, возникающим между продавцом и плательщиком, подчеркивая тем самым выполнение исключительно посреднической функции, связанной с погашением денежного обязательства своего клиента[1]. В терминологии новой Директивы ЕС об электронных деньгах подобные платежные инструменты являются многоцелевыми (универсальными), и на них начинают в полной мере распространяться требования Директивы. Почему же тогда подход Закона о НПС, исходящего из той же логики, что и Директива, должен быть иным? Только потому, что в соглашениях используется сочетание «титульные знаки» и делаются оговорки, что они не являются средством платежа за товары и услуги? Избегая излишней категоричности в выводах, хотелось бы отметить, что подобного рода схемы *могут* быть рассмотрены в качестве обхода закона, который ныне является одним из проявлений злоупотребления правом (ст. 10 ГК РФ)[2].

[1] Пункт 12 Соглашения с гарантом системы по *WMZ*: «Продавец (под продавцом в данном Соглашении понимается гарант. – *А.С.*) предупреждает Покупателя, что не несет ответственности за качество, порядок поставки, обмен товаров или услуг, представленных в списке на сервисе *www.megastock.com*. Покупатель признает и соглашается с этим, заявляя, что все взаимоотношения по получению товаров или услуг Покупатель будет строить непосредственно с Поставщиками товаров или услуг и не привлекать в этот процесс Продавца». http://www.webmoney.ru/rus/cooperation/legal/wmz.shtml

[2] Легальная дефиниция обхода закона отсутствует. Обход закона может рассматриваться в качестве собирательного выражения для обозначения целого ряда неправомерных действий, которыми различным способом пытаются придать видимость правомерности совершаемым действиям и имеют цель привести окольными путями к последствиям, противоречащим закону (см. подробнее: *Суворов Е.Д.* Обход закона. Сделка, оформляющая обход закона. М., 2008. С. 28–29).

Схожие соображения можно высказать и в отношении титульных знаков, номинированных в российской валюте – *WMR*. Формально их оборот основывается на соглашении об использовании чеков в электронной форме. В данном соглашении гарант *WebMoney* выступает в качестве чекодателя и «гарантирует любому лицу, законно владеющему и осуществляющему расчетные операции с использованием чеков в электронном виде на предъявителя (далее – ЭЧП), выданных чекодателем посредством специализированного программного обеспечения, оплату денежной суммы, указанной в ЭЧП, после предъявления ЭЧП к оплате в соответствии с правилами банка, который является плательщиком по ЭЧП». Обязательства чекодателя прекращаются с момента списания со счета чекодателя на основании предъявления ЭЧП денежной суммы, соответствующей ЭЧП. Как видно, *Webmoney* все же рассматривает возникающие отношения в качестве безналичных расчетов, но не особого рода, как это делает Закон о НПС, а в виде выдачи чеков на предъявителя. В литературе уже отмечалось, что возникающие отношения нельзя квалифицировать в качестве расчетов чеками, предусмотренных ГК РФ. Главным препятствием является тот факт, что чек является ценной бумагой и как таковой требует наличия определенных реквизитов, указанных в ст. 878 ГК РФ, а электронные «чеки» *Webmoney* их не содержат[1]. Как справедливо отмечается в литературе, попытки трактовки электронных денег в качестве бездокументарных ценных бумаг требуют внесения изменений в нормы о правовом режиме таких бумаг[2].

Приведенные соображения позволяют сделать вывод о том, что юридические модели, используемые системой *Webmoney*, являются как минимум спорными. Если данная платежная система не собирается уклоняться от соблюдения требований Закона о НПС, то ничто не мешает ей получить соответствующий статус и привести свои соглашения в соответствие с требованиями данного Закона, как это сделала система «Яндекс.Деньги». Если же за креативным подходом к юридической квалификации возникающих отношений скрывается нежелание подпадать под специальное регулирование Закона о НПС (подпадание под юрисдикцию Банка России; необходимость проведения идентификации клиента в соответствии с законодательством о противодействии легализации доходов, полученных преступным путем; соблюдение особого порядка привлечения платежного банковского агента; соблюдение обязанностей по организации системы

[1] *Балкаров А.* Указ. соч.

[2] *Башкатов М.* Правовая природа «электронных денег». С. 87.

управления рисками в платежной системе, наличие особого порядка распределения рисков совершения несанкционированных транзакций и пр.), то появление неподдельного интереса ЦБ РФ к юридической чистоте бизнес-модели *Webmoney* – это вопрос времени. Пример с *e-gold* показал, что регуляторы и суды вряд ли удовлетворятся схоластическими аргументами о том, что перевод денежных средств и перевод неких символов, выполняющих по существу ту же платежную функцию, является достаточным основанием, чтобы не соблюдать законодательство, применимое к платежным системам. Как гласит известная английская поговорка: «Если что-то выглядит как утка, плавает как утка и крякает как утка, то это, скорее всего, утка».

§ 6. Децентрализованная виртуальная валюта как особый вид электронных денег

Не успели регуляторы разобраться с регламентацией существующих систем электронных денег, как появились принципиально новые виды валюты, основанные на принципиально иных подходах, нежели классические системы электронных денег. Наиболее известным видом такой валюты является *Bitcoin*, который представляет собой весьма уникальное явление не только с юридической точки зрения, но и с экономической и социологической. В самом общем виде *Bitcoin* может быть обозначен как интернет-валюта нового поколения. Она анонимна, децентрализована и основана на принципах, лежащих в основе пиринговых сетей[1]. Это своего рода экономический торрент. Подобно тому как в обычных торрент-сетях отсутствует единый орган управления, валюта *Bitcoin* не имеет эмитента или иного органа, который осуществлял бы централизованный контроль над ее обращением. По существу, оборот *Bitcoin* контролируется сложным алгоритмом и действиями ее пользователей в отсутствие каких-либо посредников или надзирающих органов.

В качестве ценности, обеспечивающей данную валюту, выступают компьютерные вычисления. Единицы валюты создаются в результате деятельности, получившей название *mining*. Любое лицо, установившее специальное программное обеспечение, может «заработать», а точнее, – создать определенное количество валюты *Bitcoin* по факту решения

[1] *Bitcoin* является не единственным видом валюты в своем роде. Недавно появились и его аналоги: *Litecoin*, *Namecoin*, *PPcoin* и др., но пока их популярность и рыночная капитализация не идут ни в какое сравнение с *Bitcoin*, поэтому имеет смысл остановиться на рассмотрении именно данной валюты, принимая во внимание, что все иные *P2P*-платежные системы построены на схожих принципах.

его компьютером сложных вычислительных задач (*hashes*), связанных с верификацией транзакций, совершаемых в платежной системе *Bitcoin*. Возможна и кооперация: объединение вычислительных мощностей различных лиц в единый пул с последующим распределением «заработка». Сложность решения задачи обусловливает сложность заработка единицы *Bitcoin* и тем самым ее ценность, предотвращая возможные манипуляции с эмиссией. Алгоритмы, лежащие в основе функционирования *Bitcoin*, предопределяют наличие максимального размера единиц, находящихся в обращении: порядка 21 млн. Таким образом, данная валюта защищена от инфляции в отличие от обычных денег, которые потенциально могут быть напечатаны в неограниченном объеме. Ожидается, что последняя единица *Bitcoin* будет создана в районе 2040 г.[1] По состоянию на август 2013 г. в обороте находится около 11,5 млн единиц *Bitcoin*[2]. Общий объем только биткоинов в реальных деньгах сейчас оценивается примерно в 1,4 млрд долл.[3]

Таким образом, подобно тому, как затраты, связанные с добычей и обработкой золота, способствуют его ценности, затраты на производство соответствующих вычислений обусловливают лимитированный характер единиц *Bitcoin*. А ценность, необходимую для выполнения функции средства обмена, им сообщает готовность ряда продавцов товаров и услуг принимать их в качестве оплаты. Курс *Bitcoin* постоянно меняется. В ноябре 2012 г. 50 единиц продавались за сумму порядка 600 долл., что делало привлекательным включение в данную систему тех пользователей, которые располагают обширными вычислительными мощностями[4].

После того как единица *Bitcoin* была успешно заработана или приобретена иным образом, ее владелец имеет возможность выбора: 1) хранить ее в ожидании увеличения курса; 2) использовать в качестве оплаты за товары и услуги у продавцов, которые принимают их к оплате; 3) реализовать ее на специальной бирже, конвертировав ее тем самым в одну из существующих национальных валют. Возможен и обратный процесс: единицы *Bitcoin* можно приобрести за реальные деньги.

Как отмечалось ранее, любые электронные деньги имплицитно содержат в себе риск двойного расходования. В традиционных системах

[1] *FAQ Bitcoin*. С учетом постоянного возрастания сложности задач, которые необходимо решить, создание каждой последующей единицы *Bitcoin* требует все более мощных вычислительных ресурсов, что делает процесс их создания все более медленным.

[2] https://blockchain.info/charts/total-bitcoins

[3] Подробнее: http://www.kommersant.ru/doc/2213241

[4] *Twomey P.* Halting a Shift in the Paradigm: The Need for Bitcoin Regulation // Trinity College Law Review. 2013. No 16. P. 69.

электронных денег данная проблема решается посредством участия эмитента в каждой транзакции в целях верификации «электронной монеты». В системе *Bitcoin* данный подход невозможен в силу ее децентрализованного характера. Однако было предложено альтернативное решение – история всех совершенных транзакций с соответствующей виртуальной единицей является публично доступной: информация о каждом платеже распространяется по всей платежной системе, в результате чего транзакция фиксируется (*time-stamp*) с указанием ее времени совершения и уникального номера единицы *Bitcoin* (данные о сторонах транзакции и ее предмете не распространяются). Таким образом, можно проследить всю историю использования такой единицы с самого момента ее создания (такая история именуется *block chain*). При осуществлении платежа автоматически проводится валидация транзакционной истории соответствующей виртуальной единицы, и в отсутствие каких-либо установленных противоречий платеж принимается и не может быть оспорен или отменен. Валидация платежа требует значительных вычислительных мощностей. В отсутствие централизованного органа управления системой остается единственный вариант, чтобы пользователи предоставляли собственные компьютерные ресурсы для осуществления таких вычислений. Упоминавшийся ранее *mining* является тем самым еще и стимулом для пользователей выделять такие ресурсы. При этом данные о платеже посредством специальных математических алгоритмов используются для формирования математических задач для целей *mining*[1].

Сам платеж осуществляется путем указания владельцем единицы *Bitcoin* нового публичного адреса на ней и ее подписания свои частным ключом. Анонимность транзакций обеспечивается тем, что публичными становятся лишь данные о транзакции, без какой-либо привязки к личности ее участников. С технической точки зрения единицы *Bitcoin* представляют собой компьютерные файлы, подобные *mp3* или текстовым файлам, в силу чего их пересылка в сети Интернет является достаточно простым делом[2]. Данные файлы содержат уникальный номер, созданный с применением технологий шифрования. Виртуальные единицы хранятся в виртуальном кошельке, расположенном либо на компьютере пользователя, либо на удаленном сервере. Утрата кошелька по различным причинам (потеря компьютера, неисправность жесткого диска) влечет утрату виртуальных единиц, сохранен-

[1] *Satoshi Nakamoto*. Bitcoin: A Peer-to-Peer Electronic Cash System. P. 3 // www.bitcoin.org

[2] *Kaplanov N.* Nerdy Money: Bitcoin, The Private Digital Currency and The Case against its Regulation // Loyola Consumer Law Review 2013. No 25. P. 116.

ных на нем. Более того, такие единицы выпадают из оборота в целом, сокращая тем самым общий объем циркулирующей денежной массы.

Децентрализованный и анонимный характер платежной системы *Bitcoin* вызывает немало опасений со стороны регуляторов. Подобно тому, как правообладатели видят в торрентах преимущественно (а то и исключительно) средство для распространения контрафактной продукции, финансовые регуляторы и правоохранительные органы рассматривают *Bitcoin* в основном как средство платежа за совершение незаконных действий. Действительно, посредством данной виртуальной валюты осуществляются платежи на черных рынках Интернета, существующих в особом его сегменте, который недоступен при использовании традиционных программных средств и ресурсы которого не индексируются поисковыми системами[1]. Одним из таких рынков является *Silk Road* («*шелковый путь*»), где осуществляется торговля наркотиками различных видов и иными объектами, изъятыми из оборота[2]. Другим направлением использования биткоинов является финансирование различного рода организаций, в том числе преступного характера.

Как следствие регуляторы[3] и правоохранительных органы[4] выражают свою озабоченность применением *Bitcoin*. Некоторые из них пошли дальше и решились на радикальные меры. Как сообщается, в Таиланде использование *Bitcoin* запрещено. В частности, запрещены покупка и продажа данной валюты, использование ее для приобретения товаров и услуг, ее отправка за пределы Таиланда и получение ее от иностран-

[1] Для доступа к такому сегменту используется специальное программное обеспечение вроде *TOR* (*The Onion Router*), которое дает практически абсолютную анонимность пребывания в сети Интернет в отсутствие возможности отслеживания действий пользователя третьими лицами за счет постоянного изменения *IP*-адреса компьютера. *TOR* позволяет исследовать просторы *Deepnet* и посещать *.onion*-сайты, которые хостят исключительно анонимных пользователей.

[2] *Ryan Broderick*, Traveling Down the Silk Road to Buy Drugs With Bitcoins, Motherboard (June 24, 2011) // http://www.motherboard.tv/2011/6/24/traveling-down-the-silkroad-to-buy-drugs-with-bitcoins. Правда, в октябре 2013 г. Росс Ульям Ульбрихт был арестован, а сам ресурс прекратил свою работу. Однако представляется, что появление иного подобного рынка является лишь вопросом времени, подобно тому, как в свое время прекращение судом деятельности первой *P2P*-сети *Napster* повлекло появление множества иных подобных сетей с более продвинутыми алгоритмами, еще более затрудняющими возможность контроля над ними.

[3] Virtual Currency Schemes. European Central Bank Report. October 2012 // http://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf

[4] Bitcoin Virtual Currency: Intelligence Unique Features Present Distinct Challenges for Deterring Illicit Activity. FBI Report // http://www.wired.com/imagesblogs/threatlevel/2012/05/Bitcoin-FBI.pdf

ного отправителя. Данное решение мотивировано руководителями Департамента валютного регулирования Таиланда и Центрального банка отсутствием необходимого законодательства для обеспечения ее регулирования, невозможностью контроля движения средств внутри системы, а также фактами мошенничества[1].

Представляется, что власти Таиланда пошли по неправильному пути. Урегулировать правом децентрализованные валюты, подобные *Bitcoin*, в принципе невозможно. Правила эмиссии новых денег строго определены и никем не могут быть изменены. Все проводки основаны на целом комплексе алгоритмов, полностью открытых и находящихся в свободном доступе. Эти алгоритмы согласованно взаимодействуют друг с другом через пиринговые сети на разных компьютерах по всему миру и по сути живут собственной жизнью. Таким образом, если кто-то захочет внести изменения в эти алгоритмы или правила эмиссии посредством издания каких-либо правовых норм, эти изменения просто не будут приняты внутри сети и функционированию криптовалюты это никак не повредит. К тому же очевидно, что правовой запрет на расчеты биткоинами по причине того, что они используются для незаконной деятельности, вряд ли остановит тех, кто уже использует их: если данные лица уже преступили ряд законов, то ничто не препятствует им нарушить еще один.

Другим примером предпринимаемых попыток взятия под контроль валюты *Bitcoin* является направление 30 мая 2013 г. Департаментом финансовых институтов Калифорнии в адрес фонда *Bitcoin Foundation* требования о прекращении противоправной деятельности (*cease and desist letter*)[2]. В обоснование данного требования Департамент ссылался на то, что деятельность фонда представляет собой перевод денежных средств (*money transmitting*), требующий наличия лицензии, которой у фонда, естественно, не было. Ответ фонда не заставил себя долго ждать. В письме от 1 июля 2013 г.[3] указывается, что фонд является некоммерческой организацией, деятельность которой направлена на защиту целостности протоколов *Bitcoin*, развитие инфраструктуры данной валюты и иные некоммерческие цели. Далее обосновывается, что деятельность фонда не подпадает ни под одно из понятий *money transmitting*. Фонд не продает биткоины потребителям и не обменивает

[1] www.banki.ru/news/lenta/?id=5255132

[2] С текстом данного письма можно ознакомиться по ссылке: http://www.coindesk.com/california-issues-cease-and-desist-letter-to-bitcoin-foundation/

[3] С текстом данного письма можно ознакомится по ссылке: http://www.coindesk.com/bitcoin-foundation-issues-response-to-cease-and-desist-warning/

их на иную валюту; биткоины не подпадают под понятие финансового инструмента, поскольку последнее требует по законодательству штата Калифорния письменной формы. К тому же биткоины не воплощают в себе денежную стоимость, так как их цена определяется исключительно рыночными соображениями и ни одно лицо (в том числе и фонд) не обязано выкупать их по номиналу. Несмотря на то что все в итоге закончилось мирным образом, ход финансового регулятора вызвал немалый интерес общественности, поскольку подобного рода интерес к валюте *Bitcoin*, с одной стороны, свидетельствует о росте ее значения, которое более нельзя не замечать, а с другой – представляет собой своего рода «разведку боем» и сигнал компаниям, которые используют подобного рода валюту, что они не пребывают в правовом вакууме.

Отсутствие эмитента, которого можно было бы привлечь к ответственности, анонимный характер использования валюты и связанные с этим трудности по привлечению к ответственности пользователей, а также невозможность изменения технической стороны их функционирования – все это обусловливает значительные сложности для осуществления регулирования процессов, возникающих в связи с использованием децентрализованной виртуальной валюты вроде *Bitcoin*. Однако это не означает, что они являются абсолютно неуязвимыми для правового регулирования. Есть как минимум одна точка соприкосновения виртуального мира с реальным, где право вполне успешно может осуществлять свое регулирующее воздействие: виртуальные биржи, где происходит конвертация биткоинов в национальные валюты и обратно[1]. Конвертировать биткоины можно и через известный виртуальный мир *Second Life*, обменяв их на внутреннюю виртуальную валюту *Linden Dollars*, которая в свою очередь может быть реализована за традиционные деньги. Как отмечалось ранее, *Webmoney* также осуществляет расчеты в биткоинах. Лица имеют присутствие в реальном мире, активы и бизнес, который они хотят сохранить, в связи с этим они вполне могут быть объектом предписаний, касающихся контроля над сомнительными сделками и иных положений, традиционно применимых к финансовым учреждениям.

Конечно, сохраняется возможность обмена биткоинов на реальные деньги и минуя виртуальные биржи, например, путем совершения обменов между частными лицами[2]. Даже несмотря на то что многие продвинутые пользователи и хакеры смогут обойти установленные запреты

[1] Наиболее известными биржами является *Mt. Gox, Camp BX, TradeHill*.

[2] Существуют специальные сайты, которые помогают таким лицам найти друг друга, например *Bitcoin.local*.

и ограничения, такое регулирование будет все же охватывать большой пласт отношений, возникающих при использовании биткоинов в качестве средства платежа. В конце концов, регулирование не должно быть идеальным для того, чтобы быть эффективным. Достаточно того, чтобы оно устанавливало издержки, связанные с несоблюдением правовых предписаний, на уровне, превышающем возможную выгоду от такого несоблюдения. Большинство пользователей, использующих биткоины в качестве средства платежа по законным сделкам, предпочтут эффективный и прозрачный способ конвертации биткоинов в реальные деньги, подчиняясь тем самым регулированию, установленному в отношении виртуальных бирж. А хакеры и криминальные элементы и так не являются «клиентами» законодательных предписаний.

Bitcoin уникален не только с технической, экономической, но и с юридической точки зрения. Здесь отсутствуют какие-либо договорные отношения с оператором (эмитентом) электронных денег по причине отсутствия оного. Никто не может наложить арест, приостановить операции по счету, отменить платеж, что придает совершаемым сделкам дополнительную безопасность. Необратимость совершенных платежей является одним из важнейших преимуществ системы *Bitcoin*[1].

Очевидно, что биткоины не могут быть квалифицированы ни как деньги, ни как иные вещи, ни даже как имущественное право требования. Единственная категория, содержащаяся в ст. 128 ГК РФ, позволяющая хоть как-то охватить данное явление, – это «иное имущество». Биткоины, как было продемонстрировано выше, обладают вполне определенной экономической ценностью и могут быть обменены на валюту многих стран мира. Так что нет никаких оснований для исключения их из-под действия гражданского права. Равным образом договоры, предусматривающие продажу товаров и услуг за биткоины, должны признаваться действительными (разумеется, при условии, что их предметом не являются объекты, изъятые из оборота). Поскольку биткоины не могут быть рассмотрены как деньги, такие договоры имеют бартерную природу. Правда, такой договор нельзя будет рассматривать по российскому праву как договор мены, поскольку квалифицирующим признаком последнего является обмен одного товара на другой, что обусловливает необходимость наличия перехода права собственности по такому договору[2]. Представляется, что такой договор является смешанным

[1] *Kaplanov N.* Op. cit. P. 125.

[2] Так, ВАС РФ не квалифицирует в качестве мены договор, по которому осуществляется обмен товара на услуги или на имущественное право. См.: п. 1 и 3 информационного письма Президиума ВАС РФ от 24 сентября 2002 г. № 69 «Обзор практики

с элементами соответствующего договора, опосредующего предоставление товара, работы или услуги, а также элемента непоименованного договора, опосредующего передачу биткоинов в качестве оплаты[1].

Значение виртуальной валюты *Bitcoin* не стоит недооценивать. Децентрализованные виртуальные валюты несут в себе ряд преимуществ, недоступных традиционным платежным средствам: 1) существенное сокращение транзакционных издержек за счет отсутствия эмитента и иных посредников в проведении платежа; 2) уверенность в том, что после прохождения процедуры верификации платеж является окончательным и не будет отменен; 3) анонимность, которая может быть востребована не только криминальными элементами, но и лицами, опасающимися преследований со стороны определенных государств (вроде *WikiLeaks*).

Подобно тому, как торренты в свое время существенным образом изменили рынок объектов авторского права, разрушив многие успешные и казавшиеся непреложными бизнес-модели правообладателей, так и виртуальная валюта, построенная на тех же принципах, что и торрент-системы, может поколебать многие платежные средства. Даже если *Bitcoin* и прекратит свое существование со временем, на смену ему придут более совершенные системы, построенные на тех же принципах, подобно тому, как это было с *Napster*[2].

§ 7. Правовая природа электронных денег

Рассмотрев технические аспекты функционирования электронных денег, а также существующую нормативно-правовую базу, можно теперь поставить перед собой более фундаментальные вопросы: являются ли электронные деньги деньгами в собственном смысле этого слова? Какова их природа? Являются ли электронные деньги законным средством платежа?

Конечно, анализ электронных денег на предмет возможности их отнесения к деньгам в экономическом смысле хотя и представляет

разрешения споров, связанных с договором мены», рассматривая такие договоры в качестве смешанных.

[1] Подробнее о непоименованных договорах и смешанных договорах с элементами непоименованного см.: *Карапетов А.Г., Савельев А.И.* Свобода заключения непоименованных договоров и ее пределы // Вестник ВАС. 2012. № 4.

[2] Несмотря на все усилия американских властей по закрытию *Napster*, вскоре появилась более совершенная система: *KaZaa* и др. *Eric Johnson*, et al., The Evolution of the Peer-to-Peer File Sharing Industry and the Security Risks for Users // Hawaii International Conference on SYs. Science. No 41. 2008. Известный пиратский торрент-трекер *Pirate Bay* успешно существует более пяти лет, несмотря на многочисленные попытки его закрытия.

собой немалый интерес, но вряд ли возможен в рамках данной работы. Да и сами экономисты не рассматривают анализ теории денег в качестве хорошего занятия. Еще в начале XX в. было высказано мнение, что «лучший способ в кратчайший срок сойти с ума — это заняться вопросами денежной теории»[1]. Но определенные моменты упомянуть определенно стоит.

Во-первых, в экономической теории до сих пор нет единой теории, объясняющей суть денег.

В современной экономической науке сущность денег нередко выводится непосредственно из их функций[2]. Иными словами, «деньги – это то, что они делают».

Многие экономисты выделяют три основные функции денег[3]:

1) мера стоимости. Наличие счетной денежной единицы является необходимым для установления основных условий осуществления экономической деятельности (прейскурантов цен и долгосрочных контрактов). Деньги являются товаром, но прежде чем им стать, они должны быть введены в оборот согласно абстрактной счетной денежной единице;

2) средство платежа. Усложнение оборота и распространение консенсуальных договоров повлекло несовпадение во времени моментов покупок и продаж, что порождает функцию денег как средства платежа, которую они выполняют в момент погашения долга[4];

3) средство сохранения стоимости. Деньги выступают тем активом, который можно хранить и использовать в качестве инструмента накопления богатства (тезаврации).

Иногда выделяются и другие функции (например, функции мировых денег, средства обращения, масштаба цен, средства сбережения, средства накопления), но так или иначе такие дополнительные функции могут быть рассмотрены в качестве производных от вышеуказанных трех, да и для целей рассмотрения нашего вопроса их выделение никак не помогает.

---

[1] *Туган-Барановский М.И.* Бумажные деньги металл. Одесса, 1919. С. 1. В труде «К критике политической экономии» главу, в которой исследуются деньги, Маркс предваряет словами о том, «что даже любовь не сделала стольких людей дураками, сколько мудрствование по поводу сущности денег». *Маркс К.* К критике политической экономии. М., 1984. С. 51.

[2] *Ефимова Л.Г.* Банковские сделки: право и практика. М., 2001. С. 196.

[3] *Самуэлсон П.* Экономика. М., 1992. Т. 1. С. 258; *Долан Э.Дж.*, *Кэмпбелл К.Д.*, *Кэмпбелл Р.Дж.* Деньги. Банковское дело и денежно-кредитная политика. М., 1991. С. 30–34; *Friedman D.*, *Macintosh K.* The Cash of the Twenty-First Century // Computer & High Technology Law Journal. No 17. 2001. P. 274.

[4] *Новоселова Л.А.* Проценты по денежным обязательствам. 2-е изд., испр. и доп. М., 2003. С. 4.

Исходя из функционального подхода к пониманию денег в качестве таковых может использоваться все, что признается людьми за деньги и выполняет их функции. Достаточно красочно эту идею выражает Фридрих фон Хайек: «...расхожее представление, будто существует четкая разграничительная линия между деньгами и не-деньгами – а закон обычно пытается провести такое разграничение – на самом деле неверно... Мы обнаруживаем здесь скорее некий континуум, в котором объекты с разной степенью ликвидности и с разной (колеблющейся независимо друг от друга) ценностью постепенно переходят друг в друга постольку, поскольку они функционируют как деньги. Тезис о существовании одной, четко определенной вещи, именуемой «деньгами», которую можно легко отличить от других вещей, является юридической фикцией. Эта фикция, введенная для удовлетворения нужд адвоката или судьи, никогда не была истинной, поскольку явления, остающиеся за ее рамками, вполне могут вызывать последствия типично «денежного» характера»[1]. Л.А. Лунц также упоминал частные деньги в качестве особого вида денег: «Наряду с различными видами государственных денег гражданский оборот выдвигает свои собственные средства обмена, о денежной функции которых умалчивает закон. В действующем советском праве, а также в экономических исследованиях эти негосударственные деньги носят название денежных суррогатов. С юридической точки зрения этот термин представляется неточным, так как если употребление этих «денежных суррогатов» приобрело всеобщее значение и не запрещено законом, то они должны рассматриваться как настоящие деньги в юридическом смысле этого слова: платеж ими есть настоящее исполнение обязательства, а не замена исполнения. Поэтому с правовой точки зрения было бы правильнее говорить о негосударственных или частных деньгах»[2].

В зарубежном праве встречается достаточно гибкий подход к дефиниции денег. Так, в знаменитом деле *Moss v. Hancock*[3] был высказан подход, согласно которому под деньгами понимается «все, что свободно переходит из рук в руки в рамках определенного сообщества в качестве средства погашения долга... при этом будучи принимаемым в равной степени вне зависимости от характера и платежеспособности плательщика и без намерения получателя их потребить».

Электронные деньги вполне могут быть рассмотрены в качестве разновидности тех самых «частных денег», о которых говорили

[1] *Хайек Ф.* Частные деньги. М., 1996. С. 96–98.
[2] *Лунц Л.А.* Деньги и денежные обязательства в гражданском праве. М., 2004. С. 64.
[3] [1899], 2 QB 111.

Ф. Хайек и Л.А. Лунц. Правда, учитывая существующие ограничения на выплату процентов на средства, внесенные в качестве «платы» за электронные деньги, а также ограничения на максимальный размер электронных кошельков, электронные деньги, циркулирующие в России и Европейском союзе, не могут выполнять функцию тезаврации. А запреты, установленные на использование электроннных денег в расчетах между юридическими лицами и индивидуальными предпринимателями, существенно ограничивают функцию электронных денег в качестве средства платежа. Все это делает их на данном этапе «неполноценными» деньгами. Однако установленные ограничения не являются имманентными природе электронных денег, а являются следствием попыток регуляторов сохранить существующий *status quo*, найти какую-либо нишу для применения электронных денег, ограничив конкуренцию электронных денег с традиционными средствами платежа, которые уже выступают предметом эффективного контроля со стороны регуляторов.

В качестве денег в полном смысле этого слова вполне могут рассматриваться электронные деньги, функционирующие в рамках открыто циркулирующих систем. И хотя в настоящее время их достаточно мало, можно предположить их распространение в будущем, учитывая устойчивую тенденцию к дематериализации денег. В частности, Центральный банк Сингапура планирует перейти к выпуску электронных денег, выступающих в качестве законного средства платежа наряду с традиционными наличными деньгами[1]. Так что электронные деньги вполне могут рассматриваться в качестве денег в экономическом смысле этого слова при условии, что в отношении них не будут действовать те искусственные законодательные ограничения, которые препятствуют выполнению ими функций денег. Виртуальная валюта *Bitcoin* вполне может рассматриваться в качестве разновидности «частных» денег уже в настоящее время, поскольку выполняет все основные функции денег: существующие законодательные ограничения не «дотягиваются» до данной валюты, по крайней мере в настоящее время.

Квалификация явления с юридической точки зрения может существенно отличаться от его экономического понимания. Например, понятие товара в экономическом смысле включает в себя любое благо, которое может быть реализовано за деньги. Юридическое значение товара существенно у́же и охватывает только вещи (п. 1 ст. 455 ГК РФ),

[1] *Van Hove L.* Making electronic money legal tender: pros & cons. Paper prepared for «Economics for the Future» – Celebrating 100 years of Cambridge Economics, University of Cambridge. September 17–19, 2003. P. 5–6.

работы и услуги являются самостоятельными объектами гражданских прав с отдельным правовым режимом.

Различия между экономическим и юридическим пониманием определенного явления породили множество различных интерпретаций электронных денег, предложенных в юридической литературе, в числе которых можно выделить следующие трактовки понятия электронных денег:

• юридически значимые информационно-цифровые импульсы или же определенная последовательность цифр, символизирующих (заменяющих) банкноты и монеты[1];

• разновидность ценных бумаг на предъявителя[2];

• особый инструмент, средство распоряжения правом требования выплаты денежных средств[3];

• согласованный сторонами иной способ исполнения денежного обязательства[4].

Закон о НПС внес определенность в вопрос о правовой природе электронных денег. Платежи электронными деньгами рассматриваются как форма безналичных расчетов, а сами электронные деньги выступают в качестве имущественного права требования их обладателя к оператору о выдаче определенного количества наличных или безналичных денежных средств. При этом в отсутствие явного указания на то, что такое право оформляется ценной бумагой, электронные деньги нельзя рассматривать в качестве ценных бумаг на предъявителя с юридической точки зрения.

Являются ли электронные деньги при этом законным платежным средством? Как известно, правовое значение законной платежной силы, присвоенной денежному знаку, заключается в том, что кредитор по обязательству, могущему быть погашенным путем денежного платежа, отказавшись принять законное платежное средство, впадает в просрочку[5].

В соответствии со ст. 29 Федерального закона от 10 июня 2002 г. № 86-ФЗ «О Центральном банке Российской Федерации (Банке России)» (далее – Закон о Банке России) банкноты и монеты Банка России яв-

---

[1] *Тедеев А.А.* Электронная коммерция. М., 2002. С. 136–137.

[2] В качестве особой формы бездокументарного векселя интерпретирует электронные деньги В.Н. Назаров: *Назаров В.Н.* Деньги как категория финансового права // Финансовое право. 2009. № 7. Ранее уже отмечалось, что данной точки зрения и поныне придерживается система *Webmoney*, рассматривая оборот титульных знаков, номинированных в рублях, в качестве расчетов чеками в электронной форме.

[3] *Башкатов М.* Правовая природа «электронных денег». С. 90.

[4] *Калятин В.О.* Право в сфере Интернета. С. 380.

[5] *Лунц Л.А.* Деньги и денежные обязательства в гражданском праве. С. 50–52.

ляются единственным законным средством наличного платежа на территории Российской Федерации. В ст. 140 ГК РФ законное средство платежа определено несколько иначе: таковым является рубль, т.е. денежная единица Российской Федерации.

В связи с этим как отмечает М. Башкатов, нет единообразного понимания того, что же такое законное средство платежа. Согласно одной точке зрения законным платежным средством является именно рубль, а не денежные знаки, эмитируемые ЦБ РФ. Другая точка зрения исходит из того, что законной платежной силой по гражданскому законодательству обладают только монеты и банкноты Банка России[1].

Сторонники первой точки зрения распространяют статус законного платежного средства и на безналичные денежные средства, выраженные в рублях[2]. Сторонники второй, более консервативной точки зрения отдают приоритет положениям Закона о Банке России, признавая законным платежным средством лишь наличные деньги: монеты и банкноты, эмитированные ЦБ РФ.

Сторонники признания законным средством платежа исключительно наличные деньги приводят множество доводов, главным образом догматического порядка, которые, по их мнению, препятствуют признанию безналичных средств законным средством платежа. Здесь не хотелось бы их все приводить, тем более что они весьма подробно и системно уже изложены в существующих работах по данной тематике[3]. Хотелось бы отметить, что вряд ли правильно увязывать статус законного платежного средства с вещной или обязательственно-правовой природой того блага, которому предполагается его предоставить. А именно в таком увязывании и состоит основная линия аргументации и ошибка тех, кто рассматривает лишь наличные деньги в качестве законного платежного средства. Если основным значением законного платежного средства является невозможность отказа кредитора в его принятии без впадения в просрочку с освобождением должника от возможных мер ответственности за просрочку, то именно наличие или отсутствие данных последствий и должно приниматься во внимание при анализе природы безналичных денежных средств. Как известно, расчеты между юридическими лицами должны по общему правилу совершаться в безналичном порядке (п. 2 ст. 861 ГК РФ). Юридическое лицо, выступающее кредитором по денежному обязательству, не может

[1] См. подробнее: *Башкатов М.Л.* Догматическая конструкция законного средства платежа // Вестник гражданского права. 2006. № 2.

[2] См., например: *Ефимова Л.Г.* Указ. соч. С. 214–218.

[3] *Башкатов М.Л.* Догматическая конструкция законного средства платежа.

отказать в зачислении безналичных денежных средств на том основании, что ему не нравится банк, из которого они пришли. Более того, он не может потребовать от своего контрагента – юридического лица выплаты суммы задолженности наличными средствами[1], хотя многие российские предприниматели весьма бы этого хотели. Иными словами, у кредитора в таких случаях нет выбора и его согласия на то в договоре не требуется. Чем не законное средство платежа?

Как видно, погашение денежного долга безналичными денежными средствами в ряде случаев признается законом надлежащим[2]. Недаром Закон о Банке России говорит именно о законном платежном средстве *наличного* платежа, подразумевая тем самым возможность существования законного наличного средства *безналичного* платежа. Конечно, можно говорить о термине «законное платежное средство наличного платежа» как о технической оплошности законодателя, но вряд ли можно игнорировать тот факт, что объем использования наличных денег в обороте постепенно снижается, будучи вытесненным безналичными платежами[3], трактовка которых в качестве «незаконного средства платежа» вряд ли будет соответствовать здравому смыслу. К тому же налоги согласно НК РФ могут быть уплачены безналичными денежными средствами, что лишний раз подтверждает их законный характер. А ведь, как известно, «налоги делают деньги деньгами»[4].

Почему так много внимания уделяется рассмотрению правовой природы безналичных денежных средств и возможности их квалификации в качестве законного средства платежа? Потому что, как справедливо указывает М. Башкатов, электронные деньги могут рассматриваться как фикция безналичных денег, поскольку право требования к эмитенту электронных денег очень близко по своей сути к праву требования клиента к банку[5]. Если признать безналичные денежные

---

[1] За исключением случаев, подпадающих под допустимые лимиты расчетов наличными юридических лиц между собой или с индивидуальными предпринимателями. В настоящее время он составляет 100 000 руб.

[2] Есть все основания полагать, что сфера применения безналичных денег будет со временем только расти. Уже разработаны законопроекты, которые предусматривают введение максимального размера суммы сделки, она может быть оплачена наличными, и которые будут распространяться в том числе и на отношения с гражданами. См.: Минфин ограничит наличный расчет. Интерфакс. 11 октября 2013 г. // http://www.interfax.ru/finances/txt.asp?id=334072

[3] Согласно данным ЦБ РФ доля наличных денег (агрегат М0) составляет порядка 25% всей денежной массы (агрегат М2) // http://cbr.ru/statistics/credit_statistics/MS.asp

[4] *Wray R.* Modern Money Theory: A Primer on Macroeconomics for Sovereign Monetary Systems. Palgrave Macmillan. 2012. P. 49.

[5] *Башкатов М.* Правовая природа «электронных денег». С. 90.

средства в качестве законного платежного средства безналичного платежа, то возникает соблазн сделать то же самое и в отношении платежей электронными деньгами, выступающими одной из форм безналичных платежей.

Некоторые авторы уже приходят к выводам о возможности признания электронных денег законным платежным средством. Как отмечает М.В. Шевчук, электронные деньги можно рассматривать в качестве законного платежного средства между участниками платежной системы, при этом такие электронные деньги будут выступать законным платежным средством безналичного платежа[1]. Представляется, что все же данный вывод является несколько преждевременным.

Ключевым признаком законного платежного средства является возможность погашения им своего денежного обязательства без предварительного согласования его использования с кредитором. Если кредитор не участвует в системе *Webmoney*, его нельзя обязать принять в качестве платежа титульные знаки, обращающиеся в этой системе. А если кредитор выразил согласие на использование таких денежных средств, тогда это не что иное, как согласованный сторонами способ исполнения обязательства. Платежи электронными деньгами возможны на данном этапе их развития только в той мере, в какой участники основного правоотношения выразили свое согласие на их использование.

Тем более сложно признать электронные деньги законным платежным средством, пусть и ограниченной сферы действия, в условиях существующих ограничений по их использованию. В условиях когда на и без того ограниченную сферу их применения накладываются дополнительно ограничения по характеру их использования, сложно говорить о повышенной хозяйственной обращаемости, имманентной законному средству платежа.

Таким образом, на данном этапе развития и регулирования электронных денег в России признать их законным средством безналичного платежа нельзя. Их использование является сугубо добровольным и сопряжено с рядом значительных ограничений. Однако потенциально не исключена возможность придания электронным деньгам такого статуса, о чем свидетельствует практика некоторых зарубежных стран. Но для этого должны «созреть» инфраструктура, участники оборота и регуляторы, а также окончательно «отцвести» наличный денежный оборот, что уже не за горами, учитывая как быстро в последнее время происходит «оцифровка» различных аспектов личной и общественной жизни.

---

[1] *Шевчук М.В.* Правовая природа электронных денежных средств // Юрист. 2012. № 12.

Глава 8. Реклама в сети Интернет

Для успешного функционирования проекта в сфере электронной коммерции недостаточно просто разместить веб-сайт в сети Интернет, даже если такое размещение будет осуществлено под очень узнаваемым и запоминающимся доменным именем. Как отмечалось ранее, в условиях многообразия различного рода интернет-ресурсов и контента внимание пользователей приобретает статус ценного ресурса ввиду его ограниченности. Борьба за пользовательское внимание, а следовательно, и потенциальных клиентов осуществляется посредством осуществления рекламных акций, создания сообществ потребителей и иными средствами интернет-маркетинга.

Под интернет-маркетингом понимается совокупность методов электронной коммерции, направленных на увеличение экономической эффективности сайтов, включающих в себя: 1) интернет-рекламу; 2) методы удержания посетителей на сайте (оригинальный дизайн и удобная навигация сайта, подписка на новости и пр.); 3) методы создания постоянной аудитории сайта и (или) сетевого сообщества (так называемого комьюнити)[1].

В данной главе нас будут интересовать главным образом правовые аспекты интернет-рекламы, которую в зависимости от задействованных «носителей» рекламы можно условно разделить на три основных категории: 1) контекстная (поисковая) реклама, где в качестве носителя выступает поисковая система; 2) баннерная реклама, где таким носителем является веб-сайт и 3) *e-mail*-реклама, в которой носителем выступает сообщение электронной почты.

По сравнению с традиционной рекламой можно выделить следующие отличительные особенности интернет-рекламы:

1) высокая степень автоматизации размещения и анализа эффективности проведенных рекламных мероприятий, обеспечиваемая современными программными средствами, позволяющая оперативно перепланировать рекламную кампанию в зависимости от ее результатов;

---

[1] *Юрасов А.В.* Указ. соч. С. 279.

2) интерактивность – двусторонний характер связи между потребителем рекламы и рекламодателем, обеспечивающий возможность получения в режиме реального времени информации о действиях потребителей рекламы и их отношении к ней, в том числе путем организации опросов[1];

3) существенно более низкие затраты на производство и изменение содержимого такой рекламы. Создание нового видеоролика для телевидения или печать рекламного буклета требует гораздо больше времени и средств, нежели создание баннера, его размещение и последующее изменение;

4) возможность осуществления целенаправленного воздействия на целевую аудиторию (*targeting*) путем размещения рекламы на специализированных ресурсах, с учетом текущего местонахождения пользователя и его индивидуальных потребностей, определяемых его историей покупок, запросов в поисковых системах. Среднестатистический пользователь сети Интернет оставляет немало следов. Если он не применяет специальных средств, то серверам, которые он посещает, доступна информация о его *IP*-адресе. По *IP*-адресу можно установить регион (страну, город), из которого пользователь вошел в сеть, и название провайдера, услугами которого он пользуется. Кроме того, серверы, которые посещает пользователь, способны получать и накапливать информацию о том, каким браузером пользуется клиент, с какого сайта он заходит и ряд других параметров. Помимо *IP*-адреса сервера для идентификации клиента используются так называемые *cookies*. При посещении сайта пользователем или при совершении пользователем определенных действий, например регистрации, сервер сохраняет на компьютере пользователя особую идентификационную информацию. После этого, даже если при входе клиента в сеть его компьютеру будет присвоен другой *IP*-адрес, сервер опознает клиента (точнее, его компьютер);

5) существование особых бизнес-моделей размещения рекламы в сети Интернет, предопределенных ее архитектурными и техническими особенностями, например, размещение рекламы в поисковых системах, посредством баннерообменных сетей и пр. Учитывая особое значение поисковых систем в нахождении пользователем интересующего товара или услуги, анонсирование веб-сайта в таких системах и поисковая оптимизация (так называемая раскрутка веб-сайта) являются одними из первоочередных задач владельца интернет-магазина[2].

---

[1] *Кузнецов Р.В.* Маркетинговые исследования баннерной интернет-рекламы: дис. ... канд. экон. наук. М., 2008. С. 15–16.

[2] Это особенно справедливо в свете существующих исследований, согласно которым около 60% пользователей ограничиваются лишь первой страницей, выдаваемой

§ 1. Информация, размещенная на веб-сайте, и законодательство Российской Федерации о рекламе

Прежде чем перейти к рассмотрению отдельных моделей размещения рекламы в сети Интернет, необходимо рассмотреть вопрос о том, насколько информация, размещенная на веб-сайте (корпоративном сайте, интернет-магазине и т.п.), потенциально подпадает под понятие рекламы в российском законодательстве и чем грозит положительный ответ на этот вопрос.

Основным и единственным нормативным актом в данной сфере является Закон о рекламе. Субъекты РФ не вправе принимать нормативные правовые акты по вопросам регулирования рекламы, в том числе в сети Интернет (ст. 4). Данный Закон применяется к отношениям в сфере рекламы независимо от места ее производства, если распространение рекламы осуществляется на территории Российской Федерации. Учитывая специфику сети Интернет, а также признание Рунета в качестве «виртуальной территории Российской Федерации», ФАС России полагает, что под рекламой, распространенной в информационно-телекоммуникационной сети Интернет, подпадающей под действие российского законодательства, понимается реклама, размещенная на интернет-сайтах, зарегистрированных в доменных зонах *.su*, *.ru* и .рф, а также на русскоязычных страницах сайтов в иных зонах, поскольку информация на данных страницах предназначена для потребителей в России[1].

В соответствии со ст. 3 Закона о рекламе под рекламой понимается информация, распространенная любым способом, в любой форме и с использованием любых средств, адресованная неопределенному кругу лиц и направленная на привлечение внимания к объекту рекламирования, формирование или поддержание интереса к нему и его продвижение на рынке.

поисковой системой, состоящей из 10–20 ссылок. Очевидно, что задачей владельца веб-ресурса является попадание в данный список, что обеспечивается путем увеличения релевантности его сайта путем указания правильных слов в семантическом ядре сайта (совокупности ключевых слов, сопутствующих словосочетаний, отобранных на основе анализа используемых целевой аудиторией запросов в поисковых системах), а также путем увеличения индекса цитирования сайта (показатель известности веб-сайта, определяемый количеством ссылок на него, сделанных на других веб-сайтах) посредством регистрации в специальных каталогах, участия в партнерских программах и обмена ссылками. Одним из способов повышения индекса цитируемости является разрешение копирования ценного контента на условиях обязательной ссылки на первоначальный ресурс.

[1] Письмо ФАС России от 3 августа 2012 г. № АК/24981 «О рекламе алкогольной продукции в Интернете и печатных СМИ».

Из данного достаточно широко сформулированного определения следует, что для признания информации рекламой она должна одновременно удовлетворять нескольким условиям, а именно:

– быть распространенной любым способом, в любой форме;

– быть адресованной неопределенному кругу лиц;

– быть направленной на привлечение внимания к объекту рекламирования, формирование или поддержание интереса к нему и его продвижение на рынке.

Наличие первого условия применительно к информации, размещаемой на веб-сайтах, достаточно очевидно, особенно учитывая наличие специальных положений ст. 18 Закона о рекламе, посвященных особенностям распространения рекламы по сетям электросвязи[1].

Под неопределенным кругом лиц понимаются те лица, которые не могут быть заранее определены в качестве получателя рекламной информации и конкретной стороны правоотношения, возникающего по поводу реализации объекта рекламирования[2]. ФАС России интерпретирует предназначенность ее для неопределенного круга лиц как отсутствие в рекламе указания на некое лицо, для которого реклама создана и на восприятие которого направлена[3]. В связи с этим возникает вопрос, насколько устанавливаемые владельцем веб-ресурса ограничения по доступу к соответствующей информации способны вывести ее из-под действия законодательства о рекламе. Очевидно, что наличие на веб-сайте регистрации, которую может пройти *любой желающий*, никоим образом не означает для целей применения положений о рекламе, что контент такого сайте рассчитан лишь на определенный круг лиц – зарегистрированных пользователей. Другое дело, если такая регистрация доступна лишь лицам, обладающим определенным статусом (например, бизнес-партнерам компании), и соответствующая информация доступна только таким зарегистрированным пользователям[4]. В таком случае вполне можно говорить о том, что получатель такой информации является заранее определенным лицом и ее рас-

[1] Сеть Интернет относится к средствам электросвязи. См.: п. 2 письма ФАС России от 19 мая 2006 г. № АК/7654 «Об особенностях отдельных способов распространения рекламы».

[2] Постатейный комментарий к Федеральному закону «О рекламе» / Д.С. Бадалов, И.И. Василенкова, Н.Н. Карташов и др. М., 2012. Комментарий к ст. 3.

[3] См.: Письмо ФАС России от 5 апреля 2007 г. № АЦ/4624.

[4] См., например: постановление Девятнадцатого арбитражного апелляционного суда от 5 марта 2011 г. по делу № А14-7904/2010/227/10: «Сайт ООО «Медика» в сети Интернет не предполагает какого-либо ограничения в доступе путем введения паролей, кодов для получения возможности его посещения, либо прочтения подробных сведений об оказываемых Обществом услугах, в силу чего потенциальным потребителем услуг

пространение носит адресный характер, в силу чего дополнительной проверки такой информации на предмет соответствия требованиям законодательства о рекламе не требуется. В подтверждение данного тезиса можно сослаться на судебную практику, в которой признаются не подпадающими под понятие рекламы сообщения, адресованные лицам, имеющим договорные отношения с лицом, размещающим их[1].

В качестве объекта рекламирования может выступать объект гражданских прав (товар, работа или услуга, предназначенные для введения в оборот; объекты интеллектуальной собственности), субъект (изготовитель или продавец товаров) или мероприятие (конкурс, спортивное соревнование, игры или пари и т.п.). При этом необходимо, чтобы сообщение было направлено на формирование интереса к какому-либо объекту рекламирования, его продвижение на рынке.

Таким образом, для того чтобы квалифицировать информацию, размещенную на веб-сайте, в качестве рекламы, необходимо отсутствие ограничений по доступу к ней со стороны неопределенного круга лиц, наличие в ее содержании определенного объекта рекламирования и направленность такой информации на формирование или поддержание интереса к нему.

Признание той или иной информации рекламой влечет повышенные требования к качеству такой информации. В частности, она должна:

• быть достоверной и добросовестной (ч. 1 ст. 5 Закона о рекламе). Не отвечающей указанным требованиям является, в частности, реклама, содержащая некорректные сравнения рекламируемого товара с находящимися в обороте товарами, которые произведены другими изготовителями или реализуются другими продавцами, а равно сведения, не соответствующие фактическим обстоятельствам, касаются деятельности (товара) конкурентов. Например, употребление слов «лучший», «первый», «номер один» должно производиться с указанием конкретного критерия, по которому осуществляется сравнение и который имеет объективное подтверждение под страхом признания ее недостоверной[2];

Клиники является любой пользователь сети Интернет. Таким образом, информация на сайте Интернет направлена неопределенному кругу лиц».

[1] См., например: постановление ФАС Западно-Сибирского округа от 17 мая 1999 г. № Ф04/945-188/А75-99.

[2] Постановление Пленума ВАС РФ от 8 октября 2012 г. № 58 «О некоторых вопросах практики применения арбитражными судами Федерального закона «О рекламе»» (п. 9, 29). Так, например, недостоверной была по этой причине признана реклама услуг такси с формулировкой «Такси Лидер Самара – лучшее такси в Самаре». См.: постановление

• соответствовать требованиям законодательства Российской Федерации о государственном языке и не должна содержать иностранных слов и выражений, которые могут привести к искажению ее смысла (ч. 11 и п. 1 ч. 5 ст. 5 Закона о рекламе); Например, ФАС России признает недопустимым использование слова «*Sale*» для привлечения внимания к распродажам по причине существования различных значений этого слова[1]. Даже типичное для электронной коммерции слово «*on-line*» может быть признано недопустимым для использования в рекламе[2]. При этом ФАС России допускает использование в рекламе фирменных наименований, товарных знаков и знаков обслуживания на иностранном языке при условии, что они защищаются на территории Российской Федерации[3]. Таким образом, если, скажем, товарный знак на иностранном языке зарегистрирован в Роспатенте, является общеизвестным или признается в соответствии с международным соглашением (например, Мадридским соглашением о международной регистрации товарных знаков 1891 г.), то его использование в рекламе без перевода допустимо. Однако если такой товарный знак зарегистрирован в другой стране, например в США, и не признается в России, то он не подпадает под действие указанного исключения;

• соответствовать требованиям этики (ч. 6 ст. 5 Закона о рекламе). Не допускается использование бранных слов, непристойных и оскорбительных образов, сравнений и выражений, в том числе в отношении пола, расы, национальности, профессии, социальной категории, возраста, языка человека и гражданина, официальных государственных символов (флагов, гербов, гимнов), религиозных символов, объектов

ФАС Поволжского округа от 6 мая 2011 г. по делу № А55-18530/2010; реклама *BMW X5*, содержащая фразу о том, что данный внедорожник является лучшим, в отсутствие указания ссылок на факты в виде побед в конкурсах или иных источников для данного вывода. См.: постановление ФАС Северо-Кавказского округа от 21 декабря 2012 г. по делу № А63-8926/2012; реклама услуг охранного предприятия на веб-сайте *Facebook*, содержащая фразу, что данное предприятие является «крупнейшим в регионе». См.: постановление Восемнадцатого арбитражного апелляционного суда от 15 июля 2013 г. № 18АП-5539/2013 по делу № А76-20663/2012.

[1] Определение ВАС РФ от 18 февраля 2013 г. № ВАС-1040/13 по делу № А65-19639/2012; к аналогичному выводу пришел суд применительно к рекламе, размещенной на интернет-сайте магазина ЦУМ, следующего содержания: «– 30%; – 50%; *SALE*» (постановление ФАС Московского округа от 25 января 2012 г. по делу № А40-143417/10-153-966).

[2] Постановление Одиннадцатого арбитражного апелляционного суда от 23 августа 2012 г. по делу № А65-14800/2012.

[3] См.: ч. 3 ст. 3 Федерального закона от 1 июня 2005 г. № 53-ФЗ «О государственном языке Российской Федерации». См., например: постановление Тринадцатого арбитражного апелляционного суда от 31 августа 2011 г. по делу № А56-7201/2011.

культурного наследия (памятников истории и культуры) народов Российской Федерации, а также объектов культурного наследия, включенных в Список всемирного наследия. Так, использование в рекламе изображений женщин в полуобнаженном виде может быть признано ненадлежащей рекламой как нарушающей требования ч. 6 ст. 5 Закона о рекламе, поскольку к такой рекламе может получить «доступ широкий круг лиц, в том числе и дети, а образ обнаженной женщины для некоторой категории граждан в силу религиозных, философских, политических и иных убеждений является оскорбительным, суд первой инстанции сделал обоснованный вывод о том, что названная реклама носит эротический характер и ограничивает потенциального потребителя рекламы в возможности ее игнорировать»[1];

• быть полной, т.е. содержать существенную информацию о рекламируемом товаре, об условиях его приобретения или использования, не допускать искажений смысла информации и не вводить в заблуждение потребителей рекламы (ч. 7 ст. 5 Закона о рекламе);

• стоимостные параметры должны быть выражены в рублях и лишь в качестве дополнения – в иной валюте (ч. 7^1 ст. 5 Закона о рекламе);

• соответствовать ограничениям, установленным в целях защиты несовершеннолетних. В частности, не подрывать авторитет родителей, не создавать иллюзию доступности товара семьям с любым уровнем достатка, не создавать впечатления о преимущественном положении перед сверстниками вследствие обладания рекламируемым товаром и наоборот – не формировать комплекс неполноценности вследствие необладания таким товаром, не преуменьшать уровня навыков, необходимых для использования товара, не показывать несовершеннолетних в ситуациях, угрожающих их жизни и здоровью (ст. 6 Закона о рекламе);

• содержать сведения о наименовании, месте нахождения и государственном регистрационном номере записи о создании юридического лица; ФИО, ОГРН записи о государственной регистрации физического лица в качестве индивидуального предпринимателя (ст. 8 Закона о рекламе);

• соответствовать требованиям, установленным к рекламе отдельных видов товаров (услуг), указанным в гл. 3 Закона о рекламе: лекарственных средств, медицинских услуг, БАДов, финансовых услуг, основанных на риске игр и пари, табака и табачных изделий, алкогольной продукции (реклама последней в сети Интернет недопустима в принципе).

[1] Постановление Восьмого арбитражного апелляционного суда от 30 сентября 2011 г. по делу № А46-6175/2011.

Помимо этого к такой информации могут применяться положения о хранении рекламных материалов (в течение года с момента последнего распространения таких материалов, ст. 12 Закона о рекламе), а также о сроке действия рекламы, признаваемой офертой, – в течение двух месяцев, если в ней не указан иной срок (ст. 11 Закона о рекламе)[1].

Реклама, не соответствующая требованиям законодательства о рекламе, признается ненадлежащей. Надзор за соблюдением положений законодательства о рекламе осуществляют подразделения Федеральной антимонопольной службы[2], которая периодически проводит мониторинг рекламы, распространяемой в сети Интернет. В числе возможных мер ответственности установлен административный штраф по ст. 14.3 КоАП РФ: для граждан – 2000–2500 руб.; для должностных лиц – 4000–25 000 руб.; для юридических лиц – 10 0000–50 0000 руб. Субъектами административной ответственности по данной статье могут быть рекламодатель, рекламопроизводитель и рекламораспространитель. При этом если одно лицо является одновременно рекламодателем, рекламопроизводителем и рекламораспространителем в отношении одной и той же рекламы, за соответствующее правонарушение оно подлежит привлечению к административной ответственности однократно[3]. Данное положение особенно актуально в сфере электронной коммерции, поскольку, как правило, владелец интернет-магазина является одновременно рекламодателем (продавец товара или иное лицо, определяющее объект рекламирования) и рекламораспространителем (лицом, осуществляющим распространение рекламы любым способом, в любой форме и с использованием любых средств). При этом необходимо учитывать соответствующие основания разграничения ответственности за нарушения законодательства о рекламе, установленные в ч. 6–8 ст. 38 Закона о рекламе, где содержатся виды нарушений, за которые могут быть привлечены к ответственности рекламодатель, рекламораспространитель и рекламопроизводитель.

В связи с тем что дефиниция рекламы достаточно широкая, а требования к ней весьма обширны, возникает вопрос, является ли информация о реализуемых товарах или услугах, размещенная на веб-сайте, рекламой? Ведь признание информации рекламой влечет необходи-

[1] Как было отмечено в § 1 гл. 3 книги, практически любое предложение о продаже товара (услуги), размещенное на веб-сайте, является офертой с точки зрения российского законодательства.

[2] См.: постановление Правительства РФ от 30 июня 2004 г. № 331 «Об утверждении Положения о Федеральной антимонопольной службе».

[3] Постановление Пленума ВАС РФ от 8 октября 2012 г. № 58 «О некоторых вопросах практики применения арбитражными судами Федерального закона «О рекламе»» (п. 10).

мость обеспечения ее соответствия требованиям законодательства о рекламе и возможность привлечения к ответственности за такое несоответствие. В то же время очевидно, что любой проект в сфере электронной коммерции так или иначе связан с размещением информации о том, что охватывается понятием объекта рекламирования (о товарах, работах или услугах, объектах интеллектуальной собственности, сведения о продавце и т.д.). Очевидно, что для информации, размещаемой на веб-сайтах, необходимы определенные изъятия из-под понятия рекламы, в противном случае весь Интернет превратится в одну большую рекламу.

В качестве таких изъятий выступают положения п. 2 ч. 2 ст. 2 Закона о рекламе, согласно которым законодательство о рекламе не распространяется на информацию, раскрытие или распространение либо доведение до потребителя которой является обязательным в соответствии с федеральным законом. Таким образом, не является рекламой информация о производимых или реализуемых товарах, размещенная на официальном сайте производителя или продавца данных товаров, если указанные сведения предназначены для информирования посетителей сайта об ассортименте товаров, условиях их приобретения, ценах и скидках, правилах пользования, также не является рекламой информация о хозяйственной деятельности компании, акциях и мероприятиях, проводимых данной компанией, и т.п., следовательно, на такую информацию положения Закона о рекламе не распространяются[1]. Это, однако, не исключает в некоторых случаях возможности признания такой информации рекламой при наличии в ней особых обозначений, индивидуализирующих продавца, поскольку в таком случае в качестве объекта рекламирования может быть признан не товар, а его продавец[2]. К аналогичному эффекту может привести особое выделение в описании реализуемых товаров их определенных характеристик и свойств товара, которые могут привлечь интерес потребителей[3]. Как указала

[1] Письма ФАС России: от 13 сентября 2012 г. № АК/29977 «О последних изменениях в требованиях к рекламе алкоголя»; от 29 июля 2010 г. № АЦ/24295 «О ценовой информации, размещенной на сайте компании».

[2] Постановление Девятого арбитражного апелляционного суда от 31 августа 2011 г. № 09АП-19239/2011 по делу № А40-21958/11-147-169.

[3] Постановление Шестнадцатого арбитражного апелляционного суда от 6 ноября 2012 г. по делу № А63-6356/2012. В данном деле в описании травяных чаев, реализуемых продавцом, содержалось перечисление различных заболеваний с одновременным упоминанием, что данные чаи оказывают лечебно-профилактический эффект, что послужило основанием для признания ФАС России и судом такого описания рекламой, которая не соответствовала специальным требованиям, установленным в отношении рекламы БАД и лекарственных средств.

ФАС России, «когда размещаемая на сайте информация направлена не столько на информирование потребителей о деятельности организации или реализуемых товарах, сколько на выделение определенных товаров или самой организации среди однородных товаров, организаций (например, в виде всплывающего баннера), такая информация может быть признана рекламой»[1].

В качестве другого изъятия, потенциально применимого к информации, размещаемой на веб-сайте и выводящего ее из-под действия Закона о рекламе, можно указать п. 3 ч. 2 ст. 2 Закона о рекламе, согласно которому положения законодательства о рекламе не распространяются на «справочно-информационные и аналитические материалы (обзоры внутреннего и внешнего рынков, результаты научных исследований и испытаний), не имеющие в качестве основной цели продвижение товара на рынке и не являющиеся социальной рекламой». Учитывая, что многие веб-сайты содержат обзоры и аналитические материалы, посвященные товарам, которые можно приобрести на таких сайтах, данное изъятие также является весьма полезным.

Правда, тут тоже много нюансов. Например, если такой справочно-аналитический материал упоминает объект рекламирования и выставляет его в выгодном свете, он может быть признан рекламой. Особенно это касается различного рода статей и обзоров, которые нередко размещаются на веб-сайтах. Так, в одном деле размещенная на веб-сайте статья «Девальвация-2012?» была признана рекламой, поскольку содержала информацию о выпускаемой обществом ценной бумаге. Формирование интереса к рекламируемому продукту осуществлялось путем первоначального описания общей негативной ситуации в стране и последующего предложения обращаться в офис общества для приобретения рекламируемой ценной бумаги в качестве выхода из такой ситуации. При этом в начале текста рекламы содержится указание на данные Минэкономразвития России, формирующее у потребителя рекламного продукта впечатление сопричастности указанного органа к размещенной рекламе[2].

За пределами данных, достаточно узких по сфере своего действия, исключений практически любая информация, размещенная на веб-сайте, в которой можно выделить объект рекламирования, а также направленность на формирование или поддержание интереса к нему,

[1] Письмо ФАС России от 29 июля 2010 г. № АЦ/24295 «О ценовой информации, размещенной на сайте компании».

[2] Постановление Восемнадцатого арбитражного апелляционного суда от 9 июля 2012 г. № 18АП-5796/2012 по делу № А07-4227/2012.

может быть интерпретирована в качестве рекламы с распространением на нее соответствующего правового режима.

Отечественной судебной практике известно немало случаев признания информации, размещенной на веб-сайтах, в качестве рекламы. Так, содержащееся в сети Интернет на сайте *www.nn.ru* сообщение следующего содержания: «Все [неценз.], один ты классный», чередующееся с сообщением: «*nn.ru* понимает своих посетителей» было признано ненадлежащей рекламой[1].

В другом деле информация, размещенная на официальном сайте стоматологической клиники в сети Интернет, была признана ненадлежащей рекламой по причине неполноты информации. На сайте содержалось сообщение следующего содержания: «В клинике Вы можете оформить любое лечение в рассрочку и кредит. Вместе с нашими специалистами Вы сможете подобрать наиболее удобную для Вас программу (11 вариантов). Отсутствуют любые скрытые комиссии, досрочное погашение – бесплатно». Как указал суд, «размещенная Обществом реклама фактически вводила потребителей в заблуждение, так как не содержала в себе всех условий, которые определяют фактическую стоимость кредита, в том числе: фактическую процентную ставку по кредиту, отсутствие сведений о возможности получения потребителем скидки от рекламодателя на погашение процентов по кредиту. Это привело к искажению смысла информации и в свою очередь вводило в заблуждение потребителей, что свидетельствует о нарушении Обществом ч. 7 ст. 5, ч. 1 п. 2 ст. 2, ч. 3 ст. 28 Закона о рекламе»[2]. Данное дело свидетельствует о том, что в случае наличия на веб-сайте интернет-магазина программ кредитования необходимо максимально детально описывать его условия и соответствовать требованиям ст. 28 Закона о рекламе.

Указание на сайте организации информации о том, что данная организация является единственным официальным представителем какого-либо производителя на определенной территории без достаточных доказательств их истинности может рассматриваться в качестве недостоверной рекламы[3]. Аналогичным образом будет признано не-

[1] Постановление Первого арбитражного апелляционного суда от 29 апреля 2013 г. по делу № А43-23179/2011.

[2] Постановление Первого арбитражного апелляционного суда от 18 мая 2011 г. по делу № А43-29149/2010. См. также: постановления ФАС Северо-Западного округа от 12 апреля 2012 г. по делу № А56-30646/2011; Шестого арбитражного апелляционного суда от 10 февраля 2012 г. № 06АП-212/2012 по делу № А73-13859/2011.

[3] См., например: постановление Второго арбитражного апелляционного суда от 31 января 2013 г. по делу № А28-9625/2012. В данном деле основанием для такого

достоверной рекламой размещение на веб-сайте компании недостоверной информации относительно гарантий исполнения обязательств по договору вроде фразы «все вклады застрахованы»[1] или неполной информации о проводимой акции, из которой нельзя определить группы товаров, участвующих в ней[2].

Если попытаться обобщить существующую практику по спорам, связанным с признанием размещенной на веб-сайтах информации не соответствующей требованиям законодательства о рекламе, можно указать следующее.

Во-первых, суды без особых колебаний признают информацию, размещенную на веб-сайтах коммерческих организаций, рекламой. Как отмечено в одном из решений, «распространение информации на сайте Интернета является рекламой, так как размещенная информация не обращена к определенному кругу лиц, она может быть доступна любому лицу»[3].

Во-вторых, практически во всех делах, за редким исключением, связанных с оспариванием постановлений ФАС России о привлечении к ответственности по ст. 14.3 КоАП РФ за ненадлежащую рекламу, суды вставали на сторону ФАС России и оставляли соответствующие постановления в силе.

В связи с этим рекомендуется со всей ответственностью подходить к качеству информации, размещаемой на веб-сайте, связанном с осуществлением предпринимательской деятельности, с доменным именем, зарегистрированным в зоне *.ru*, .рф, и на русскоязычных веб-сайтах под иными доменными именами. В частности, не допускать

вывода послужило следующее сообщение, размещенное на веб-сайте компании: «салон «Мир климата» является единственным в Кирове официальным представителем фирмы Panasonic» в то время как официальный сайт компании «*Panasonic*» содержал упоминание о семи официальных дистрибьюторах.

[1] Постановление Шестого арбитражного апелляционного суда от 2 февраля 2011 г. № 06АП-6050/2010 по делу № А73-12012/2010. Определением ВАС РФ от 24 мая 2011 г. № ВАС-6179/11 отказано в передаче дела № А73-12012/2010 в Президиум ВАС РФ для пересмотра в порядке надзора данного постановления. В данном деле ключевую роль сыграла неопределенность фразы «все сделки», которая предполагает расширительное толкование видов сделок, заключаемых в связи с оказанием обществом риелторских услуг, к которым относятся как сделки, заключаемые им со своими клиентами по поиску объектов недвижимости, так и сделки с этими объектами, совершаемые клиентами самостоятельно или при его посредничестве. В то же время существующий договор страхования не охватывал данные сделки в полной мере.

[2] Постановление Девятого арбитражного апелляционного суда от 27 марта 2012 г. № 09АП-4440/2012-АК по делу № А40-127575/11-106-650.

[3] Постановление Седьмого арбитражного апелляционного суда от 17 января 2011 г. № 07АП-10905/10 по делу № А45-15922/10.

указания недостоверных сведений, использования фраз, допускающих неоднозначное толкование. В особенности это касается использования превосходных степеней применительно к объектам рекламирования («лучший», «самый», «лидер» и пр.) в тех случаях, когда отсутствует возможность привести объективный источник таких выводов. Даже безобидная на первый взгляд фраза вроде «Индивидуальный подход к каждому клиенту, гибкая система скидок, точность исполнения обязательств являются главным нашим отличием от других компаний» может быть признана не соответствующей законодательству о рекламе как некорректное сравнение с предложениями конкурентов[1]. Разумеется, не должны использоваться недобросовестные приемы юридической техники вроде использования мелкого или сливающегося с фоном шрифта, рассредоточение значимой информации по множеству страниц или даже веб-сайтов или иных техник, которые могут ввести пользователя в заблуждение.

§ 2. Отдельные модели распространения рекламы в сети Интернет. Поисковая (контекстная) реклама

Одним из эффективных средств интернет-маркетинга является использование так называемой контекстной рекламы, под которой понимается размещение рекламы на страницах результатов поиска средствами специализированных поисковых систем Интернета при использовании в качестве основного критерия для показа текст поискового запроса пользователя.

Крупнейшими сервисами контекстной рекламы являются *AdWords* (*Google*); *Bing Ads* (*Bing* и *Yahoo!*), «Яндекс.Директ» (Яндекс). Доходы от размещения поисковой рекламы являются одним из основных источников прибыли для поисковых систем[2].

---

[1] См.: постановление ФАС Уральского округа от 27 декабря 2011 г. № Ф09-8458/11 (Определением ВАС РФ от 24 апреля 2012 г. № ВАС-4870/12 отказано в передаче дела № А47-3906/2011 в Президиум ВАС РФ для пересмотра в порядке надзора данного постановления). В данном решении суд указал, что «в тексте рекламы использовано некорректное сравнение качества рекламируемых услуг с услугами других компаний, путем утверждения о том, что другие компании оказывают услуги худшего качества, недобросовестно исполняют свои обязательства, не предлагают гибкой системы скидок и индивидуального подхода к каждому клиенту. При этом доказательств того, что компания «Центр медицинской техники» имеет самые выгодные условия исполнения обязательств, предприниматель антимонопольному органу не представил».

[2] *Jansen B.* The Comparative Effectiveness of Sponsored and Nonsponsored Links for Web E-commerce Queries // ACM Transactions on the Web. Vol. 1. No 1. May 2007.

Преимущества интернет-рекламы в поисковых службах проявляются в ее высокой степени адресности, а также возможности оплаты лишь за реальных посетителей сайта (*pay per click*). Недостатки также очевидны: они заключаются в малом охвате аудитории и потере большого сегмента потребителей, которые в данный момент не вводят определенный запрос. К тому же такая реклама визуально непривлекательна, не имеет каких-либо существенных отличий от аналогичной рекламы конкурентов и, следовательно, не может быть имиджевой[1].

Разумеется, реклама, размещаемая в поисковых системах Интернета, признается рекламой для целей применения законодательства Российской Федерации о рекламе и должна ему соответствовать без каких-либо изъятий[2].

Соглашение на размещение контекстной рекламы заключается между рекламодателем и поисковой системой или ее партнером (агентом). С точки зрения законодательства о рекламе такое лицо может быть обозначено как рекламораспространитель (лицо, осуществляющее распространение рекламы любым способом, в любой форме и с использованием любых средств). Как рекламодатель оно несет ответственность за соответствие размещаемой рекламы требованиям Закона о рекламе в части требований к ее распространению (ч. 7 ст. 38).

По своей правовой природе договор о размещении контекстной рекламы является договором возмездного оказания услуг. Одной из специфических черт услуг по размещению рекламы в сети Интернет является особая метрика, применяемая для определения размера вознаграждения за оказанные услуги. В качестве таковой обычно выступает так называемый клик, под которым понимается прохождение пользователя по ссылке, содержащейся в рекламе (*cost per click, CPC*). Общая стоимость оказанных услуг определяется количеством кликов за установленный отчетный период, определяемый в соответствии с данными статистики контекстной системы.

Основной обязанностью рекламодателя является формулирование текста рекламных объявлений, которые должны быть размещены, а также сопутствующих параметров. К числу последних относится выбор ключевых слов и словосочетаний, при наличии которых в запросе пользователя ему будет показано рекламное сообщение; выбор так называемых минус-слов, при наличии которых в запросе ему не будет показываться реклама (например, «бесплатно», «дешево» и т.д.);

[1] *Кузнецов Р.В.* Указ. соч. С. 25.

[2] См., например: постановление Девятого арбитражного апелляционного суда от 2 августа 2011 г. № 09АП-17064/2011-АК по делу № А40-21456/11-72-121.

установки географического и временно́го таргетинга[1]. В совокупности указанные параметры, образующие своего рода «техническое задание» рекламодателя, на практике именуются как «рекламная кампания».

В связи с тем что неотъемлемой частью размещения контекстной рекламы в Интернете является указание определенных ключевых слов, весьма актуален на практике вопрос, насколько использование таких слов может нарушать исключительные права других лиц на товарные знаки или фирменные наименования, текстуально совпадающие с такими ключевыми словами? Ведь грамотный подбор ключевых слов позволяет «подвинуть» конкурентов с точки зрения доступности предложений о соответствующих товарах или услугах для восприятия потребителями[2]. Существующие формулировки правомочий, входящих в состав исключительного права на фирменное наименование и товарный знак, включают в себя возможность их использования в рекламе, а исключительное право на товарный знак вдобавок еще включает и отдельное правомочие на размещение товарного знака в сети Интернет (ст. 1474, 1484 ГК РФ). Таким образом, формальное толкование закона вроде бы дает основание для признания нарушением исключительного права на товарный знак действий рекламодателя, использующего в качестве ключевых слов обозначения, зарегистрированные в качестве товарного знака третьим лицом, для размещения рекламы собственных товаров (работ, услуг), относящихся к той же категории, в отношении которой зарегистрирован товарный знак.

---

[1] *Юрасов А.В.* Указ. соч. С. 306.

[2] До появления и масштабного распространения рынка контекстной рекламы цель привлечения внимания пользователей на сайт за счет использования обозначений, воспроизводящих товарные знаки или фирменные наименования конкурентов, достигалась посредством метатегов – неотображаемой пользователю служебной информации о странице сайта, в которой обычно содержится краткое описание страницы и ключевые слова, в наибольшей степени отражающие ее суть. На практике владельцы веб-сайтов для привлечения как можно большего количества посетителей на свой сайт включали в качестве метатегов обозначения, аналогичные товарным знакам и фирменным наименованиям конкурентов, продающих схожие товары. Споры, связанные с возможными нарушениями прав на товарные знаки метатегами, стали прообразами споров по поводу ключевых слов в контекстной рекламе и в настоящее время полностью уступили им место. В настоящее время метатеги уже не так актуальны, так как современные поисковые системы анализируют весь текст страницы, а не только метатеги, что дает более верные данные о ее содержимом. Более того, многие поисковые системы вообще игнорируют записи в полях метатегов для наиболее объективного анализа содержимого страницы. В связи с этим, а также принимая во внимание, что в России громких споров по метатегам так и не случилось, вряд ли тематика метатегов заслуживает дальнейшего рассмотрения в контексте настоящей работы.

В связи с этим представляет интерес зарубежная судебная практика. Одними из первых с данным вопросом столкнулись суды США. Первым спором по данной тематике стало дело *Playboy Enterprises, Inc. v. Netscape Communications*[1], в котором истец обратился с требованием о прекращении продажи ответчиком ключевых слов, воспроизводящих зарегистрированные товарные знаки *Playboy* и *Playmate*. Указанные ключевые слова были приобретены конкурентами истца, осуществляющими продажу товаров «для взрослых». Суд отклонил данный иск по причине того, что он был предъявлен к поисковой системе, которая не осуществляла продажи подобного рода товара и не являлась тем самым конкурентом истца.

Некоторое время после вынесения указанного решения поисковые системы, выступающие в качестве рекламораспространителей контекстной рекламы, чувствовали себя спокойно. Ситуация изменилась после дела *Rosetta Stone Ltd. v. Google, Inc.*[2] В данном деле истец, являвшийся продавцом продуктов для удаленного изучения языков, обратился с иском к поисковой системе *Google* в связи с тем, что она якобы осуществляла активное содействие в нарушении товарного знака истца путем продажи зарегистрированного обозначения в качестве ключевого слова иным лицам, что также вводило в заблуждение потребителей. Суд первой инстанции отказал в удовлетворении требований, не усмотрев фактов введения в заблуждение потребителей действиями ответчика, указав, что потребители такого рода продуктов в состоянии отличить контекстную рекламу под тегом «*Sponsored links*» от результатов поискового запроса. Суд также указал, что *Google* не занимается продажами продуктов, конкурирующих с продуктами истца, поэтому не мог нарушить его товарный знак. Окружной суд изменил решение суда первой инстанции, признав ответчика виновным в «размывании» (*dilution*) товарного знака истца[3]. В тех спорах, где в качестве ответчика выступал непосредственно рекламодатель, использующий в своей рекламе ключевые слова, американские суды признавали его виновным в нарушении товарного знака посредством заманивания покупателей, заинтересованных в приобретении товаров истца, на свой сайт (так на-

[1] 354 F.3d 1020 (9th Cir. 2004).

[2] Rosetta Stone Ltd. v. Google, Inc., 730 F. Supp. 2d 531 (E.D. Va. 2010), aff'd in partandvacatedinpart 676 F.3d 144 (4th Cir. 2012).

[3] Под «размыванием» товарного знака в США понимается один из видов нарушения исключительного права на товарный знак, выражающийся в его использовании в отношении иных товаров, не связанных с теми, в отношении которых он обычно используется, что влечет ослабление различительной способности товарного знака. См.: 15 U.S. Code §1125 (c).

зываемая доктрина *initial interest confusion*)[1]. В деле *Orion Bancorp, Inc. v. Orion Residential Finance LLC and others*[2] суд не только признал неправомерными действия ответчика по включению в качестве ключевых слов товарного знака истца, но и обязал его впоследствии включать данные слова в качестве «минус-слов» при размещении контекстной рекламы.

В Европе судебная практика по данному вопросу отличается значительным разнообразием даже в пределах одной страны. Во Франции некоторые суды признавали поисковые системы, «продающие» ключевые слова, нарушающими права третьих лиц на товарный знак[3]. Другие суды не находили нарушений со стороны поисковых систем, указывая, что нарушителем является рекламодатель[4].

В качестве иллюстрации можно привести Германию, где мнения судов различных земель по рассматриваемой проблематике долгое время различались. Одни суды (земель Брауншвейг[5], Мюнхен[6], Штутгарт[7], Дрезден[8]) сочли использование в качестве ключевых слов обозначений, воспроизводящих товарный знак третьих лиц, нарушением исключительного права на такой товарный знак. Суды Франкфурта[9], Дюссельдорфа[10], Кельна[11], напротив, сочли такое использование допустимым. Недавно точку в вопросе поставил Верховный суд Германии, указав, что использование ключевых слов, воспроизводящих товарный знак третьих лиц, является допустимым, если контекстная реклама и выдаваемые поисковой системой результаты поиска по запросу пользователя четко разделены[12].

Отсутствие единообразной практики применения положений о товарном знаке к новым способам рекламирования товаров в сети Интернет, а также общеевропейский характер законодательства о товарных

---

[1] См., например: Australian Gold, Inc. v. Hatfield, 436 F.3d 1228 (10th Cir. 2006); Storus Corp. v. Aroa Mktg., Inc., No C-06-2454 MMC, 2008 WL 449835 (N.D. Cal. Feb. 15, 2008).

[2] US District Court for the Middle District of Florida, 25.03.2008, № 8:07-cv-1753-T-26 MAP.

[3] Cour D'Appel de Paris, 01.02.2008, Case No 06/13884, GIFAM et autres/SARL Google France et Google Inc.

[4] Tribunal de grande instance de Strasbourg, 20.07.2007, Atrya / Google France et autres; Cour D'Appel de Paris. 13.02.2007. Laurent C/Google France.

[5] Oberlandesgericht Braunschweig. 05.12.2006. No 2 W 23/06; Oberlandesgericht Braunschweig. 11.12.2006. No 2 W 177/06; Oberlandesgericht Braunschweig. 12.07.2007. No 2 U 24/07.

[6] Oberlandesgericht Minchen. 06.12.2007. No 29 U 4013/07.

[7] Oberlandesgericht Stuttgart. 09.08.2007. No 2 U 23/07.

[8] Oberlandesgericht Dresden. 09.01.2007. No 14 U 1958/06.

[9] Oberlandesgericht Frankfurt. 26.02.2008. No 6 W 17/08.

[10] Oberlandesgericht Dusseldorf. 23.01.2007. No 1-20 U 79/06.

[11] Oberlandesgericht Koln. 31.08.2007. No 6 U 48/07.

[12] Bundesgrerichtshof. 13.12.2012. No I ZR 217/10.

знаках[1] послужили основанием для обращения национальных европейских судов в Европейский суд за разъяснениями. Такие разъяснения были даны в нескольких решениях от 23 марта 2010 г.[2] и от 22 сентября 2011 г.[3] В первом деле, где предметом рассмотрения была практика французских судов, Европейский суд пришел к выводу о том, что *Google* как поисковая система и владелец сервиса *AdWords* не несут ответственность за нарушение исключительных прав на товарный знак, продавая ключевые слова, воспроизводящие такой знак, конкурентам его владельца. Ответственность за нарушение товарного знака должен нести по общему правилу рекламодатель, если использование таких ключевых слов в рекламе вводит в итоге потребителей в заблуждение, что должно быть предметом установления национальными судами. При этом, для того чтобы воспользоваться иммунитетом интернет-провайдера, предусмотренным ст. 14 Директивы об электронной коммерции, *Google* должен оперативно удалить соответствующую рекламу по получении уведомления от правообладателя товарного знака. Таким образом, Европейский суд оградил поисковые системы от требований правообладателей, распространив на них общие положения об иммунитете за размещаемый контент и указав, что основной мишенью должны выступать рекламодатели.

Второе решение Европейского суда касалось спора уже между правообладателем и рекламодателем, конкурирующими на одном рынке. Суд выделил три основные функции товарного знака: идентифицирующую происхождение товара, рекламную и репутационную. По мнению суда, о нарушении идентифицирующей функции можно говорить в том случае, когда создается риск возникновения у потребителя заблуждения относительно происхождения товара либо о характере взаимоотношений между конкурирующими компаниями (например, потребитель может воспринять их как входящие в одну сеть). Рекламная функция, по мнению суда, как правило, не нарушается в том случае, когда в качестве ключевого слова используется обозначение, зарегистрированное как товарный знак конкурента, поскольку право-

[1] См.: Директива ЕС «О гармонизации законодательства в области товарных знаков»: Directive 2008/95/EC of the European Parliament and of the Council of 22 October 2008 to approximate the laws of the Member States relating to trade marks.

[2] Google France SARL and Google Inc. v Louis Vuitton Malletier SA (C-236/08), Google France SARL v Viaticum SA and Luteciel SARL (C-237/08) and Google France SARL v Centre national de recherche en relations humaines (CNRRH) SARL and Others (C-238/08). ECJ. 23.03.2010, Joined cases C-236/08 to C-238/08.

[3] Interflora Inc. and Interflora British Unit v Marks & Spencer plc et Flowers Direct Online Ltd. ECJ. 11.09.2011. C-323/09.

обладатель может использовать то же самое ключевое слово для своей рекламы и потеснить рекламу конкурента, предложив большую цену за клик. Репутационная функция товарного знака может быть серьезно затронута такой практикой, поскольку использование таких ключевых слов с последующим «уводом» потребителей на свой сайт может воспрепятствовать накоплению репутации в их глазах и удержанию их лояльности в том случае, когда такая репутация уже накоплена. Соответственно, по мнению суда, в тех случаях, когда использование ключевого слова в поисковой рекламе создает препятствия для реализации одной из указанных выше функций товарного знака, правообладатель может воспрепятствовать использованию его товарного знака в качестве ключевого слова. Помимо указанных случаев это возможно в ситуациях, когда действия конкурента приводят к «размыванию» знака с риском утраты его различительной способности, а также к его очернению.

Указанные решения Европейского суда легли в основу последующих решений национальных судов. Так, Высокий суд Англии в деле *Interflora, Inc. v Marks & Spencer plc*[1] признал использование в качестве ключевого слова в сервисе *Google AdWord* обозначения, эквивалентного товарному знаку истца, нарушением исключительного права на товарный знак. Основным аргументом выступало порождаемое такой контекстной рекламой заблуждение потребителя, который мог ошибочно полагать, вводя в виде запроса слово *Interflora* и проходя по ссылке рекламы флористических услуг *Marks & Spencer*, что последнее является составной частью сети *Interflora*, притом что указанные компании являются самостоятельными и конкурирующими между собой.

Отечественная судебная практика также не обделена решениями, в которых затрагивается проблематика возможности квалификации указания ключевых слов при размещении контекстной рекламы в качестве использования средства индивидуализации. В настоящее время суды, как правило, исходят из того, что ключевые слова, используемые при размещении контекстной рекламы, употребляются *исключительно в технических целях*. Как отмечается, «одно и то же ключевое слово может быть выбрано для рекламных объявлений различных рекламодателей. Ключевые слова не являются частью самого рекламного объявления, не входят в его содержание и не демонстрируются пользователям. Пользователь не обладает информацией о том, по каким ключевым словам размещается показанное ему поисковой системой рекламное объявление, а также не может соотнести определенное

[1] Interflora Inc. & Anor v Marks and Spencer plc & Anor. 21.05.2013. EWHC 1291.

объявление с конкретными ключевыми словами. В связи с этим ключевые слова, используемые при размещении контекстной рекламы, не обладают индивидуализирующей способностью по отношению к каким-либо товарам, услугам или лицам». Их указание в качестве ключевых не является, таким образом, использованием фирменного наименования или товарного знака и не нарушает исключительных прав правообладателей указанных объектов[1].

Представляется, что данный подход российской судебной практики является в целом вполне адекватным. Действительно, регистрация определенного слова или словосочетания в качестве товарного знака не означает возникновения монополии правообладателя над любым их употреблением и далеко не всякое использование таких слов может быть квалифицировано в качестве нарушения товарного знака, особенно если такое использование является «невидимым» для третьих лиц. Товарный знак имеет своей целью индивидуализацию товаров путем придания различительной способности товару или производителю в целях предотвращения смешения товаров. Эта цель находит свое отражение в каждом из способов использования товарного знака, обозначенном в ст. 1484 ГК РФ. В связи с этим правообладатель не вправе ограничивать третьих лиц в указании обозначения, эквивалентного или сходного с товарным знаком, в случае когда такое указание не направлено на индивидуализацию товаров, работ или услуг и не способно вызвать их смешения. Поэтому указание третьими лицами товарного знака или сходного с ним обозначения с целями, отличными от цели индивидуализации товаров, работ или услуг, при отсутствии вероятности смешения различных товаров и производителей не является использованием товарного знака в понимании ст. 1484 ГК РФ и соответственно – нарушением исключительных прав на товарный знак[2].

Нельзя говорить и об использовании товарного знака в виде размещения его в иных формах адресации сети Интернет (подп. 5 п. 2 ст. 1484 ГК РФ), поскольку ключевое слово не позволяет однозначно определить какое-либо рекламное объявление, лицо или товар. Каждому ключевому слову может соответствовать неограниченное количество рекламных объявлений неограниченного количества рекламодателей. Так же как каждому объявлению может соответствовать

[1] См.: постановления Девятого арбитражного апелляционного суда: от 5 августа 2013 г. № 09АП-22393/2013-ГК по делу № А40-159412/12 и от 24 июля 2013 г. № 09АП-19422/2013-ГК по делу № А40-164436/12; Двенадцатого арбитражного апелляционного суда от 20 июня 2012 г. по делу № А12-1125/2012.

[2] Постановление Девятого арбитражного апелляционного суда от 24 июля 2013 г. № 09АП-19422/2013-ГК по делу № А40-164436/12.

почти неограниченное количество ключевых слов. То есть в данном случае отсутствует основной признак адресации – уникальность адреса в определенной адресной системе[1].

Также вряд ли можно во всех случаях использования в качестве ключевого слова товарного знака конкурента говорить о введении потребителей в заблуждение: даже если потребитель и проследует по ссылке контекстной рекламы, он, попав на сайт, увидит, кому он принадлежит, и будет далее основывать свое решение исходя из этого (например, если компания *Toyota* закажет контекстную рекламу с ключевым словом *Honda*, то потребитель, первоначально интересовавшийся автомобилями *Honda*, пройдя по ссылке *Toyota*, будет иметь четкое представление, с товаром какого производителя он имеет дело). К тому же, как правило, спорное объявление может появляться не только при введении ключевого слова, эквивалентного или схожего с товарным знаком третьего лица, но и иных ключевых слов, никоим образом не связанных с охраняемым обозначением (например, «японские автомобили»), что также не позволяет говорить о том, что подобное рекламное объявление всегда вводит в заблуждение пользователей.

Складывающуюся ситуацию с использованием ключевых слов, воспроизводящих товарный знак третьего лица, и отвлечение тем самым пользователей от продуктов такого третьего лица в пользу своих можно уподобить размещению своей рекламы напротив магазина конкурента, что вполне допустимо с точки зрения закона. В итоге свободное использование ключевых слов в контекстной рекламе дает пользователям больший выбор, способствует конкуренции и стимулирует правообладателей товарных знаков не быть «собакой на сене», а внедрять инновационные подходы к продвижению своих продуктов. Свобода осуществления предпринимательской деятельности является не меньшей ценностью, нежели права на товарный знак, последние не должны быть удавкой, которой они непременно станут в случае усиления защиты товарного знака за счет включения в его состав исключительного права на использование ключевых слов в интернет-рекламе. Поэтому следует с осторожностью относиться к существующим за рубежом тенденциям к абсолютизации прав на товарный знак и распространению их на новые типы отношений. Как видно из зарубежной практики, такое распространение носит все же исключительный характер и сопряжено с наличием обстоятельств, при которых потребители вводятся в заблуждение.

[1] См.: решение Арбитражного суда г. Москвы от 13 декабря 2012 г. по делу № А40-36511/11.

Безусловно, нельзя отрицать тот факт, что использование ключевых слов может осуществляться весьма недобросовестно (особенно когда в качестве ключевого слова используются исключительно охраняемые средства индивидуализации третьих лиц – конкурентов). Зарубежная судебная практика демонстрирует немало примеров этому. Можно согласиться с В.О. Калятиным в том, что здесь корректнее говорить о недобросовестной конкуренции, а не о нарушении исключительных прав[1]. Положения Закона о защите конкуренции допускают достаточную гибкость при решении вопроса о квалификации того или иного действия в качестве акта недобросовестной конкуренции. Положения п. 1 ст. 14 данного Закона закрепляют перечень видов недобросовестной конкуренции, к числу которых относится, в частности, введение в заблуждение в отношении характера, способа и места производства, потребительских свойств, качества и количества товара или в отношении его производителей. Важно отметить, что данный перечень включает в себя ряд недобросовестных действий, связанных с манипуляциями исключительными правами третьих лиц. Напрямую они вряд ли могут применяться, потому что, как было указано выше, использование ключевых слов имеет техническую функцию и не является использованием товарного знака в юридическом смысле. Но перечень ст. 14 не является исчерпывающим и вполне может в себя вместить и иные способы манипуляции с информацией, связанной с исключительными правами, которые схожи по существу с теми актами, которые прямо поименованы в качестве недобросовестной конкуренции.

В практике российских судов уже встречались дела, где контекстная реклама была признана ненадлежащей по причине того, что она порочит деловую репутацию конкурента. В качестве иллюстрации можно привести дело, в котором суд пришел к выводу о том, что реклама «Ренова СтройГруп» (экспертиза, взыскание и продажа долгов «Ренова СтройГруп» и ООО «Мегастрой»), с указанием ссылки на сайт ответчика (коллекторской организации) в поисковой системе «Яндекс» при вводе запроса «Ренова», указывает на наличие долговых обязательств у ЗАО «Ренова СтройГруп» перед другими хозяйствующими субъектами и формирует негативное отношение к данной компании»[2]. В данном случае было установлено, что правопредшественник истца действительно имел долги, которые были взысканы с использованием услуг ответчика, но на момент размещения рекламы задолженность

[1] *Калятин В.О.* Право в сфере Интернета. С. 400.

[2] Постановление Девятого арбитражного апелляционного суда от 17 ноября 2011 г. № 09АП-27661/2011-АК по делу № А40-51810/11-145-421.

была уже давно погашена в полном объеме, в связи с чем использование имени известной компании с указанием недостоверной информации, направленное на привлечение внимания потенциальных клиентов, противоречит законодательству о рекламе.

Примечательно, что Европейский суд также говорит о возможности использования арсенала законодательства о рекламе в случаях недобросовестного использования чужих товарных знаков или фирменных наименований в качестве метаданных сайта, которые используются поисковыми системами и могут влиять на результаты поисковых запросов. В одном из решений было указано, что «размещение ответчиком наименований товаров конкурентов или их фирменных наименований в качестве метатегов может повлечь неадекватное представление потребителей о продукции или фирме ответчика, а также необоснованную уверенность в том, что его веб-сайт реализует необходимую ему продукцию или по крайней мере ее прямые аналоги. Суд отверг довод ответчика, что метатеги не являются вариантом рекламирования, поскольку не видны потребителям и рассчитаны на обработку поисковыми системами. По мнению Европейского суда, понятие рекламы достаточно широко для того, чтобы охватить в том числе и такие ее формы, как метатеги, которые способны воздействовать на экономическое поведение потребителей и, следовательно, наносить вред конкуренту, чье наименование или продукция упоминаются в метатегах[1].

Представляется, что схожие подходы могут быть использованы и в России применительно к контекстной рекламе. Таким образом, несмотря на непризнание арбитражными судами нарушений исключительного права на товарный знак (обоснованное на наш взгляд), у потерпевшего есть возможность защитить свои права средствами законодательства о рекламе. В соответствии с п. 3 ч. 2 ст. 5 Закона о рекламе недобросовестной является реклама товара, которая осуществляется под видом рекламы другого товара, товарный знак или знак обслуживания которого тождествен или сходен до степени смешения с товарным знаком или знаком обслуживания товара, в отношении рекламы которого установлены соответствующие требования и ограничения, а также под видом рекламы изготовителя или продавца такого товара. Учитывая существующий обвинительный уклон ФАС России и склонность арбитражных судов соглашаться с ее выводами, данный способ защиты может оказаться весьма эффективным.

[1] Belgian Electronic Sorting Technology NV (BEST NV) v Bert Peelaers, Visys NV, ECJ. 11 July 2013. C-657/11.

Приведенные зарубежные и отечественные судебные споры свидетельствуют о том, что при размещении контекстной рекламы надо быть предельно внимательным по отношению к юридической чистоте такой рекламы с точки зрения возможного использования обозначений, воспроизводящих товарный знак или фирменное наименование конкурентов, а также содержащих потенциально недостоверные или порочащие их деловую репутацию сведения. Следует ожидать, что со временем российская судебная практика по вопросам контекстной рекламы обрастет множеством судебных решений и перестанет считать использование ключевых слов носящим исключительно технический характер.

Баннерная реклама

Баннерная реклама была и остается одним из основных инструментов интернет-рекламы. Под баннером понимается графическое изображение или текстовый блок рекламного характера, содержащий гиперссылку на веб-страницу с расширенным описанием продукта или услуги[1]. Это своего рода «виртуальное окно» в интернет-магазин или иной ресурс, продвигаемый рекламодателем. Баннеры бывают различных видов в зависимости от типов и размера. По типу различают статические баннеры, *gif*-баннеры в виде последовательности сменяющих друг друга кадров с установленным временем задержки, *flash*- или *java*-баннеры, позволяющие включать анимацию и звуковые эффекты. Размеры баннерной рекламы унифицированы и имеют свои так называемые типоразмеры (*IMU – Interactive Marketing Unit*). Наиболее авторитетной в области установления стандартов на рекламу в сети Интернет является компания *IAB* (*Interactive Advertising Bureau*).

Существует три основных способа размещения баннерной рекламы:

1) индивидуальные договоренности с конкретными сайтами (платные или на основе двусторонних соглашений о взаимном обмене баннерами, что типично для сайтов с тематически близкой направленностью[2]);

2) обращение к услугам специализированного рекламного агентства, которое размещает баннеры на определенных сайтах;

3) баннерообменные сети.

---

[1] *Филатова О.А.* Гражданско-правовые особенности рекламы в Интернете: дис. ... канд. юрид. наук. М., 2003. С. 3.

[2] В нашей совместной с А.Г. Карапетовым книге о свободе договора мы квалифицировали данный договор как особый тип смешанного договора с «зеркальными» встречными предоставлениями (см. подробнее: *Карапетов А.Г., Савельев А.И.* Свобода договора и ее пределы: в 2 т. М., 2012. Т. 2: Пределы свободы определения условий договора в зарубежном и российском праве).

Наибольший интерес с точки зрения правового анализа представляет третий случай – использование баннерообменных сетей для размещения рекламы. Под баннерообменной сетью понимается рекламная сеть, в которой участвуют веб-сайты, демонстрирующие баннеры друг друга на основе единых для всех правил. В основу работы баннерообменной сети положен принцип взаимности: один участник предоставляет возможность для размещения на своем веб-сайте баннеров других участников, входящих в баннерообменную сеть, в обмен на совершение ими аналогичных действий. Таким образом, участник баннерообменной сети является одновременно и рекламодателем, и рекламораспространителем. Выгода самой баннерообменной сети состоит в некоторой доле от количества показов (например, 15% у сайта *tbn.ru*), оговоренной заранее, которую баннерообменная сеть получает от каждого участника и может использовать для размещения баннеров коммерческих клиентов. При этом участник баннерной сети может приостанавливать показ своих баннеров, тем самым накапливая определенное количество показов на своем аккаунте, которые могут быть впоследствии использованы им для продажи, обмена или собственных нужд.

Принято различать: а) баннерообменные сети общей направленности[1], в которых содержится минимум ограничений к тематике веб-сайтов участников, исключая обычно сайты эротической (порнографической) направленности или нарушающие законодательство Российской Федерации (например, экстремистской направленности); б) тематические баннерообменные сети[2], в которых существуют строгие ограничения на тематику сайтов-участников.

С точки зрения правовой природы соглашения, возникающие в связи с участием в баннерообменных сетях, представляют собой весьма своеобразную модель договорных отношений. Участники не заключают соглашений между собой. Вступая в баннерообменную сеть[3], они принимают условия этой сети, сформулированные ее администратором, вступая тем самым в отношения с администратором сети[4].

---

[1] См., например: The Banner Network, TBN (*www.tbn.ru*); Russian Link Exchange, RLE (*www.rle.ru*).

[2] См., например: сеть для сайтов автомобильной тематики АвтоБаннер.Ру; *TBN Webmaster*, объединяющий ресурсы для веб-мастеров, веб-разработчиков, веб-дизайнеров и веб-программистов.

[3] Участник обычно даже не знает заранее, на каком именно веб-сайте будет размещен его баннер.

[4] См., например: Правила участия в баннерной сети *TBN*: «Общие правила для всех сетей *TBN* устанавливают отношения между владельцами сайтов-участников всех сетей *TBN* и администрацией» // http://tbn.ru/members/common/rules/index.html

Поэтому договорных отношений непосредственно между участниками не возникает и они не могут предъявлять каких-либо требований друг к другу в связи с неисполнением каких-либо условий правил. Максимум, что они могут сделать в таких случаях, – это обратиться к администратору, который в свою очередь уже обратится к другому участнику от своего имени[1]. По своей правовой природе обязательства администратора можно квалифицировать как услугу по организации процесса размещения рекламы в соответствии с установленными правилами. Все размещаемые баннеры обычно проходят премодерацию администратором на предмет их соответствия требованиям правил, иногда соответствующую модерацию проходят и веб-сайты участников (особенно если баннеры размещаются в сетях, ориентированных на бизнес-сообщество, где особенно важны репутация веб-сайта, характер размещаемого на нем контента и посещаемость). Услуги администратора предоставляются небезвозмездно. Как отмечалось ранее, администратор получает определенный процент от количества показов, которые могут быть им использованы либо для собственной рекламы, либо при реализации рекламных услуг на основании классических коммерческих договоров о размещении интернет-рекламы. Таким образом, отношения между участником и администратором баннерообменной сети могут быть квалифицированы в качестве договора возмездного оказания услуг.

Основной «валютой» в баннерообменных сетях выступают так называемые показы. Под показом понимается одна демонстрация баннера посетителю веб-сайта. Иными словами, каждый раз когда новый посетитель заходит на веб-сайт с соответствующим баннером, участник баннерообменной сети – владелец этого веб-сайта – зарабатывает один показ (за вычетом комиссии администратора). Чем выше популярность сайта, тем больше его посещаемость, а следовательно, тем больше показов зарабатывает его владелец. Информация о посещаемости сайта и количестве показов отражается у администратора сети в разделе «статистика», доступном под логином и паролем конкретного участника. Там же можно ознакомиться с одним из главных показателей эффективности баннерной рекламы *CTR* (*click through ratio*), показывающим, сколько нажатий на баннер пользователями приходится на количество его показов, иными словами, сколько

[1] Английское договорное право является более гибким в этом вопросе и допускает в некоторых случаях признание наличия договорных отношений между участниками, объединенными требованиями общих правил, установленных организатором мероприятия. См.: Clark v. Earl of Dunraven (The Satanita) [1897] A.C. 59.

человек из каждой тысячи, увидев баннер, проходит по ссылке, содержащейся в нем[1].

В зависимости от действующих в баннерообменной сети правил участник может распорядиться своими накопленными показами различными способами: 1) истратить их («открутить») на показ своего баннера на сайтах других участников сети; 2) перевести определенное количество показов на аккаунт другого участника сети; 3) продать баннерные показы администрации баннерообменной сети по ее расценкам (как правило, в качестве метрики используется оплата за 1000 показов или за клик); 4) продать баннерные показы на специализированной бирже (системы электронных торгов баннерными показами различных сетей) по рыночной цене. Таким образом, показ представляет собой особое имущественное право повышенной оборотоспособности, содержанием которого является обязанность администратора соответствующей баннерообменной сети обеспечить размещение баннера управомоченного лица на веб-сайтах участников такой сети.

Расценки на баннерные показы могут существенно варьироваться и зависят от размера баннера, баннерообменной сети и иных факторов. Так, например, сеть *TBN* выкупает 1 млн показов баннера типа *Business* 600×200 за 3320 руб.[2], что позволяет составить некоторое представление о расценках в данной сфере.

Вследствие возможности участников баннерообменных сетей по распоряжению заработанными показами путем их продажи третьим лицам возникает вторичный рынок показов. На данном рынке заинтересованное лицо (рекламодатель) может приобрести определенное количество показов без необходимости размещения на своем веб-сайте баннеров других участников (так называемые коммерческие показы). Обычно их стоимость существенно дешевле, чем в случае приобретения таких показов напрямую у администратора сети.

Как видно, рынок баннерной рекламы и оборот прав на ее размещение (показы) развивается достаточно бурно, принимая весьма оригинальные формы и не нуждаясь в особом правовом регулировании. Это та сфера, где саморегулирование вполне успешно выполняет свою роль. Низкая стоимость показов, высокая динамика отношений

[1] По мере того как баннеры стали обычным делом в сети Интернет и пользователи к ним выработали определенный иммунитет, этот показатель снизился с некогда высоких 10% и более в среднем до 0,1–0,5% (см.: *Калятин В.О.* Право в сфере Интернета. С. 398. Существуют определенные уловки, направленные на повышение *CTR*, связанные как с определенным дизайном баннера и его содержанием, так и с использованием технологий таргетинга; см. подробнее: *Юрасов А.В.* Указ. соч. С. 326–329).

[2] http://tbn.ru/members/common/ransom/wm.html

и широкие полномочия администраторов баннерообменных сетей по пресечению недобросовестных действий участников выступают серьезными сдерживающими факторами для попадания возможных споров в государственные суды. Гораздо проще решить возникшие разногласия в онлайн-режиме[1]. Однако это справедливо в отношении частноправовых аспектов возникающих отношений. Что же касается публично-правовых аспектов, то здесь баннерная реклама, как и любая другая, выступает предметом надзора ФАС России.

Наиболее часто рекламодателей баннерной рекламы обвиняют в предоставлении потребителям неполной информации. Ввиду ограниченных размеров баннера бывает невозможно изложить всю информацию, которая должна быть предоставлена в силу законодательства (ссылки на номера лицензий, исчерпывающие условия кредитования). Нетрудно представить, во что превратится баннер, если в него втиснуть всю необходимую информацию. Привлекать внимание он точно уже не будет. В связи с этим рекламодатели обычно ограничиваются указанием нескольких наиболее привлекательных параметров своего товара (услуги), вся остальная информация содержится на их веб-сайте, ссылка на который является неотъемлемой частью баннера.

Судебная практика достаточно формально подходит к рассмотрению вопроса о соответствии такого подхода к законодательству о рекламе. В большинстве случаев суды поддерживают ФАС России в ее формальном толковании закона, указывая, что отсылка к веб-сайту как источнику дополнительной информации для целей выполнения требований Закона о рекламе является недопустимой[2].

Примечательно, что к вопросу в отношении контекстной рекламы суды готовы более либерально подходить, чем к вопросу в отношении баннерной рекламы. Как указал один из судов, «суд первой инстанции пришел к правильному выводу о том, гиперссылка сразу после «клика» на текст контекстной рекламы содержала всю необходимую

[1] В связи с этим не имеет практического смысла реализация предложений отдельных авторов о введении в законодательство о рекламе специальных положений о баннерной рекламе (см., например: *Филатова О.А.* Указ. соч. С. 123).

[2] См., например, постановления Девятого арбитражного апелляционного суда от 21 января 2013 г. № 09АП-38518/2012-АК по делу № А40-106328/12-148-1018; от 2 февраля 2012 г. № 09АП-35027/2011 по делу № А40-81118/11-17-698; Одиннадцатого арбитражного апелляционного суда от 14 марта 2013 г. по делу № А65-25522/2012; ФАС Северо-Кавказского округа от 20 сентября 2012 г. по делу № А53-8701/2012; Семнадцатого арбитражного апелляционного суда от 14 ноября 2012 г. № 17АП-11567/2012-АК по делу № А71-9177/2012.

информацию в соответствии со ст. 28 Закона «О рекламе»»[1]. При этом суд принял во внимание существо поисковой рекламы, основной функцией которой является «предоставление потребителю ссылки на конкретный источник информации о товаре, который соответствует содержанию запроса поисковой системы».

Возможно, причиной такого дифференцированного подхода является большая техническая ограниченность возможностей контекстной рекламы и ее неразрывная связь со ссылками, предоставляемыми поисковой системой. При конструировании баннера у рекламодателя гораздо больше пространства для маневра, как в выборе его размера, так и в определении его содержания. При грамотном подходе к созданию баннера вполне можно уместить в него всю необходимую информацию, не жертвуя его привлекательностью. В одном деле суд признал незаконным решение антимонопольного органа о привлечении к ответственности рекламодателя за неполную рекламу. В данном споре реклама была выполнена «в форме всплывающего анимационного баннера на странице в сети Интернет, состоящего из 7 страниц, первые 5 из которых содержат рекламную информацию о продукте, реализуемом обществом, и с интервалом в 1–2 секунды автоматически сменяют друг друга, а на остальных 2 страницах размещена вся предусмотренная Законом о рекламе информация о предлагаемой финансовой услуге. При этом последние две страницы баннера открываются при наведении курсора на строку «юридическая информация», расположенную на первых трех из пяти страниц баннера (на тех, которые имеют непосредственное отношение к оказываемым финансовым услугам)»[2].

В приведенном судебном решении также указаны обстоятельства, которые, по мнению суда, обеспечили соответствие баннерной рекламы требованиям законодательства: 1) наличие у потребителя возможности ознакомиться со всеми условиями, размещенными в рекламе, без каких-либо затруднений; 2) обеспечение использованным в рекламном баннере шрифтом возможности нормального восприятия потребителем всей информации. Также, по мнению суда, переход по ссылке «юридическая информация» не являлся затруднительным,

[1] Постановление Девятого арбитражного апелляционного суда от 2 августа 2011 г. № 09АП-17064/2011-АК по делу № А40-21456/11-72-121. Определением ВАС РФ от 2 декабря 2011 г. № ВАС-15405/11 отказано в передаче дела № А40-21456/11-72-121 в Президиум ВАС РФ для пересмотра в порядке надзора данного постановления.

[2] Постановление Одиннадцатого арбитражного апелляционного суда от 22 января 2013 г. по делу № А65-15781/2012.

а способ размещения информации позволял просматривать анимационный баннер неоднократно, без ограничения количества просмотров.

Правда, по вопросам соответствия используемого шрифта могут быть различные позиции. В одном решении суд указал, что «способ описания условий тарифа в сочетании с характером и особенностями размещения рекламы не позволяют потребителю понять и уяснить с равной степенью концентрации внимания всю совокупность изложенных в рекламе условий тарифа, искажает действительный смысл информации, размещенной крупным шрифтом... несоразмерность шрифта привела к потере читаемости существенных условий по кредиту, что создало препятствия для восприятия указанной информации»[1].

В связи с вышеизложенным необходимо искать взвешенный компромисс между идеями маркетологов, которые направлены на привлечение внимания к рекламируемому товару (услуге) за счет проставления акцентов на определенных аспектах их предложения, и требованиями законодательства о рекламе в части предоставления полной и достоверной информации. Достаточный размер и многостраничный характер баннера с четким изложением информации в ряде случаев позволяют обеспечить такой компромисс.

§ 3. Электронная почта как средство рекламы. Спам

Еще одним распространенным способом рекламы в сети Интернет является рассылка сообщений на электронные почтовые ящики. Как отмечалось ранее, появление электронной почты стало важной вехой в развитии Интернета, вызвав интерес к его использованию за пределами узкого круга ученых, занятых его разработкой. Разумеется, потенциал электронной почты не мог не быть замеченным субъектами электронной коммерции, так как в отличие от иных видов рекламы электронная почта обеспечивает адресное обращения к конкретному пользователю. Согласно ряду зарубежных исследований отклик на рекламу, распространяемую по электронной почте, выше, чем отклик на баннеры[2].

Закон о рекламе содержит специальные положения, посвященные регулированию распространения рекламы по сетям электросвязи, к которым помимо телефонной, сотовой и факсимильной связи от-

[1] Постановление Девятого арбитражного апелляционного суда от 23 января 2013 г. № 09АП-39458/2012 по делу № А40-51588/12-153-548.

[2] *Юрасов А.В.* Указ. соч. С. 335.

носится и сеть Интернет. В соответствии со ст. 18 распространение рекламы по таким сетям допускается только при условии предварительного согласия абонента или адресата на получение рекламы. Под абонентом или адресатом надлежит понимать лицо, на чей адрес электронной почты или телефон поступило соответствующее рекламное сообщение[1].

Реклама признается распространенной без предварительного согласия абонента или адресата, если рекламораспространитель не докажет, что такое согласие было получено. Согласие абонента может быть выражено в любой форме, достаточной для его идентификации и подтверждения волеизъявления на получение рекламы от конкретного рекламораспространителя. На практике согласие на рассылку сообщений электронной почты обычно получается в процессе регистрации на соответствующем веб-сайте либо при оформлении различных документов на участие в бонусных программах (получение скидочных карт, карт постоянного клиента, участие в розыгрышах и пр.). Устная форма выражения согласия является достаточно рискованной, поскольку впоследствии практически невозможно доказать не только факт его предоставления, но и предоставление его конкретным лицом – получателем рассылки[2].

Согласно ст. 18 Закона о рекламе рекламораспространитель обязан немедленно прекратить распространение рекламы в адрес лица, обратившегося к нему с таким требованием. В связи с этим каждое электронное сообщение должно содержать указание на возможность от отказа от рассылки, либо такая возможность должна быть обеспечена при обращении адресата по контактным данным интернет-магазина, размещенным на его веб-сайте.

Не трудно заметить, что Закон о рекламе рисует некую идеальную картину мира, в которой должны циркулировать рекламные сообщения электронной почты: пользователь сам решает, желает он получать рекламную рассылку от определенного отправителя или нет (*«opt-in» approach*), и в любой момент после дачи такого согласия может переду-

[1] Постановление Пленума ВАС РФ от 8 октября 2012 г. № 58 «О некоторых вопросах практики применения арбитражными судами Федерального закона «О рекламе»» (п. 15).

[2] См., например: решение Арбитражного суда г. Москвы от 14 сентября 2011 г. № А40-101998/2011. В данном деле компания ООО «СК Софтлайн» была привлечена к ответственности за нарушение законодательства о рекламе за отправление сообщения рекламного характера на почтовый ящик адресата без его предварительного согласия. Доказать факт получения его согласия в устной форме в ходе предварительной беседы по телефону компании не удалось.

мать и отказаться от него. На практике ситуация принципиально иная. Почтовые ящики пользователей забиты так называемым спамом[1] – незапрошенными рекламными сообщениями, носящими массовый характер, а некогда санкционированные рассылки продолжают поступать даже после выражения отказа от них.

Спам является одной из болезней Интернета, для которой пока не найдено эффективного решения. Основными причинами, обусловливающими его вредоносный характер, являются:

• ухудшение пропускной способности каналов связи. Еще в 2003 г. общий объем рассылаемого спама составлял около 50% всего мирового трафика. С тех пор ситуация ухудшается. По данным ЗАО «Лаборатория Касперского», по состоянию на июль 2013 г. доля спама в почтовом трафике составила 71,2%[2];

• дополнительные затраты интернет-провайдеров и пользователей на приобретение специального программного обеспечения, фильтрующего спам;

• риски удаления полезных сообщений вследствие использования спам-фильтров, что снижает надежность электронной почты как средства коммуникации;

• стоимость времени, потраченного на удаление спама из почтового ящика и (или) возврат полезных сообщений, удаленных в специальную папку «спам», а также трафика, который пользователи небезлимитных тарифных планов вынуждены оплачивать интернет-провайдеру за полученный спам. В мировом масштабе убытки, подпадающие под данную категорию, могут достигать сумм, близких к 100 млрд долл. в год[3];

• ущерб окружающей среде. Согласно исследованиям *McAfee* на распространение спама затрачивается порядка 33 млрд кВт/ч, что эк-

[1] По данным *Wikipedia*, слово «*SPAM*» впервые появилось в 1936 г. в качестве обозначения мясных консервов компании *Hormel Foods Corporation* и расшифровывалось как *SPiced hAM* (острая ветчина). В историю вошла рекламная кампания данных консервов, при которой слово «*SPAM*» бросалось в глаза на каждом углу: с витрин всех дешевых магазинов, бортов автобусов и трамваев, фасадов домов и газет. Реклама консервов «*SPAM*» беспрерывно транслировалась по радио. Всемирную известность в применении к назойливой рекламе термин «*SPAM*» получил благодаря знаменитому скетчу «Спам» из известного английского телевизионного шоу «Летающий цирк Монти Пайтона», вышедшего в 1969. В Интернет спам принесли юристы: первая рассылка такого рода была сделана 5 марта 1994 г. двумя юристами, рекламировавшими услуги их юридической фирмы.

[2] http://www.securelist.com/ru/analysis/208050808/Spam_v_iyule_2013

[3] *Soma J., Singer P., Hurd J.* Spam Still Pays: The Failure of the CAN-SPAM Act of 2003 and Proposed Legal Solutions // Harvard Journal of Legislation. No 45. 2008. P. 165–166.

вивалентно количеству электричества, потребляемому 2,4 млн американских домов[1];

• зачастую спам содержит недостоверную информацию, мошеннические схемы, информацию порнографического характера, непристойные высказывания или иные виды информации вредоносного характера[2].

Неудивительно, что на противодействие спаму направлен ряд законодательных норм как в России, так и за рубежом.

В России существуют три нормативных правовых акта, потенциально применимых к спаму, при этом содержащих различное отношение к нему.

Так, помимо ранее приведенных положений ст. 18 Закона о рекламе, устанавливающих *opt-in*-подход в отношении рекламных рассылок по сети Интернет, в ней содержится специальная норма, указывающая недопустимость использования сетей электросвязи для распространения рекламы с применением средств выбора и (или) набора абонентского номера без участия человека (автоматического дозванивания, автоматической рассылки) (п. 2 ст. 18).

Следует подчеркнуть, что положения законодательства о рекламе по своей природе касаются только спама, носящего коммерческий характер. Идеологический спам (сообщения политического, религиозного или агитационного содержания), а также хулиганский спам (бессмысленные сообщения, содержащие нецензурные выражения, направленные из хулиганских мотивов) не охватываются данными положениями, а следовательно, за рассылку такого спама его отправителя нельзя привлечь к ответственности по ст. 14.3 КоАП РФ.

По мнению В.Б. Наумова, включение норм против спама непосредственно в Закон о рекламе не стало оптимальным решением, так как рамки Закона не позволяют детализировать регулирование и раскрыть требования к интернет-провайдерам в части хранения информации (ст. 12 Закона), а также определить условия распространения информации некоммерческого характера[3].

В связи с этим неудивительно, что попытки борьбы со спамом были предприняты и в иных нормативных актах. Следующим по счету стал Закон об информации, согласно ст. 10 которого при использовании

---

[1] The Carbon Footprint of Email Spam Report (2009) // http://www.twosides.info:8080/content/rsPDF_130.pdf

[2] См.: *Наумов В.Б.* Право и Интернет: очерки теории и практики. С. 97–98.

[3] См.: *Наумов В.Б.* Противодействие спаму: российское законодательство через призму опыта США // Информационное право. 2007. № 3.

почтовых отправлений и электронных сообщений лицо, распространяющее информацию, обязано обеспечить получателю информации возможность отказа от такой информации, а также включать в себя достоверные идентификационные сведения о лице, распространяющем такую информацию. Как видно, в отличие от Закона о рекламе данный Закон применительно к рассылке сообщений электронной почтой исходит уже из принципа *opt-out*. К тому же в силу упоминавшихся ранее положений п. 3 ст. 17 Закона об информации интернет-провайдеры могут рассчитывать на иммунитет от гражданско-правовой ответственности за распространение спама «по передаче информации, предоставленной другим лицом, при условии ее передачи без изменений и исправлений». Так что даже в случае идентификации интернет-провайдера, предоставившего доступ спамеру, привлечь его к ответственности за возникшие убытки не получится.

Тема распределения ответственности за спам между интернет-провайдерами и пользователями была развита в Правилах оказания телематических услуг связи, которые примечательны тем, что в них содержится легальная дефиниция спама: «телематическое электронное сообщение, предназначенное неопределенному кругу лиц, доставленное абоненту и (или) пользователю без их предварительного согласия и не позволяющее определить отправителя этого сообщения, в том числе ввиду указания в нем несуществующего или фальсифицированного адреса отправителя».

Правда, на этом позитивная роль правил в противодействии спаму заканчивается. Во-первых, приведенное определение страдает существенным недостатком, выражающимся в наличии признака «направление сообщения неопределенному кругу лиц», поскольку с технической точки зрения спам отправляется вполне определенным лицам, точнее на вполне определенные адреса электронной почты.

Во-вторых, данная дефиниция была введена в Правила по существу лишь для того, чтобы привязать ее к обязанности пользователя (абонента) препятствовать распространению спама с его компьютера, обязанности интернет-провайдера проинформировать пользователя о мерах, препятствующих распространению спама, а также о предусмотренной договором ответственности за действия (бездействие), способствующие распространению спама. Как видно, Правила никоим образом не возлагают какой-либо ответственности на интернет-провайдеров за спам, распространяемый при помощи их услуг. Правила предлагают им предусмотреть такую ответственность, но вполне очевидно, что данное «предложение» не находит отклика у интернет-провайдеров.

Таким образом, как справедливо отмечает В.Б. Наумов, «в России отсутствуют устойчивые представления о том, как следует определить и регулировать массовые рассылки и какие запреты надлежит реализовать в законодательстве»[1]. Отдельные нормативные акты предусматривают *opt-out*-подход (Закон об информации), другие – *opt-in*-подход (Закон о рекламе, Правила оказания телематических услуг связи).

Насколько принципиальны различия между *opt-in*- и *opt-out*-подходами? Первый более легок в применении на практике: пользователю почтового ящика или правоприменительному органу достаточно доказать факт получения массовой рассылки от определенного лица, бремя доказывания наличия предварительного согласия от пользователя несет отправитель. Факт наличия письма в почтовом ящике доказать легче, чем факт получения согласия от адресата, особенно если оно было выражено в электронной форме. При *opt-out*-подходе потенциального спамера гораздо сложнее привлечь к ответственности: пользователю или правоприменительному органу необходимо доказать не только факт получения электронного письма, но и факт его несоответствия установленным требованиям, в частности отсутствие возможности для отписки, что сделать весьма непросто, особенно учитывая, что в большинстве своем спам-сообщения включает в себя ссылки, пройдя по которым можно якобы отписаться от дальнейших рассылок, чего на практике не происходит, но это еще надо доказать. Таким образом, бремя доказывания, лежащее на инициаторах процесса против предполагаемого спамера, существенно выше, а следовательно, споров в этой области существенно меньше. И это притом, что большинство спамеров и так уходят от ответственности в связи со сложностями их идентификации.

С теоретической точки зрения механизм *opt-out* представляет собой своего рода ограниченное право на спам. В его основе лежит предположение, что спам не отличается качественно от иных сообщений, на получение которых пользователь почтового ящика дал свое согласие конклюдентными действиями в виде регистрации такого ящика[2]. Некоторые специалисты утверждают, что такой подход в большей степени соответствует ценностям свободного общества, предполагающим отсутствие необходимости получения

[1] *Наумов В.Б.* Противодействие спаму: российское законодательство через призму опыта США.

[2] *Khong D.* An Economic Analysis of Spam Law // Erasmus Law and Economics Review/ No 1. 2004. P. 33.

разрешения на то, чтобы одному члену общества инициировать коммуникации с другим[1]. Абстрагируясь от высоких демократических идеалов, необходимо отметить, что основная проблема с *opt-out*-подходом заключается в том, что он стимулирует недобросовестное поведение. Реализация пользователем права на отписку является сигналом того, что владелец почтового ящика активен и отвечает на спам, что повышает ценность такого почтового ящика в глазах спамеров. В результате реализация *opt-out*-подхода количество спама только возрастает.

Отечественная судебная практика не может похвастаться большим количеством споров, связанных с привлечением к ответственности распространителей спама по электронной почте. В основном это связано со сложностями идентификации почтового ящика, с которого была сделана рассылка, и последующей идентификацией личности спамера. Те споры, где распространитель рекламных сообщений посредством электронной почты был привлечен к ответственности за ненадлежащую рекламу (нарушение ст. 18 Закона о рекламе), касаются случаев, когда личность такого распространителя была установлена и не выступала предметом споров[2]. Таким образом, такие споры не касаются классических спамеров, которые используют «одноразовые» почтовые ящики или, что еще хуже, зараженные компьютеры обычных пользователей в удаленном режиме (так называемые ботнеты, от англ. *botnet*), сами располагаясь, как правило, в иных юрисдикциях, нежели те, где находится целевая аудитория спама.

Несовершенство российского законодательства в области противодействия спаму обычно приводится в качестве одной из главных причин роста его количества в России. Тем не менее ситуация за рубежом, где существуют более продвинутые законы в этой области, ненамного лучше.

---

[1] *Templeton B.* Problems with opt-out lists for E-mail // http://www.templetons.com/brad-/spam/globout.html

[2] Постановление ФАС Уральского округа от 15 февраля 2011 г. № Ф09-113/11-С1: «...поскольку общество не представило доказательств наличия согласия ООО «Рубин» на получение указанной рекламы, распространенная информация, направленная на привлечение внимания к услугам общества и других юридических лиц, является ненадлежащей рекламой, нарушающей требования, установленные ч. 1 ст. 18 Закона о рекламе»»; постановление Семнадцатого арбитражного апелляционного суда от 3 сентября 2008 г. № 17АП-5887/2008-АК по делу № А50-7333/2008: «...рассылка информации о новогодних подарках проводилась ОАО «Кондитерская фабрика «Пермская»» посредством сети Интернет на электронные адреса 20 абонентов в период с 14.10.2007 по 16.10.2007 г., в том числе и на электронный адрес ИП Кошина без предварительного его согласия на получение рекламы».

В США к декабрю 2003 г. в 36 штатах были приняты законы против спама, которые использовали различные подходы: от введения требований указания достоверной информации об отправителе и теме письма в соответствующих полях, до введения *opt-out*- и даже *opt-in*-регулирования. В ответ на сложившийся разнобой в подходах был принят федеральный закон *CAN-SPAM Act*[1], целью которого было установление единообразных требований к массовым рассылкам электронной почты коммерческого характера, поскольку на практике их отправителям было очень сложно определить, законодательство какого штата подлежит применению к соответствующей рассылке.

CAN-SPAM Act не запретил массовые рассылки сообщений на электронную почту *per se*. Во-первых, данный закон касается лишь незапрошенных коммерческих рассылок. Во-вторых, закон установил определенные условия, которым такие сообщения должны соответствовать. В частности, они должны содержать: 1) достоверную информацию о содержимом письма в названии его темы (*subject*), а также об отправителе и его почтовом адресе; 2) предупреждение о направленности сообщения на взрослую аудиторию в случае, если оно носит сексуальный характер; 3) обеспечение возможности отписки (*opt-out*). Надзор за соблюдением положений законодательства в области массовых рассылок возложен на Федеральную торговую комиссию (*FTC*) и прокуроров штата. Интернет-провайдерам также была предоставлена возможность предъявления исков, вызванных убытками от рассылок, нарушающих данный закон. Рядовым пользователям, пострадавшим от спама, такой возможности предоставлено не было. В американском стиле за нарушение данного закона были установлены высокие штрафы и даже тюремное заключение. В реальности же указанный закон мало что сделал для того, чтобы уменьшить количество спама в США. США являлись и являются поныне одними из лидеров стран – источников спама[2]. В американской доктрине единодушно утверждается о неэффективности *CAN-SPAM Act*[3]. Критики указывают на то, что данный закон способствует увеличению спама, так как фактически содержит в себе инструкцию о том, как можно «спамить» легально. В то же время «легальный» спам раздражает пользователей ненамного меньше, чем

[1] Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003.

[2] http://www.securelist.com/ru/analysis/208050806/Spam_vo_vtorom_kvartale_2013

[3] См., например: *Zhang L.* The CAN-SPAM Act: An Insufficient Response to the Growing Spam Problem // Berkeley Technology Law Journal. No 20, 2005; *Reyero J.* The CAN-SPAM Act of 2003: A False Hope // SMU Science and Technology Law Review. No 11. 2008; *Arora V.* The CAN-SPAM Act: An Inadequate Attempt to Deal with a Growing Problem // Columbia Journal of Law and Social Problems. No 39. 2006.

весь остальной. К тому же Закон не запрещает и не ограничивает политический и иной некоммерческий спам, допуская тем самым почти легальное вторжение в личное пространство пользователей.

Европейский союз также не остался в стороне от проблемы спама. Одной из первых попыток противодействия ему были положения ст. 7 Директивы № 2000/31/ЕС об электронной коммерции, которые устанавливали *opt-out*-механизм отписки от массовых рассылок коммерческого характера, а также определенные требования к маркировке таких сообщений. При этом государства – члены ЕС могли вводить более жесткие требования в национальном законодательстве. Одной из основных отличительных черт положений ст. 7 Директивы являлось создание так называемых реестров почтовых адресов пользователей, отказавшихся от рассылок, с которыми отправители должны регулярно ознакамливаться и которые должны принимать во внимание.

Неопределенность критериев «регулярности», а также тот факт, что такие списки так и не были созданы, привели к тому, что Европейский союз пересмотрел свое отношение к регулированию массовых рассылок по электронной почте. Соответствующие положения были включены в ст. 13 Директивы № 2002/58/ЕС о частной жизни и электронных коммуникациях[1]. Главной новеллой стало введение режима *opt-in*. В качестве исключений устанавливается случай осуществления рассылки с рекламой на адреса, полученные от покупателей в процессе продажи товаров (услуг) при условии, что: 1) такая рассылка осуществляется непосредственно лицом (организацией), получившим такой электронный адрес; 2) для рекламирования схожих (*similar*) товаров (услуг); 3) покупателю в момент получения от него электронного адреса была предоставлена простая и бесплатная возможность отказа от использования их электронного адреса для указанных целей.

Однако и эти положения было достаточно сложно реализовать на практике. Во-первых, они создавали сложности для организаций, входящих в группу лиц, поскольку формально головная компания и иные аффилированные лица не могли воспользоваться вышеуказанным исключением, не являясь организацией, непосредственно получившей электронный адрес от покупателя. Во-вторых, понятие схожего товара (услуги) отличается достаточной неопределенностью. В-третьих, национальные законодательства по-разному трактуют понятие «процесс продажи». Так, в Англии достаточно одного фак-

[1] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) // OJ L 201. 31.07.2002.

та проведения переговоров о возможной продаже товара. В Германии, напротив, необходим факт совершения сделки купли-продажи[1]. Наконец, обязательность *opt-in*-механизма была установлена лишь для адресатов – физических лиц. Распространение его на юридических лиц оставлялось на усмотрение национального законодательства государств-членов (ст. 13 (5) Директивы № 2002/58/ЕС).

Нельзя сказать, что положение со спамом в Европе существенно улучшилось с момента принятия вышеуказанных законодательных положений. В отчете Европейской комиссии отмечалась неоднородность подходов, принятых в правоприменительной практике стран – участниц ЕС, а также результатов имплементации. По мнению Комиссии, необходимы более активные меры по принудительному исполнению положений законодательства в области противодействия спаму со стороны национальных органов, более масштабная поддержка со стороны бизнес-сообщества, а также активное международное сотрудничество в указанной сфере для того, чтобы добиться осязаемых результатов[2]. Несмотря на то что в некоторых странах (например, Голландии) удалось снизить объем исходящего спама, объем получаемого спама не снизился существенно, поскольку он исходит в большинстве своем из иных стран, нежели из стран Евросоюза[3].

Как показывает зарубежный опыт, даже в тех правопорядках, где сформировалось четкое видение того, какой должна быть политика в отношении массовых рассылок (принцип *opt-in* или *opt-out*, требования к маркировке и пр.), проблема спама является не менее актуальной, чем в России. Более того, можно сказать, что российское законодательство в данной области в целом отражает подходы, принятые в Европе. Так, массовые рассылки коммерческого характера могут быть квалифицированы в качестве рекламы, должны осуществляться при наличии *предварительного согласия* получателя и должны соответствовать всем требованиям, предъявляемым к рекламе (добросовестность и достоверность, полнота предоставляемой информации и пр.). В связи с этим массовые рассылки коммерческого характера, которые делаются без согласия получателя либо даже если и с согласия, но содержат недостоверную или неполную информацию, являются ненадлежащей рекламой со всеми вытекающими последствиями по ст. 14.3 КоАП РФ.

---

[1] *Mutchler A.* Op. cit. P. 972.

[2] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on Fighting Spam, Spyware, and Malicious Software, at 11-12, COM (2006) 688 final (Nov. 15 2006) // http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2006:0688:FIN:EN:PDF

[3] *Mutchler A.* Op. cit. P. 975.

Казалось бы, регулирование есть, оно в целом соответствует «лучшим практикам», существующим в мире. Почему же количество спама только растет с каждым годом? Представляется, что причина кроется отнюдь не в качестве законодательства. Это тот случай, когда в качестве первопричины необходимо искать экономические, а не юридические предпосылки.

Во-первых, в отличие от классических видов рекламы спам перераспределяет издержки, связанные с ее распространением, с рекламораспространителя на получателя. Основные издержки несет получатель (его работодатель): именно его время тратится на разбор почты и удаление лишнего из почтового ящика, именно он прямо или косвенно (в виде повышенной цены услуг интернет-провайдеров) оплачивает специальные программные средства по фильтрации спама, именно он несет потери в случае удаления нужного письма такими программными средствами. Спамер не несет особых затрат на распространение спама: в отличие от распространения рекламы в виде листовок ему безразлично, сто или несколько тысяч электронных адресов стоит в поле адресата. Различного рода технические меры противодействия спаму, безусловно, снижают в какой-то степени объем получаемого пользователями спама, но, с другой стороны, они делают спамеров более агрессивными, заставляя увеличивать масштабы рассылки в расчете на то, что шансы на успешный «прорыв» обороны таких технических мер тем самым возрастут. Получается, чем активнее используются технические средства, тем больше спама появляется в ответ, что в свою очередь влечет повышение спроса на такие технические средства. Замкнутый круг, от которого в определенной степени выигрывают производители соответствующего программного обеспечения или по крайней мере уж точно не проигрывают.

Именно потому, что спам представляет собой легкий и оперативный способ обращения к множеству людей с минимальными затратами, он пользуется такой популярностью. Поэтому чтобы минимизировать количество спама, необходимо или повысить стоимость его распространения[1], или усложнить процесс использования электронной

[1] Теоретически можно увеличить издержки спамеров путем усложнения приобретения ими электронных адресов пользователей, в частности, этому должно способствовать усиление их охраны в качестве персональных данных. Однако на практике законодательство о защите персональных данных показало свою малую эффективность, возлагая немалые затраты лишь на добросовестных участников электронной коммерции. Учитывая тот немалый арсенал способов получения электронных адресов, который имеется у спамеров (автоматическая генерация электронных адресов, кража контактов с зараженных компьютеров, приобретение нелегальных баз данных рабочих

почты, сделав ее менее удобной для распространения информации множеству лиц. Поскольку второй способ чреват тем, что «вместе с водой выплеснут и ребенка», наибольший эффект может быть достигнут принятием мер по удорожанию стоимости одного сообщения, рассылаемого множеству лиц.

Одно из возможных решений было предложено компанией *Microsoft*. Суть предложения (так называемой *Penny Black*) состоит в возложении на компьютер отправителя бремени осуществления определенных вычислительных задач, на решение которых уйдет порядка 5–10 секунд за каждое письмо. Вкратце суть идеи выражается в следующем: «Если я тебя не знаю и ты хочешь отправить мне сообщение, ты должен продемонстрировать, что ты приложил определенное количество усилий для отправки этого сообщения лично мне». Если исходить из того, что в сутках порядка 80 000 сек., при введении «вычислительного налога» в размере 10 сек. количество возможных спам-сообщений с одного компьютера не будет превышать 8000[1]. Предполагается, что для обычных писем с небольшим количеством адресатов данный вычислительный «налог» не будет существенным бременем, но в то же время он существенно ограничит возможности отсылки письма тысячам адресатов.

Другая идея заключается в том, чтобы сделать просмотр рекламных сообщений платным: если пользователь откроет письмо и сочтет его бесполезным, ему будет зачислена со счета отправителя определенная сумма (в пределах нескольких центов)[2]. Данный метод предполагает наличие у каждого переписчика некоего счета, на котором будет храниться определенная сумма. Несмотря на то что в настоящее время получили всеобщее распространение электронные деньги, позволяющие осуществлять микроплатежи, вопросы, связанные с организацией необходимой инфраструктуры для реализации данного предложения, являются весьма непростыми. Однако использование данного метода вполне возможно если не в качестве основного, то в качестве дополнительного по отношению к иным, в частности к описываемому ниже способу разделения всех адресов электронной почты на доверенные

электронных адресов, сбор сведений об электронных адресах на различных форумах и иных интерактивных ресурсах, взлом веб-серверов с получением доступа к базам данных о зарегистрированных пользователях и т.д.), проблем с нахождением электронных адресов у них никоим образом не прибавится от совершенствования законодательства в сфере защиты персональных данных.

[1] http://research.microsoft.com/en-us/projects/PennyBlack/

[2] *Soma J., Singer P., Hurd J.* Spam Still Pays: The Failure of the CAN-SPAM Act of 2003 and Proposed Legal Solutions. P. 173.

и иные. Получение платежа за рекламное объявление может свидетельствовать о добросовестности отправителя и являться основанием для включения его адреса в «белый» список.

Существуют и иные предложения внеправового характера, направленные на решение проблемы спама. Так, высказано предложение о разделении электронной почты на два больших сегмента: доверенные адреса (*whitelist*), которые обладают доверием и в отношении которых могут быть применены реальные санкции в случае нарушения правил отправки почтовых сообщений, и все остальные адреса. В отношении сообщений, исходящих от доверенных источников, не применяется никаких технических средств вроде фильтрации или блокирования. В случае нарушения правил личность нарушителей известна и к ним могут быть применены реальные санкции, что будет стимулировать отправителей к соблюдению установленных правил. В отношении всех остальных сообщений будет действовать следующая процедура: они будут попадать на специальный пул компьютеров, выступающих в качестве своего рода фильтров, пока будет производиться анализ количества сообщений, исходящих с определенного *IP*-адреса, а также проводиться стандартная проверка сообщения техническими средствами (фильтрация, блокировка). В случае если будет установлено, что с этого *IP*-адреса осуществляется массовая рассылка сообщений, которая является нетипичной для такого адреса, либо такой адрес только появился, а рассылаемые сообщения подпадают под понятие спама в соответствии с программой, то они не будут доставлены адресатам из «белого» списка[1]. Представляется, что удешевление вычислительных ресурсов, развитие облачных технологий и *open source* вполне позволяют реализовать подобное предложение на практике при условии корректировки почтовых протоколов и поддержки данного предложения интернет-сообществом. Однако это дело относительно отдаленной перспективы.

В американской литературе также было высказано мнение о целесообразности привлечения интернет-провайдеров к решению проблемы спама путем возложения на них дополнительных обязанностей. В частности, обязанности отслеживать массовые рассылки и обеспечивать идентификацию лиц, их осуществляющих. Это, по мнению авторов данного предложения, позволит возложить решение проблемы на тех лиц, которые в большей степени способны ее решить. Проводя аналогии с иными сферами деятельности, это подобно тому, как решать проблему очистки загрязненного воздуха на заводе не путем выдачи

[1] *Templeton B.* The Best Way to End Spam.

индивидуальных масок каждому рабочему, а путем создания централизованной системы его очистки. В случае выявления провайдером факта массовой рассылки он будет иметь выбор: либо блокировать трафик, исходящий от его клиента (предварительно предусмотрев это в договоре с ним), либо принять на себя риск предъявления к нему иска со стороны потерпевшей стороны о возмещении убытков и, возможно, заранее установленной в законе компенсации, о целесообразности введения которой имеет смысл подумать[1].

Безотносительно к тому, будут ли имплементированы вышеуказанные положения, очевидно, что без международной кооперации в сфере противодействия спаму вряд ли будет возможно добиться значимых результатов, так как возможность спамеров спрятаться в недосягаемых юрисдикциях является одной из главных причин их безнаказанности, стимулирующей к дальнейшей деятельности. Другим вопросом является обеспечение не только юридической кооперации, но и технической, поскольку без модернизации технических стандартов распространения электронной почты вряд ли возможно решить проблему спама.

В свете приведенных аргументов можно сделать вывод о том, что в отсутствие мер экономического характера, направленных на увеличение издержек от распространения спама, дальнейшее ужесточение законодательства в области массовых рассылок сообщений рекламного характера вряд ли целесообразно. Ибо оно будет бить главным образом по добросовестным участникам рынка, а не по тем недобросовестным спамерам, которые являются источником основной части спама по всему миру. Участник рынка, который пытается воплотить в своей деятельности пожелания законодателей, несет риск наступления неблагоприятных последствий в случае неправильной с точки зрения правоприменителей интерпретации порой весьма неоднозначных положений законодательства. В отличие от него спамер, окопавшийся в иностранной юрисдикции и использующий различного рода технические средства и уловки для минимизации возможности его идентификации, в принципе не заботится о том, чтобы соответствовать требованиям какого-либо законодательства. Только комплексный экономический, технический и правовой подход может решить проблему спама с минимальными потерями для добросовестных субъектов электронной коммерции.

---

[1] *Soma J., Singer P., Hurd J.* Spam Still Pays: The Failure of the CAN-SPAM Act of 2003 and Proposed Legal Solutions. P. 186–193.

Глава 9. Персональные данные в сфере электронной коммерции

Любой интернет-магазин или иной веб-ресурс, который ориентирован на пользователя, будет так или иначе иметь дело с информацией, позволяющей его идентифицировать. Это может быть логин и пароль, адрес электронной почты, иные сведения, которые пользователь указывает о себе при регистрации на веб-сайте или оформлении заказа. В условиях высокой конкуренции, существующей в сети Интернет, а также дефиците внимания со стороны пользователей, обусловленной беспрецедентным многообразием информации, размещенной в ней, любой клиент, что называется, «на вес золота». В данном случае в качестве «золота» выступает информация о нем, которая может быть использована для различных коммерчески значимых целей (например, для адресной рекламы). Современные технологии сбора и обработки информации позволяют составлять достаточно детальные профайлы пользователей, которые содержат данные о предпочтениях и текущих потребностях отдельно взятого пользователя, его индивидуальных характеристиках и позволяют делать предположения о его финансовой состоятельности и платежеспособности. При составлении подобных профайлов могут активно использоваться данные, размещенные пользователем в социальных сетях, информация о нем, размещенная его друзьями в таких сетях, информация о сделанных им запросах в поисковых системах, посещенных сайтах, комментариях в форумах, и любое иное действие, совершенное им в сети Интернет. Очевидно, что все это создает уникальные возможности для субъектов электронной коммерции, как, впрочем, и традиционных офлайновых компаний, которыми они до этого не обладали: возможность вести «прицельный огонь» по пользователям, а также восполнить недостаток информации, необходимый для принятия коммерчески значимых решений в отношении конкретного клиента. Однако не менее очевидно и то, что сбор и последующее использование информации, связанное с личностью лица и отражающее его индивидуальные характеристики, неразрывно связаны со вторжением в его личную сферу, которое такое лицо, имея возможность, постаралось бы максимально минимизировать.

В качестве правового инструмента, направленного на поиск баланса между легитимным стремлением субъектов электронной коммерции к взаимодействию со своими контрагентами на условиях «индивидуального подхода» и стремлением последних к ограничению бесконтрольной циркуляции их личной информации в цифровой среде, выступает законодательство о персональных данных. Имеет смысл остановиться на рассмотрении его положений, учитывая, что с их действием приходится сталкиваться любому лицу, ведущему предпринимательскую деятельность в сети Интернет, заботящемуся о своей клиентской базе, равно как и любому пользователю, который делится своими данными с окружающим миром.

§ 1. Законодательство о персональных данных. Основные понятия и сфера действия

Законодательство о персональных данных появилось в 70-х гг. XX в. и представляет собой развитие в технологическую эпоху права на неприкосновенность личности. До появления информационных технологий сбор, обработка и хранение персональных данных были крайне дорогостоящим занятием как для компаний, так и для государства, что служило своего рода «естественным барьером» личного пространства физического лица[1]. Появление возможности автоматизированной обработки таких данных в значительной степени снизило данный барьер и обусловило появление альтернативного «правового барьера», который бы позволил защитить личное пространство физического лица.

Специальные положения, посвященные проблематике автоматизированной обработки персональных данных, сначала появились в Европе, впоследствии они распространились по всему миру. По состоянию на начало 2012 г. законы о персональных данных были приняты в 89 странах мира[2].

Основополагающим актом в данной сфере стала Конвенция о защите физических лиц при автоматизированной обработке персональных данных, принятая Советом Европы 28 января 1981 г., впоследствии дополненная протоколом по вопросам полномочий наблюдательных органов и трансграничной передачи данных. На основе положений данной Конвенции на национальном уровне страны Европы приня-

[1] *Войниканис Е.* Указ. соч. С. 199.

[2] *Greenleaf G.* Global Data Privacy Laws: 89 Countries, and Accelerating // Privacy Laws & Business International Report. No 115. February 2012; Queen Mary School of Law Legal Studies Research Paper No. 98/2012. http://ssrn.com/abstract=2000034

ли отдельные законы, посвященные регулированию персональных данных. Впоследствии национальное законодательство было гармонизировано рядом директив ЕС, в числе которых следует упомянуть Директиву № 95/46/ЕС от 24 октября 1995 г. о защите прав частных лиц применительно к обработке персональных данных и о свободном движении таких данных[1] и Директиву № 2002/58/ЕС от 31 июля 2002 г.[2], касающуюся использования персональных данных и защиты неприкосновенности частной жизни в сфере телекоммуникаций. Также немалую роль играет Директива № 2006/24/ЕС «О сохранении данных»[3], предусматривающая обязанности провайдеров телекоммуникационных услуг по сохранению данных о коммуникациях по телефону или электронной почте (время, место, продолжительность, личность участников) в течение срока от 6 месяцев до 2 лет. Целью Директивы является содействие в предупреждении, выявлении и расследовании «серьезных» преступлений, перечень которых конкретизируется в национальном законодательстве. Данная Директива не распространяется на гражданско-правовые и иные споры, но даже несмотря на весьма узкую сферу применения, вызвала немало споров и нареканий в Европе[4].

Указанные директивы были имплементированы в национальное законодательство государств – членов ЕС. Несмотря на то что в общем и целом национальные законы содержат схожие положения, по мере углубления в детали регулирования выявляются различия в подходах[5]. В настоящее время идет работа над унификацией европейского законодательства в этой области посредством введения Общего регламента о защите персональных данных (*General Data Protection Regulation, GDPR*), который помимо всего прочего учел бы произошедшие изменения в сфере компьютерных технологий, существенным образом повлиявших на процесс обработки данных (например, широкое

[1] Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

[2] Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector [as amended by Directive 2009/136/EC].

[3] Directive 2006/24/EC on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks.

[4] См. подробнее: *Loideain N.* The EC Data Retention Directive: Legal Implications for Privacy and Data Protection // Personal Data Privacy and Protection in a Surveillance Era: Technologies and Practices / ed. by C. Akrivopoulou and A. Psygkas. N.Y., 2011. P. 256 ff.

[5] Подробный компаративный анализ см.: Data Protection Laws in the EU. European Commission Working Paper. No 2. 20 January 2010 // http://ec.europa.eu/justice/policies/privacy/docs/studies/new_privacy_challenges/final_report_working_paper_2_en.pdf

распространение социальных сетей, облачных вычислений и т.п.)[1]. Наиболее важные новеллы проекта указанного регламента будут рассмотрены далее.

США, как ни странно, не могут похвастаться наличием единого и структурированного подхода к защите персональных данных (именуемых обычно *personal identifiable information*). Вопросы, связанные с регламентацией порядка использования таких данных, разбросаны по множеству актов, касающихся вопросов здравоохранения[2], проката видеофильмов[3], финансовых услуг[4], защиты данных автовладельцев[5], защиты персональных данных малолетних лиц в сети Интернет[6] и ряда иных тематических законов, принятых как на федеральном уровне, так и на уровне отдельных штатов[7]. Немалую роль играют и акты рекомендательного характера[8].

Как отмечается, причиной особого подхода США к вопросам регулирования персональных данных является отношение к ним как к составной части права на неприкосновенность частной жизни (*privacy*), которое в свою очередь рассматривается через призму свободы слова и права на невмешательство государства в частную жизнь[9]. Не последнюю роль в отсутствие целостного восприятия в США проблематики защиты персональных данных на законодательном уровне сыграла и вера в возможности саморегулирования и в то, что рынок «все расставит по местам». Федеральная торговая комиссия, которая длительное время осуществляла роль регулятора по вопросам использования персональных данных в сети Интернет, стимулировала компании к выработке политик конфиденциальности и использованию Принципов справедливых информационных практик (*Fair Information Practice*

[1] Proposal for a Regulation of the European Parliament and of the Council on on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation). Brussels. 25.01.2012. COM(2012) 11 Final // http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf

[2] The US Health Insurance Portability and Accountability Act of 1996.

[3] The US Video Privacy Protection Act of 1988.

[4] The US Financial Services Modernization Act of 1999.

[5] The US Drivers Privacy Protection Act of 1994.

[6] The Children's Online Privacy Protection Act of 1998.

[7] См., например: the California Online Privacy Protection Act of 2003 (OPPA); the Massachusetts General Law Chapter 93H & 201 CMR 17.00 Regulations of 2010.

[8] NIST Guide to Protecting the Confidentiality of Personally Identifiable Information (PII) NIST Special Publication 800-122. April 2010 // http://csrc.nist.gov/publications/nistpubs/800-122/sp800-122.pdf

[9] *Metille S.* Swiss Information Privacy Law and the Transborder Flow of Personal Data // Journal of International Commercial Law and Technology. No 8. 2013. P. 71.

Principles) для обеспечения информированности пользователя о судьбе его персональных данных[1].

Неудивительно, что в условиях столь «лоскутного» законодательства существует большой разнобой в дефинициях и подходах к персональным данным, в результате чего субъект не может предсказать заранее с высокой степенью достоверности, как его данные будут собираться и использоваться[2]. Как следствие, США не рассматривается в качестве страны, обеспечивающей надлежащий уровень защиты персональных данных, с точки зрения европейского законодательства, что потребовало выработки специальных принципов (*safe harbor*), присоединение к которым обеспечивает соответствующей американской компании статус обеспечивающей должный уровень защиты для целей европейского законодательства о защите персональных данных.

Очевидно, что в части законодательства о защите персональных данных США не являлись хорошим примером для подражания. К тому же в 2005 г. Россия ратифицировала Конвенцию Совета Европы о защите физических лиц при автоматизированной обработке персональных данных 1981 г.[3], поэтому вопроса о том, чьи правовые нормы взять в качестве источника вдохновения, не возникло. В результате был принят Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных» (далее – Закон о персональных данных).

Закон о персональных данных регулирует отношения, связанные с обработкой персональных данных, осуществляемой как государственными и муниципальными органами власти, так и юридическими и физическими лицами с использованием средств автоматизации, в том числе в информационно-телекоммуникационных сетях[4] (ст. 1).

---

[1] *Soma J. et al.* An Analysis of the Use of Bilateral Agreements Between Transnational Trading Groups: The U.S./EU E-Commerce Privacy Safe Harbor // Texas International Law Journal. No 39. 2004. P. 183–184.

[2] *Tennis B.* Privacy and Identity in a Networked World // Personal Data Privacy and Protection in a Surveillance Era: Technologies and Practices / ed. by C. Akrivopoulou and A. Psygkas. N.Y., 2011. P. 8.

[3] Федеральный закон от 19 декабря 2005 г. № 160-ФЗ «О ратификации Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных». Процесс ратификации был завершен 15 мая 2013 г. Конвенция вступила в силу в отношении России с 1 сентября 2013 г.

[4] Сфера действия Закона о персональных данных также охватывает отношения по обработке персональных данных без использования автоматизированных средств, если она соответствует характеру действий (операций), совершаемых с персональными данными с использованием средств автоматизации, т.е. позволяет осуществлять в соответствии с заданным алгоритмом поиск персональных данных, зафиксированных на материальном носителе и содержащихся в картотеках или иных систематизированных собраниях персональных данных, и (или) доступ к таким персональным данным. Однако

Поскольку, как следует из законодательной дефиниции, под автоматизированной обработкой понимается любая обработка персональных данных с помощью средств вычислительной техники, любые действия с персональными данными пользователей, осуществляемые в цифровой среде, будут охватываться понятием автоматизированной обработки. Те немногие исключения из сферы действия Закона (обработка персональных данных физическими лицами для личных и семейных нужд; для использования документов в соответствии с законодательством об архивном деле; обработка персональных данных, отнесенных к государственной тайне) вряд ли могут быть применимы в процессе осуществления предпринимательской деятельности в сети Интернет. Поэтому можно с уверенностью утверждать, что любая обработка персональных данных в сфере электронной коммерции потенциально подпадает под действие Закона о персональных данных.

При этом понятие «обработка персональных данных» включает в себя практически любое действие с ними, как то: сбор, запись, систематизация, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передача (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение. Подобный всеобъемлющий перечень не дает возможности представить себе действие, совершаемое с персональными данными, которое не являлось бы их обработкой.

Поэтому ключевым понятием, которое может повлиять на применимость Закона о персональных данных к тем или иным данным, получаемым от пользователя или связанным с ним, является само понятие персональных данных. В соответствии с законодательной дефиницией под ними понимается любая информация, относящаяся к прямо или косвенно к определенному или определяемому физическому лицу (субъекту персональных данных).

Первое, что необходимо отметить, – это то, что субъектами персональных данных могут выступать только физические лица. Контактные данные и реквизиты юридического лица, а также иные сведения, по которым можно его определить, не подпадают под понятие персональных данных.

Во-вторых, соответствующие сведения должны обладать определенным идентифицирующим потенциалом для того, чтобы признаваться персональными данными. Некоторые виды сведений являются уникальными в своем роде, что позволяет однозначно установить

данная сфера не представляет собой интереса в контексте проблематики электронной коммерции, поэтому не будет рассматриваться далее.

на их основе определенное физическое лицо – например: паспортные данные[1], ИНН, сведения паспорта транспортного средства.

Однако нередко данные могут быть отнесены к определенному индивиду только в сочетании с другими данными. Так, например, одной только фамилии или имени обычно недостаточно для идентификации физического лица, если они носят распространенный характер (скажем, Иванов Иван). Необходимо нечто большее, что бы позволило привязать их к конкретной личности (например, адрес проживания или места работы, возраст и т.п.).

Или иной пример. *IP*-адрес сам по себе не идентифицирует физическое лицо, выступая средством идентификации компьютерного устройства, подключенного к сети Интернет. Однако в сочетании с иными данными, например временем сеанса и данными *log*-файлов интернет-провайдера, он может служить способом идентификации пользователя в сети Интернет. То же самое можно сказать о сведениях о посещаемых веб-сайтов. Они потенциально могут характеризовать интересы пользователя, а следовательно, и его определенные индивидуальные характеристики, но статус персональных данных они обретут только в связке с дополнительными данными, позволяющими «привязать» их к определенной личности[2].

Следует иметь в виду, что дефиниция персональных данных включает в себя в том числе информацию, *косвенно* относящуюся к *определяемому* лицу. Если соответствующие фрагменты данных, из совокупности которых можно идентифицировать определенное лицо, находятся в распоряжении одного и того же лица (оператора), то каждый фрагмент

[1] Следует отметить, что существуют судебные решения, в которых серия и номер паспорта, по мнению суда, относятся не к личности гражданина, а к бланку документа, удостоверяющего его личность, вследствие чего такая информация не может быть отнесена к персональным данным См., например: определение Московского городского суда от 29 февраля 2012 г. № 33-6709; постановление Тринадцатого арбитражного апелляционного суда от 21 июня 2010 г. по делу № А56-4788/2010. Представляется, что такой подход не выдерживает никакой критики. Во-первых, он противоречит здравому смыслу: идентифицировав по номеру бланк документа, удостоверяющего личность, можно без труда определить личность, на имя которой этот бланк был выдан. Во-вторых, такой подход не соответствует дефиниции персональных данных, включающей в их состав информацию, в том числе и *косвенно* относящуюся к лицу. Для сравнения: в Латвии паспортные данные признаются персональными данными и требование работодателем копии паспорта у сотрудника является нарушением Закона о защите персональных данных физических лиц, за которое работодателю может грозить административный штраф до 10 000 латов // http://www.telegraf.lv/news/kopiya-pasporta-obernetsya-shtrafom

[2] *Малеина М.Н.* Право на тайну и неприкосновенность персональных данных // Журнал российского права. 2010. № 11.

таких данных подпадает под понятие «персональные данные»[1]. Если же такие фрагменты данных находятся во владении различных операторов, то говорить о том, что они являются персональными, вряд ли возможно: непонятно, как статистика посещения определенного веб-сайта, которой обладает провайдер хостинга, может иметь характер персональных данных без наличия дополнительных данных, позволяющих «привязать» данные посещения к конкретным пользователям, которыми обладает другое лицо – интернет-провайдер доступа. Нельзя отрицать возможную ценность соответствующих фрагментов информации самих по себе, но эта ценность не будет предопределена наличием у нее статуса персональных данных. Скорее данные фрагменты можно рассматривать в качестве своего рода обезличенных данных.

Представляется, что именно признание наличия подобного рода взаимосвязей между различного рода фрагментами информации, совокупность которых позволяет отнести ее к определенному физическому лицу, и послужила основанием для изменения законодательной дефиниции персональных данных. Ранее, до 27 июля 2011 г., она звучала иначе: «...любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация». Как видно, основным отличием современной формулировки является исключение из дефиниции перечня возможных видов персональных данных, что было компенсировано включением оговорки о том, что информация может относиться к субъекту прямо или косвенно. Представляется, что данный подход хотя и привносит дополнительную неопределенность, превращая вопрос о квалификации информации в качестве персональных данных в вопрос факта, зависящего от конкретных обстоятельств, но является более адекватным. Ведь очевидно, что сами по себе ни дата рождения, ни адрес, ни составляющие имени не имеют достаточных идентификационных характеристик для того, чтобы их безусловно считать персональными данными, как это следовало из ранее действовавшей дефиниции.

[1] Данного подхода придерживается зарубежная практика, и как представляется, он вполне применим и у нас, учитывая сходство дефиниций «персональные данные», используемых в России и в Европе. См., например: *Carey P.* Data Protection. A Practical Guide to UK and EU Law. Oxford University Press. 2004. P. 15; Data Protection Principles in the Personal Data (Privacy) Ordinance from the Privacy Commissioner's perspective (2nd Edition). Hong Kong, 2010. P. 21 // https://www.pcpd.org.hk/tc_chi/publications/files/Perspective_2nd.pdf

В-третьих, не имеет значения, соответствуют данные действительности или нет, являются они точными или полными, вымышленными или достоверными. Даже недостоверные или неточные сведения могут прямо или косвенно указывать на определенное лицо, что является достаточным основанием для признания их персональными данными[1]. Данный вывод следует не только из широко сформулированной дефиниции персональных данных, но и из предусмотренного в п. 1 ст. 14 Закона о персональных данных правомочия субъекта персональных данных требовать от оператора уточнения, блокирования или уничтожения неполных, устаревших или неточных персональных данных, что предполагает возможность существования сведений, обладающих статусом персональных данных, даже в случае, если они некорректно отражают действительное положение вещей.

На практике нередко возникает вопрос, можно ли отнести адрес электронной почты к категории персональных данных? Представляется, что ответ на данный вопрос будет зависеть от характера обозначения, использованного в адресе электронной почты, а также принадлежности такого почтового ящика.

Если почтовый ящик является корпоративным и его название включает в себя фамилию и имя его владельца, то совокупность указанных данных вполне позволяет определить его владельца – физическое лицо.

Напротив, если почтовый ящик зарегистрирован на публичном сервисе электронной почты, где в отличие от корпоративной почты получить адрес может любой желающий, условия признания адреса такого почтового ящика персональными данными должны быть более жесткими. Если имя такого почтового ящика включает в себя достаточно идентификационных сведений (например, фамилию и инициалы лица с указанием года рождения), то вряд ли есть основания не считать такой электронный адрес разновидностью персональных данных. С другой стороны, если название такого почтового ящика не содержит в себе сведений, которые могли бы быть квалифицированы в качестве персональных данных, то такой электронный адрес может быть отнесен к категории персональных данных только при наличии дополнительных сведений, позволяющих его привязать к определенному лицу. Например, если пользователь при регистрации на веб-сайте или оформлении заказа указал свой почтовый адрес вроде *powerboy1234@mail.ru*, такой адрес должен считаться персональными данными, поскольку в распоряжении оператора имеются иные сведения, позволя-

[1] Opinion 4/2007 Article 29 Data Protection Working Party // http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_en.pdf

ющие определить физическое лицо. При этом, как отмечалось выше, достоверность таких сведений не имеет значения: лицо может указать вымышленное имя и иные данные, что не лишает такие данные характера персональных. В связи с этим на практике субъектам электронной коммерции целесообразно придерживаться строгого подхода к природе адресов электронной почты: велика вероятность, что база данных таких адресов будет включать как адреса, которые вполне точно могут идентифицировать определенное физическое лицо, так и анонимные адреса. Однако наличия в базе данных хотя бы одного электронного адреса, подпадающего под дефиницию персональных данных, достаточно для применения соответствующих положений законодательства о персональных данных ко всей базе данных[1].

В связи с возможностью квалификации адреса электронной почты в качестве персональных данных целесообразно достаточно осторожно подходить к массовым рассылкам сообщений, на копии которых указано множество физических лиц, а также к использованию функций «переслать» и «ответить всем» с сохранением указанных лиц в рассылке, поскольку подобные действия формально подпадают под понятие обработки персональных данных, которая должна осуществляться с соблюдением соответствующих требований. Гораздо разумнее воспользоваться функцией *Blind copy*.

Наконец, возникает вопрос, должно ли физическое лицо, к которому относятся сведения, представляющие собой «любую информацию, относящуюся к прямо или косвенно определенному или определяемому физическому лицу», являться живым? Некоторые зарубежные акты о защите персональных данных, например Великобритании[2], содержат указание на то, что соответствующие сведения могут относиться только к *living individual*, т.е. к живущему физическому лицу. Если лицо является умершим, то данные о нем не могут относиться к категории персональных данных[3]. Российский Закон о персональных данных не делает никаких оговорок относительно статуса физического лица в дефиниции персональных данных, однако его положения ст. 9 («в случае смерти субъекта персональных данных согласие на обработку его персональных данных дают наследники субъекта персональных данных, если такое согласие не было дано субъектом персональных данных при его жизни»)

[1] *Carey P.* Op. cit. P. 233.

[2] UK Data Protection Act 1998. Article 1 (1).

[3] § 2.2.2. Data Protection Act 1998: Legal Guidance. Version 1. 2001 // http://www.ico.org.uk/upload/documents/library/data_protection/detailed_specialist_guides/data_protection_act_legal_guidance.pdf

позволяют сделать вывод о том, что информация об умершем лице может являться персональными данными. Правда, Закон о персональных данных не содержит специальных положений о том, что наследники могут требовать удаления или блокировки доступа к персональным данным умершего. В то же время на практике нередко возникают вопросы о судьбе профайлов умерших пользователей в социальных сетях. Очевидно, что в ряде случаев наследники и иные близкие родственники предпочли бы удалить такой аккаунт. Автору известно немало случаев, когда продолжение существования аккаунта в социальных сетях после смерти его владельца причиняло боль его близким. Особенно это касается случаев, когда на стене такого аккаунта начинается обсуждение обстоятельств смерти, хамство или злые шутки на сей счет.

Представляется, что на такие случаи за наследниками должно быть предусмотрено право требования удаления профайлов умерших пользователей. В связи с этим сложно согласиться с мнением отдельных авторов, что соответствующие интересы могут быть обеспечены введением в Закон о персональных данных положения о том, что «...в случае, если незаконная обработка персональных данных лица после его смерти привела к причинению морального вреда его наследникам, в том числе посредством умаления чести, достоинства или деловой репутации, его компенсация производится в порядке, предусмотренном гражданским законодательством»[1]. Во-первых, не всегда можно говорить об умалении чести и достоинства во всех случаях, когда близкие хотят удаления из Интернета персональных данных умершего лица. Во-вторых, компенсация как таковая не способна удовлетворить интерес близких в таких случаях, да и размеры морального вреда, обычно взыскиваемые российскими судами, являются скорее издевательством, чем компенсацией как таковой, и сами по себе способны причинять моральный вред.

§ 2. Требования к обработке персональных данных

Если те или иные сведения подпадают под понятие персональных данных, их обработка должна осуществляться в соответствии с установленными требованиями. Лицом, ответственным за обеспечение такого соответствия, является оператор. Под оператором (в англоязычной терминологии – *data controller*) понимается любое лицо, которое «самостоятельно или совместно с другими лицами организует и (или) осуществляет обработку персональных данных, а также определяет

[1] *Кучеренко А.В.* Особенности обработки персональных данных лица в случае его смерти // Информационное право. 2011. № 2.

цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными». Иными словами, под оператором понимается лицо, которое использует персональные данные других лиц для достижения определенных целей, которое оно само и определяет.

От оператора следует отличать «лицо, которое осуществляет обработку персональных данных по поручению оператора» (в англоязычной терминологии – *data processor*). Учитывая, что используемая в законе терминология весьма громоздка, для краткости такое лицо будет далее именоваться обработчиком[1]. В качестве лиц, выступающих обработчиками персональных данных, можно указать, в частности, провайдеров облачных сервисов; организации, осуществляющие расчеты заработной платы на условиях аутсорсинга (*payroll companies*); организации, в чьих дата-центрах размещаются серверы оператора персональных данных (*co-location*)[2]. Отличительной чертой статуса обработчика персональных данных является то, что *он не определяет цели обработки* персональных данных – они задаются оператором. Закон о персональных данных указывает, что в поручении оператора обработчику должны быть определены перечень действий (операций) с персональными данными, которые будут совершаться обработчиком, цели обработки, а также должна быть установлена обязанность обработчика соблюдать конфиденциальность персональных данных и обеспечивать их безопасность с указанием требований к защите обрабатываемых персональных данных в соответствии со ст. 19 Закона о персональных данных (ч. 3 ст. 6). Из текста данного положения можно сделать вывод, что наличие такого поручения является необходимым условием получения лицом статуса обработчика. При этом Закон никак не конкретизирует форму и характер такого поручения: представляет оно собой отдельный договор[3] или является

[1] В постановлении Правительства РФ от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» такое лицо именуется «уполномоченное лицо», однако вряд ли данный термин можно считать удачным в силу весьма общего характера данного термина, а также неудобства его использования при рассмотрении отдельных проблем защиты персональных данных. Так, например, сразу возникают вопросы: кем такое лицо уполномочено, на что уполномочено? Ответ на них приводят к той же самой громоздкой формулировке, от которой хотелось уйти.

[2] В данном случае можно говорить о том, что они осуществляют обработку персональных данных в форме их хранения.

[3] Даже несмотря на использование законодателем слова «поручение», такое соглашение не может быть квалифицировано в качестве договора поручения, поскольку предметом такого договора является совершение юридических действий (ст. 971 ГК РФ),

дополнительным условием в основном договоре. Представляется, что возможны оба варианта, причем первый вариант может быть на практике иногда удобнее, так как не предполагает необходимости внесения изменений в типовые формы договоров, используемых обработчиком

Отличительной особенностью статуса обработчика является то, что он не имеет обязанностей непосредственно перед субъектом персональных данных, ответственность за его действия несет непосредственно оператор (ч. 5 ст. 6 Закона о персональных данных). Иными словами, субъект персональных данных не может предъявлять свои требования напрямую к обработчику, такие требования должны быть предъявлены непосредственно к оператору. Однако не следует забывать, что одно и то же лицо может выступать по отношению к различным персональным данным и в роли оператора, и в роли лица, осуществляющего обработку персональных данных по поручению оператора, в связи с чем оно все равно будет вынуждено соблюдать все основные положения законодательства о персональных данных.

Основными требованиями, предъявляемыми Законом к обработке персональных данных, являются:

1) наличие законного основания для такой обработки;

2) добросовестный характер такой обработки;

3) принятие организационно-технических мер для выполнения обязанностей оператора и защиты персональных данных;

4) соблюдение особых требований к трансграничной передаче персональных данных;

5) в подлежащих случаях – направление уведомления в уполномоченный орган об обработке персональных данных.

Рассмотрим подробнее указанные требования.

2.1. Наличие законного основания для обработки персональных данных

Одним из главных требований, предъявляемых к обработке персональных данных, является наличие законного основания для их обработки. Исчерпывающий перечень таких оснований предусмотрен в п. 1 ст. 6 Закона о персональных данных. К ним относится:

1) наличие согласия субъекта персональных данных на такую обработку;

в то время как предметом поручения оператора является совершение преимущественно фактических действий. Скорее всего, данное поручение можно рассматривать в качестве соглашения особого рода (*sui generis*), существенные условия которого указаны в ч. 3 ст. 6 Закона о персональных данных.

2) необходимость такой обработки персональных данных для достижения целей, предусмотренных Законом, а также для осуществления и выполнения возложенных законодательством Российской Федерации на оператора функций, полномочий и обязанностей[1];

3) необходимость такой обработки персональных данных для осуществления правосудия, исполнения судебного акта, акта другого органа или должностного лица, подлежащих исполнению в порядке исполнительного производства;

4) необходимость такой обработки персональных данных для исполнения полномочий государственных и муниципальных органов на едином портале государственных и муниципальных услуг;

5) необходимость такой обработки персональных данных для исполнения договора, стороной которого либо выгодоприобретателем или поручителем по которому является субъект персональных данных, а также для заключения договора по инициативе субъекта персональных данных или договора, по которому субъект персональных данных будет являться выгодоприобретателем или поручителем;

6) необходимость такой обработки персональных данных для защиты жизни, здоровья или иных жизненно важных интересов субъекта персональных данных, если получение согласия субъекта персональных данных невозможно;

7) необходимость такой обработки персональных данных для осуществления прав и законных интересов оператора или третьих лиц либо для достижения общественно значимых целей при условии, что при этом не нарушаются права и свободы субъекта персональных данных;

8) необходимость такой обработки персональных данных для осуществления профессиональной деятельности журналиста и (или) законной деятельности средства массовой информации либо научной, литературной или иной творческой деятельности при условии, что при этом не нарушаются права и законные интересы субъекта персональных данных;

9) обработка персональных данных осуществляется в статистических или иных исследовательских целях, за исключением целей, указанных в ст. 15 Закона о персональных данных, при условии обязательного обезличивания персональных данных;

---

[1] Следует подчеркнуть, что в данном случае речь идет именно о законодательстве РФ, а не о законодательстве в принципе. Поэтому иностранным компаниям, ведущим свою деятельность на территории России, не получится ссылаться на данное основание в тех случаях, когда они осуществляют обработку в рамках предписаний своего «родного» законодательства.

10) общедоступный характер персональных данных вследствие предоставления доступа к ним неограниченному кругу лиц субъектом персональных данных либо по его просьбе иным лицом;

11) осуществление обработки персональных данных, подлежащих опубликованию или обязательному раскрытию в соответствии с Законом.

В сфере электронной коммерции наибольшую актуальность представляют основания, указанные в п. 1, 5 и 10. Рассмотрим их подробнее.

Согласие субъекта персональных данных является одним из основных способов придания обработке персональных данных законного характера. Такое согласие в соответствии с ч. 1 ст. 9 Закона о персональных данных должно быть «конкретным, информированным и сознательным». Согласие субъекта персональных данных на их обработку может быть дано по общему правилу в любой форме, позволяющей подтвердить факт его получения. Правда, оператор должен быть готов предоставить доказательства наличия такого согласия, что заставляет искать компромисс между свободой формы и ее надежностью с точки зрения возможности последующего доказывания факта дачи согласия, предоставленного в такой форме. Очевидно, что устная форма создает немало сложностей в процессе доказывания оператором факта дачи согласия субъектом персональных данных. К тому же, если персональные данные подпадают под понятие специальных или биометрических, необходимо оформление согласия в письменной форме, с обеспечением наличия в нем определенных реквизитов.

Важно подчеркнуть, что отсутствие возражений субъекта персональных данных на производящуюся оператором обработку его персональных данных не является согласием, так как не носит конкретного характера[1]. Молчание вообще, как известно, не является (вопреки распространенной поговорке) знаком согласия в праве. А вот предоставление самим субъектом персональных данных определенных сведений о себе может в некоторых случаях быть расценено как выражение согласия на их обработку в конклюдентной форме[2].

---

[1] Не менее интересным является вопрос о соответствии требованиям конкретности и сознательности согласия на обработку персональных данных наличия на веб-сайте или техническом устройстве определенных настроек конфиденциальности, особенно если они носят предустановленный характер. Представляется, что о наличии согласия если и можно говорить в таких случаях, то только в том случае, когда имеются доказательства, что соответствующие настройки были сделаны самим субъектом персональных данных, а не представляли собой состояние «по умолчанию».

[2] См., например: решение Сысертского районного суда Свердловской области от 14 мая 2012 г. № 2-526/2012 (в данном случае подача субъектом персональных данных письменного обращения, в котором содержались его персональные данные, была

В сфере электронной коммерции получила широкое распространение практика дачи согласия на обработку персональных данных путем проставления «галочки» в соответствующем поле на экране при оформлении заказа или регистрации на веб-сайте. В принципе, нет оснований считать недействительным такое согласие при условии, что оно было информированным и сознательным[1]. Другое дело, что необходимо быть готовым доказать не только факт дачи такого согласия, но и факт дачи согласия конкретным лицом. Как вариант можно отражать факт его наличия в электронном письме, направляемом пользователю в подтверждение произведенной регистрации или размещенного заказа, копия которого остается у оператора. Хотя, конечно, в случае возникновения споров относительно наличия или отсутствия факта дачи такого согласия и оспаривания аутентичности содержания предоставленного оператором электронного письма шансы на успешное доказывание факта дачи согласия на обработку персональных данных будут невелики[2]. Факт дачи согласия определенным лицом в отсутствие ЭЦП может быть доказан только косвенными доказательствами, например фактом использования в качестве средства платежа банковской карты, принадлежащей субъекту персональных данных.

К тому же необходимо учитывать судебную практику по вопросам включения условия о даче согласия на обработку персональных данных в договоры присоединения. Так, известны случаи, когда суд не признавал наличие согласия на обработку персональных данных, даже несмотря на то, что соответствующее условие было включено в такой договор. По мнению суда, у субъекта персональных данных в таких случаях отсутствовал выбор, поскольку единственной возможностью не давать такое согласие выражалось в отказе от заключения договора[3].

признана судом конклюдентной формой выражения согласия на их последующую обработку адресатом).

[1] *Зоркольцев Р.Д.* Персональные данные, получаемые через Интернет: практические вопросы // СПС «КонсультантПлюс». 2012.

[2] Справедливости ради надо отметить, что дача согласия на обработку персональных данных в электронной форме носит проблемный характер не только для оператора, но и для самого субъекта персональных данных, поскольку существенно затрудняет возможность последующего отзыва такого согласия и в особенности защиту своих прав в случае отказа оператора удовлетворить поступившее заявление об отзыве.

[3] См.: постановления Семнадцатого арбитражного апелляционного суда от 12 апреля 2013 г. № 17АП-2955/2013-АК по делу № А60-39156/2012, оставленное без изменений постановлением ФАС Уральского округа от 29 июля 2013 г. № Ф09-5767/13; Восьмого арбитражного апелляционного суда от 18 марта 2013 г. по делу № А70-8957/2012; Восемнадцатого арбитражного апелляционного суда от 28 мая 2013 г. № 18АП-3864/2013 по делу № А47-13986/2012.

Также рискованной является практика включения условия о согласии на обработку персональных данных не в текст документа, против которого пользователь выражает свое согласие, а в текст иного документа, к которому содержится отсылка в первом. Учитывая малую вероятность того, что пользователь ознакомится с его содержимым, говорить о наличии информированного и сознательного согласия в таких случаях вряд ли возможно, о чем свидетельствует и судебная практика[1].

В свете вышеизложенного вдвойне сомнительным является включение условия о даче субъектом персональных данных согласия на обработку его персональных данных в текст *browse-wrap*-соглашений, например, различного рода *Privacy policy*, с которыми субъект обычно не знакомится. Говорить о наличии конкретного, информированного и сознательного согласия в таких случаях нельзя. Что, однако, не умаляет роли данных документов, о которой будет сказано далее.

Особые требования к даче согласия на обработку персональных данных предусмотрены в отношении так называемых специальных категорий персональных данных, которые в доктрине иногда также именуются как «чувствительные» данные. К ним относятся данные о расовой, национальной принадлежности, политических взглядах, религиозных или философских убеждениях, состоянии здоровья, интимной жизни. Для обработки таких данных согласие субъекта должно быть выражено в письменной форме, которая должна включать в себя, в частности:

1) фамилию, имя, отчество, адрес субъекта персональных данных, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе;

2) фамилию, имя, отчество, адрес представителя субъекта персональных данных, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе, реквизиты доверенности или иного документа, подтверждающего полномочия этого представителя (при получении согласия от представителя субъекта персональных данных);

3) наименование или фамилию, имя, отчество и адрес оператора, получающего согласие субъекта персональных данных;

4) цель обработки персональных данных;

5) перечень персональных данных, на обработку которых дается согласие субъекта персональных данных;

[1] См., например: постановление Второго арбитражного апелляционного суда от 16 июля 2012 г. по делу № А31-3106/2012.

6) наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению оператора, если обработка будет поручена такому лицу;

7) перечень действий с персональными данными, на совершение которых дается согласие, общее описание используемых оператором способов обработки персональных данных;

8) срок, в течение которого действует согласие субъекта персональных данных, а также способ его отзыва, если иное не установлено Законом;

9) подпись субъекта персональных данных.

Закон о персональных данных содержит перечень случаев, при которых обработка «чувствительных» данных возможна и без согласия их субъекта (ч. 2 ст. 10 Закона о персональных данных), однако они малоприменимы к сфере электронной коммерции. Видимо, предполагается, что обладание указанными данными не является необходимым для осуществления предпринимательской или иной экономической деятельности, что в целом можно признать обоснованным.

В свете вышеизложенных положений, особенно касающихся повышенных требований к форме дачи согласия на обработку «чувствительных» персональных данных, в зоне риска оказываются различного рода тематические форумы (религиозной, политической, философской направленности, в области здравоохранения и пр.), которые предполагают предоставление обширных данных о пользователях при регистрации, совокупное обладание такими данными позволяет потенциально определить личность такого пользователя. В совокупности с содержанием его высказываний на форуме такие регистрационные данные позволяют приписать такому пользователю наличие определенных убеждений и качеств, сведения о которых являются специальной категорией персональных данных. Разумеется, ни один из владельцев подобных ресурсов не выполняет вышеуказанные требования Закона, являясь при этом вполне полноценным оператором персональных данных. Для минимизации риска привлечения к ответственности за несоответствие требованиям Закона можно посоветовать максимально минимизировать перечень сведений, собираемых в процессе регистрации на таких ресурсах, для того чтобы они обладали минимальным идентифицирующим потенциалом, тем самым поддерживая максимально анонимный статус участников подобного рода форумов и информационных ресурсов.

В качестве примера актуальности вопросов, связанных с размещением «чувствительных» персональных данных на различных

веб-ресурсах, в том числе и личного характера, можно привести дело *Lindqvist*, рассмотренное Европейским судом[1]. В решении по данному делу суд признал нарушением законодательства о персональных данных действия г-жи Линдквист, разместившей на своем личном веб-сайте информацию об именах и телефонах своих коллег и в особенности – «чувствительных» персональных данных, в частности о том, что одна из них повредила ногу и работает неполный день. При этом Суд особо подчеркнул, что предусмотренное в Директиве № 95/46/ЕС «О персональных данных» положение о ее нераспространении к случаям обработки персональных данных физическим лицом для личных нужд не распространяется на обработку персональных данных в виде их размещения на веб-сайте в сети Интернет, доступном неопределенному кругу лиц. Указанная позиция Европейского суда вполне актуальна и для России, принимая во внимание схожесть российского и европейского законодательства по данной проблематике.

Если же пользователь форума сам указал в своем профиле свои персональные данные, в силу чего его высказывания, носящие политический, религиозный или иной характер, могут быть отнесены к нему, соответствующие сведения могут быть квалифицированы в качестве общедоступных. В таком случае специального согласия на их обработку не требуется, она допустима в силу Закона (п. 2 ч. 2 ст. 10 Закона о персональных данных).

Сложности, связанные с получением согласия субъекта персональных данных на их обработку, в определенной степени компенсируются наличием в Законе специальных положений, позволяющих производить обработку и в отсутствие такого согласия. Указанные положения приобретают особую актуальность в свете наличия у субъекта персональных данных безусловного права в любой момент отозвать ранее данное согласие[2]. В таком случае оператор вправе продолжить их обработку только при наличии иных оснований, предусмотренных Законом.

К числу таких оснований относится положение о допустимости обработки персональных данных для целей заключения договора по инициативе субъекта персональных данных либо для исполнения договора, стороной (выгодоприобретателем, поручителем) которого

[1] ECJ Case C-101/01. 06.11.2003.

[2] Данное право закрепляется императивной нормой, что обусловливает недействительность различного рода ограничений, которые пытаются наложить на субъекта персональных данных в договорном порядке, включая условия, запрещающие отзыв персональных данных в течение определенного периода, и т.п.

является субъект персональных данных (п. 5 ч. 1 ст. 6 Закона о персональных данных). Понятие «договор» в данном случае охватывает не только гражданско-правовые, но и трудовые договоры[1].

Следует отметить, что судебная практика достаточно ограничительно толкует указанное положение. Речь идет именно об исполнении договора, стороной (выгодоприобретателем, поручителем) которого является субъект персональных данных, но не о вспомогательных договорах, заключение которых может потребоваться для исполнения основного договора с субъектом персональных данных. В частности, данное основание не было признано применимым к случаям передачи персональных данных субъекта персональных данных, выступающего заемщиком по кредитному договору, коллекторскому агентству, с которым кредитор заключил договор о взыскании задолженности по кредитному договору[2]. В данном случае первостепенной целью обработки персональных данных заемщика агентом является надлежащее исполнение условий агентского договора, стороной которого субъект персональных данных не является. Поэтому нельзя говорить о тождественности целей обработки персональных данных по основному договору и агентскому, несмотря на всю взаимосвязь между ними[3].

Представляется, что данный принцип применим и к иным случаям, когда оператор заключает с третьими лицами договоры, необходимые для исполнения договора, заключенного между оператором и субъектом персональных данных, в частности: субподрядные договоры, лицензионные договоры с правообладателями и пр. Для передачи персональных данных таким третьим лицам формально необходимо информированное согласие субъекта персональных данных.

Наконец, необходимо сказать несколько слов о так называемых общедоступных персональных данных, которые могут обрабатываться операторами без получения согласия их субъекта (п. 10 ч. 1 ст. 6 Закона о персональных данных). Речь идет о тех данных, к которым субъектом персональных данных либо по его просьбе иным лицом

---

[1] См. п. 6 письма ФНП от 23 декабря 2011 г. № 2515/07-17 «О применении ряда положений Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных»».

[2] Постановление ФАС Западно-Сибирского округа от 20 марта 2013 г. по делу № А27-13226/2012; апелляционное определение Ярославского областного суда от 5 марта 2012 г. по делу № 33-939/2012; кассационное определение Оренбургского областного суда от 8 февраля 2012 г. по делу № 33-805/2012. Противоположный подход см.: постановление Тринадцатого арбитражного апелляционного суда от 29 марта 2013 г. по делу № А21-10205/2012.

[3] *Анохин Д.А.* Возможность обработки персональных данных субъекта-должника без его согласия // Банковское право. 2012. № 6.

был предоставлен доступ неограниченному кругу лиц. Статья 8 Закона о персональных данных содержит определенное регулирование, посвященное источникам таких общедоступных персональных данных. Она предусматривает, что в общедоступные источники персональных данных с письменного согласия субъекта персональных данных могут включаться его фамилия, имя, отчество, год и место рождения, адрес, абонентский номер, сведения о профессии и иные персональные данные, сообщаемые субъектом персональных данных. В качестве примеров таких источников в данной статье приведены справочники и адресные книги. Однако ничто не мешает рассматривать в качестве общедоступных источников и различного рода веб-сайты в сети Интернет, в том числе социальные сети, которые являются в настоящее время основным источником сведений о физических лицах, использованием которых не гнушаются даже судебные приставы[1]. Правда, говорить об общедоступном характере персональных данных, размещенных в социальных сетях, можно только в том случае, если их доступность не ограничена настройками приватности. Другим примером общедоступных персональных данных в сети Интернет являются сертификаты ключей проверки электронной подписи, которые в силу своего существа не могут относиться к иной категории персональных данных.

Закон о персональных данных исходит из возможности изменения субъектом статуса общедоступности персональных данных. Предполагается, что поскольку они приобретают такой статус лишь в результате волеизъявления субъекта персональных данных, то в результате волеизъявления их обладателя они могут и утратить такой статус. Закон предусматривает право субъекта персональных данных потребовать в любой момент исключения персональных данных из общедоступных источников (ч. 2 ст. 8 Закона о персональных данных). Правда, применительно к общедоступным данным, размещенным в сети Интернет, данная норма носит преимущественно декларативный характер, поскольку даже в случае их оперативного исключения с соответствующего ресурса нет никаких гарантий, что никакое другое лицо не осуществляет их обработку. Найти всех таких лиц и повлиять на них практически невозможно. Поэтому лицо, размещающее свои персональные данные в социальных сетях и на иных веб-сайтах в режиме, предполагающем неограниченный доступ к ним, должно отдавать себе отчет, что с этого момента оно никак не может повлиять на их дальнейшее исполь-

[1] См.: Методические рекомендации по использованию сети Интернет в целях поиска информации о должниках и их имуществе, утв. ФССП России от 30 ноября 2010 г. № 02-7 // СПС «КонсультантПлюс».

зование, которое становится фактически бесконтрольным. Однако и потенциальные операторы таких данных также оказываются не в лучшем положении. Поскольку легитимная обработка общедоступных персональных данных возможна только в том случае, когда они были сделаны таковыми самим субъектом персональных данных или с его согласия, то размещение на общедоступных интернет-ресурсах персональных данных определенного лица без его согласия не придает их последующей обработке законного характера.

Систематическое толкование положений Закона о персональных данных позволяет сделать вывод о том, что реализация субъектом персональных данных права исключения его персональных данных из общедоступных источников невозможна в случаях, когда оператор таких данных имеет право их обработки в силу Закона (например, когда персональные данные сотрудников компании размещаются на официальном веб-сайте компании). Несмотря на то что можно говорить о таком сайте как об источнике общедоступной информации, подпадающем под действие ст. 8 Закона о персональных данных, обработка персональных данных в таком случае осуществляется во исполнение существующего трудового договора и согласия субъекта персональных данных на их обработку не требуется. А раз не требуется волеизъявления на инициацию обработки персональных данных, оно не имеет значения и для определения их дальнейшей судьбы, пока сохраняется основание для их законной обработки оператором (трудовые отношения). Однако это справедливо лишь в случае соответствия такой обработки принципам, указанным в ст. 5 Закона о персональных данных (см. далее), и не лишает субъекта персональных данных всех остальных прав, предусмотренных законодательством о персональных данных, в частности права требовать исправления некорректных данных.

2.2. Добросовестный характер обработки персональных данных

Одного только наличия законного основания для обработки персональных данных недостаточно для того, чтобы оператор мог испытать чувство удовлетворения от обеспечения соответствия его деятельности требованиям законодательства о персональных данных. Необходимо, чтобы обработка персональных данных осуществлялась в соответствии с принципами, изложенными в ст. 5 Закона о персональных данных, суть которых можно свести к обеспечению добросовестности и прозрачности такой обработки. Таких принципов семь.

1. Обработка персональных данных должна осуществляться на законной и справедливой основе.

2. Обработка персональных данных должна ограничиваться достижением конкретных, заранее определенных и законных целей. Не допускается обработка персональных данных, несовместимая с целями сбора персональных данных.

3. Не допускается объединение баз данных, содержащих персональные данные, обработка которых осуществляется в целях, несовместимых между собой.

4. Обработке подлежат только персональные данные, которые отвечают целям их обработки.

5. Содержание и объем обрабатываемых персональных данных должны соответствовать заявленным целям обработки. Обрабатываемые персональные данные не должны быть избыточными по отношению к заявленным целям их обработки.

6. При обработке персональных данных должны быть обеспечены точность персональных данных, их достаточность, а в необходимых случаях и актуальность по отношению к целям обработки персональных данных. Оператор должен принимать необходимые меры либо обеспечивать их принятие по удалению или уточнению неполных или неточных данных.

7. Хранение персональных данных должно осуществляться в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели обработки персональных данных, если срок хранения персональных данных не установлен федеральным законом, договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных. Обрабатываемые персональные данные подлежат уничтожению либо обезличиванию по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом.

В большинстве своем данные принципы скопированы с положений зарубежных актов. Основным источником вдохновения выступила, безусловно, Директива № 95/46/ЕС «О персональных данных», ст. 6 которой содержит схожие принципы. Отдельные законы, имплементирующие положения данной Директивы, даже содержат в качестве приложения перечень принципов обработки данных и их законодательную интерпретацию[1].

Анализ содержания вышеуказанных принципов позволяет сделать вывод, что они направлены преимущественно на обеспечение права субъекта персональных данных на информацию о том, как используются его персональные данные, что, в частности, необходимо

[1] См., например: Schedule 1, UK Data Protection Act 1998.

для обеспечения возможности предоставления ему информированного, конкретного и сознательного согласия на обработку своих персональных данных и влияния на процесс их обработки. Соответственно добросовестная обработка персональных данных оператором предполагает следующее:

1) предоставление субъекту персональных данных информации о конкретно сформулированной цели обработки, которая на практике не должна выходить за рамки такой цели;

2) отсутствие чрезмерности: объем и содержание обрабатываемых персональных данных должны быть минимально необходимыми для достижения поставленной цели и не быть более того, а по достижении такой цели – удалены;

3) субъекту персональных данных предоставлена реальная возможность влияния на процесс их обработки, в частности возможность требования их уточнения, дополнения, а в некоторых случаях – удаления.

Указанные принципы находят свою конкретизацию в ряде положений Закона о персональных данных. В частности, в нормах, регламентирующих важнейшее право субъекта персональных данных – право на доступ к обрабатываемым персональным данным, порядок реализации которого предусмотрен в ст. 14. На основании запроса субъекта персональных данных оператор должен в доступной форме предоставить ему следующие сведения:

1) подтверждение факта обработки персональных данных оператором;

2) правовые основания и цели обработки персональных данных;

3) цели и применяемые оператором способы обработки персональных данных;

4) наименование и местонахождение оператора, сведения о лицах (за исключением работников оператора), которые имеют доступ к персональным данным или которым могут быть раскрыты персональные данные на основании договора с оператором или на основании федерального закона;

5) обрабатываемые персональные данные, относящиеся к соответствующему субъекту персональных данных, источник их получения, если иной порядок представления таких данных не предусмотрен федеральным законом;

6) сроки обработки персональных данных, в том числе сроки их хранения;

7) порядок осуществления субъектом персональных данных прав, предусмотренных Законом о персональных данных;

8) информацию об осуществленной или о предполагаемой трансграничной передаче данных;

9) наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению оператора, если обработка поручена или будет поручена такому лицу;

10) иные сведения, предусмотренные Законом.

Особые информационные обязанности предусмотрены для оператора, который получил персональные данные не от субъекта персональных данных. В таком случае оператор, не дожидаясь запроса, до начала обработки таких персональных данных обязан предоставить субъекту персональных данных следующую информацию:

1) наименование либо фамилию, имя, отчество и адрес оператора (его представителя);

2) цель обработки персональных данных и ее правовое основание;

3) предполагаемые пользователи персональных данных;

4) установленные Законом права субъекта персональных данных;

5) источник получения персональных данных.

В ч. 4 ст. 18 Закона о персональных данных предусмотрены исключения из данной достаточно обременительной обязанности. К их числу относятся случаи уведомления субъекта о такой обработке «своим» оператором, которое может быть сделано в существующем между ними договоре, политике конфиденциальности или в индивидуальном порядке. В идеале данное исключение должно стимулировать операторов к максимальной прозрачности в части предоставления субъектам персональных данных информации об иных лицах, которые могут обрабатывать их данные, поскольку неисполнение этой обязанности будет возлагать дополнительные обременения на их контрагентов, чему те будут явно не рады. Другие исключения во многом повторяют перечень случаев, при которых допустима обработка персональных данных без согласия их субъекта (наличие связи с договором, стороной которого является такой субъект; общедоступный характер персональных данных; получение данных на основании Закона; осуществление такой обработки для статистических или иных исследовательских целей и некоторые другие.)

Реализация права субъекта персональных данных на доступ к обрабатываемым персональным данным является условием для реализации другого условия добросовестности их обработки – предоставления ему реальной возможности влияния на такую обработку[1]. В соответствии

[1] College van burgemeester en wethouders van Rotterdam v. M.E.E. Rijkeboer. ECJ. Case C553/07. 07.05.2009.

со ч. 1 ст. 14 Закона о персональных данных субъект персональных данных вправе требовать от оператора уточнения его персональных данных, их блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные Законом меры по защите своих прав.

На практике, к сожалению, добросовестная обработка персональных данных является скорее исключением, нежели правилом. Цели обработки формулируются весьма широко, то что называется на все случаи жизни; формы, заполняемые субъектами персональных данных, содержат в себе данные, которые являются чрезмерными; информация, предусмотренная Законом, редко предоставляется в объеме, предусмотренном Законом, если вообще предоставляется.

Помимо установленных мер ответственности, о которых будет сказано отдельно далее, соблюдению рассматриваемых принципов обработки персональных данных призвано способствовать принятие оператором специальных организационных и технических мер, направленных на соблюдение законодательства о персональных данных, в том числе по обеспечению сохранности персональных данных.

2.3. Реализация определенных организационно-технических мер для обеспечения выполнения обязанностей оператора и защиты персональных данных

Любые, даже наиболее продуманные законодательные положения обречены на декларативность в отсутствие реальных мер по их приведению в жизнь, выполняющих роль своего рода мостика между абстрактными требованиями закона и реальной практикой, сложившейся в сфере регулируемых отношений. Неудивительно, что законодательство о персональных данных, само появление которого стало следствием развития информационных технологий и обусловленных ими проблем, содержит ряд положений, регламентирующих технические аспекты защиты персональных данных. Однако, как известно, законодательство не может успеть за развитием технологий и его положения весьма быстро и неизбежно устаревают в этой части. Отсюда возникает основная проблема, связанная с обеспечением соблюдения положений законодательства о персональных данных, – отсутствие четкого представления о том, какие организационно-технические меры являются необходимыми и достаточными для того, чтобы не было оснований для привлечения оператора к ответственности за нарушение

требований Закона. Идентификация и последующая реализация таких мер составляет основное бремя законопослушного оператора персональных данных, и нередко самостоятельно он справиться с данной задачей не в состоянии.

С одной стороны, Закон вроде бы закрепляет отдельные меры и принципы их реализации. С другой стороны, Закон предусматривает обширное подзаконное регулирование, которое в свою очередь отдает его детализацию на откуп регуляторам (в частности, ФСБ России и ФСТЭК России). Следствием данного подхода является наличие ряда противоречащих друг другу разъяснений и избирательное правоприменение. Естественно, что в такой ситуации даже самые тщательные попытки обеспечения соответствия требованиям Закона о персональных данных не гарантируют ожидаемых результатов.

Начнем с того, что Закон о персональных данных в ст. 18[1] приводит *неисчерпывающий* перечень мер, направленных на обеспечение соблюдения оператором законодательства о персональных данных:

1) назначение ответственного за организацию обработки персональных данных;

2) издание документов, определяющих политику оператора в отношении обработки персональных данных, локальных актов по вопросам обработки персональных данных и т.п.;

3) применение правовых, организационных и технических мер по обеспечению безопасности персональных данных в соответствии со ст. 19 данного Закона;

4) осуществление внутреннего контроля и (или) аудита соответствия обработки персональных данных требованиям законодательства по защите персональных данных, политике оператора в отношении обработки персональных данных, локальным актам оператора;

5) оценка вреда, который может быть причинен субъектам персональных данных в случае нарушения требований Закона, соотношение указанного вреда и принимаемых оператором мер, направленных на обеспечение выполнения обязанностей, предусмотренных Законом;

6) ознакомление работников оператора, непосредственно осуществляющих обработку персональных данных, с положениями законодательства о персональных данных, в том числе с требованиями к защите персональных данных, документами, определяющими политику оператора в отношении обработки персональных данных, локальными актами по вопросам обработки персональных данных, и (или) обучение указанных работников.

Вроде бы указанные меры являются относительно понятными и разумными. К тому же Закон отдает на усмотрение самих операторов состав и перечень мер, которые являются, по его мнению, необходимыми и достаточными для обеспечения выполнения своих обязанностей. И даже рекомендует применение при этом риск-ориентированного подхода, т.е. оценки возможного вреда, который может быть причинен субъектам персональных данных в случае нарушения требований законодательства с последующим его соизмерением с характером мер, принимаемых для его предотвращения[1]. Однако на практике их реализация связана с существенными затруднениями.

Применительно к сфере электронной коммерции здесь важно отметить, что в качестве обязательной меры для реализации всеми субъектами электронной коммерции выступает мера № 2. В соответствии с ч. 2 ст. 18[1] Закона о персональных данных «оператор, осуществляющий сбор персональных данных с использованием информационно-телекоммуникационных сетей, обязан опубликовать в соответствующей информационно-телекоммуникационной сети документ, определяющий его политику в отношении обработки персональных данных, и сведения о реализуемых требованиях к защите персональных данных, а также обеспечить возможность доступа к указанному документу с использованием средств соответствующей информационно-телекоммуникационной сети». Таким образом, наличие на веб-сайте субъекта, осуществляющего предпринимательскую деятельность в сети Интернет, которая так или иначе связана с обработкой персональных данных клиентов, политики конфиденциальности (*privacy policy*) является не просто отражением современных «лучших практик» (*best practices*), но и требованием Закона.

Однако наибольшие сложности в практическом плане представляет реализация меры № 3, а именно определение необходимого уровня принимаемых организационных и технических мер по защите персональных данных от неправомерного или случайного доступа к ним,

[1] Любопытно, что Закон о персональных данных упоминает применение риск-ориентированного подхода в качестве одной из мер, обеспечивающих выполнение обязанностей оператора, обозначая ее следующим образом: «...оценка вреда, который может быть причинен субъектам персональных данных в случае нарушения Закона, соотношение указанного вреда и принимаемых оператором мер, направленных на обеспечение выполнения обязанностей, предусмотренных Законом» (п. 5 ч. 1 ст. 18[1]). Однако очевидно, что оценка вреда и соизмерение с ним характера принимаемых мер по его предотвращению является скорее критерием для решения вопроса о целесообразности и достаточности вводимых мер, а не самостоятельной мерой.

уничтожения, изменения, блокирования, копирования, распространения, а также от иных неправомерных действий.

Для того чтобы определить, какие именно меры в этой части должны быть приняты, необходимо сначала установить, к какому уровню защищенности должна относиться используемая оператором система обработки персональных данных. В соответствии с Постановлением Правительства РФ от 1 ноября 2012 г. № 1119[1] существует четыре уровня защищенности, дифференцируемые в зависимости от:

1) категории обрабатываемых персональных данных (специальные, биометрические, общедоступные, иные);

2) характера отношений между оператором и субъектом персональных данных (является работником (сотрудником) оператора или нет);

3) количества субъектов, данные которых обрабатываются (менее 100 000 или более 100 000);

4) типов актуальных угроз безопасности такой системы (угрозы 1-го типа – наличие недекларированных (недокументированных) возможностей в системном программном обеспечении, используемом в системе; угрозы 2-го типа – наличие недекларированных возможностей в прикладном программном обеспечении, используемом в ИСПДн; угрозы 3-го типа – наличие недекларированных возможностей в обоих видах программного обеспечения, используемого в системе)[2].

После определения требуемого уровня защищенности в отношении системы персональных данных оператор должен применять организационно-технические меры, предусмотренные для данного уровня защищенности[3]. Вряд ли имеет смысл приводить здесь их подробный перечень и описание, учитывая, что их подбор и реализация – вопрос не столько юридический, сколько технический. В то же время имеет смысл отметить, что при невозможности технической реализации отдельных предписанных в подзаконных актах мер по обеспечению безопасности персональных данных, а также с учетом экономической целесообразности оператором могут разрабатываться иные (компен-

[1] Постановление Правительства РФ от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

[2] Данный критерий является наиболее сложным для оценки и в ряде случаев потребует привлечения специализированной организации в области информационной безопасности.

[3] Перечень указанных мер содержится в приказе ФСТЭК России от 18 февраля 2013 г. № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

сирующие) меры, направленные на нейтрализацию актуальных угроз безопасности персональных данных. В этом случае в ходе разработки системы защиты персональных данных должно быть проведено обоснование применения компенсирующих мер для обеспечения безопасности персональных данных. На практике указанный процесс находит свое воплощение в составлении модели угроз, в которой идентифицируются актуальные для данного оператора угрозы, а также принимаемые организационные и технические меры их нейтрализации. При этом, несмотря на то, что и Закон о персональных данных, и подзаконные акты гласят, что в основе моделирования угроз должна лежать так называемая оценка вреда, который может быть причинен субъектам персональных данных в случае нарушения требований закона, на настоящий момент отсутствует методика его расчета.

Как видно, подзаконные акты используют достаточно сложную систему критериев, применяемых при определении требуемого уровня защищенности системы персональных данных, но допускают определенную степень усмотрения оператора при выборе мер защиты в зависимости от технических и экономических реалий. Все это уже создает неопределенность относительно того, насколько «конечный результат» реализации данных положений устроит регулирующий орган. Однако на этом проблемы операторов не заканчиваются.

Так, например, на практике часто возникает вопрос, должны ли используемые в системе персональных данных средства защиты информации быть сертифицированными или нет. По мнению ФСТЭК России, такие средства должны пройти оценку соответствия в форме обязательной сертификации[1]. При этом обычно делаются ссылки на некое Постановление Правительства РФ от 15 мая 2010 г. № 330[2], которое содержит гриф «Для служебного пользования» и не является

[1] См., например: информационное сообщение ФСТЭК России от 4 мая 2012 г. № 240/24/1701 «О работах в области оценки соответствия продукции (работ, услуг), используемой в целях защиты сведений, составляющих государственную тайну или относимых к охраняемой в соответствии с законодательством Российской Федерации иной информации ограниченного доступа» (п. 4).

[2] Постановление Правительства РФ от 15 мая 2010 г. «Об особенностях оценки соответствия продукции (работ, услуг), используемой в целях защиты сведений, относимых к охраняемой в соответствии с законодательством Российской Федерации информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну, а также процессов ее проектирования (включая изыскания), производства, строительства, монтажа, наладки, эксплуатации, хранения, перевозки, реализации, утилизации и захоронения, об особенностях аккредитации органов по сертификации и испытательных лабораторий (центров), выполняющих работы по подтверждению соответствия указанной продукции (работ, услуг)»

опубликованным. Алексей Лукацкий, один из наиболее видных специалистов в области информационной безопасности, весьма убедительно аргументирует незаконность такого толкования со ссылкой на положения Федерального закона от 27 декабря 2002 г. № 184 «О техническом регулировании» (далее – Закон о техническом регулировании) и ч. 2 ст. 4 Закона о персональных данных, предусматривающей необходимость публикации нормативных актов по вопросам обработки персональных данных. Тем не менее риск возникновения проблем, связанных с использованием несертифицированных средств защиты информации, является пока вполне ощутимым[1].

Как видно, обеспечение соответствия используемой оператором системы обработки персональных данных является весьма трудозатратным и дорогостоящим процессом, который к тому же в ряде случаев оператор не сможет реализовать без помощи специализированных организаций и консультантов.

2.4. Направление уведомления в уполномоченный орган об обработке персональных данных

Оператор до начала обработки персональных данных должен направить в уполномоченный орган по защите прав субъектов персональных данных (в настоящее время – Роскомнадзор[2]) уведомление о намерении осуществлять обработку персональных данных, на основании которого он ведет общедоступный реестр операторов персональных данных[3].

Данное уведомление подлежит направлению во всех случаях, кроме предусмотренных Законом случаев допустимости осуществления обработки без такого уведомления. В числе таких оснований, актуальных для сферы электронной коммерции, Закон предусматривает обработку оператором персональных данных: 1) своих работников; 2) своих контрагентов для целей, связанных исключительно с заключением или исполнением договора, без распространения их третьим лицам; 3) носящих общедоступный характер; 4) если обрабатываемые персональные данные ограничены исключительно фамилией, именем и отчеством субъекта (см. ч. 2 ст. 22 Закона о персональных данных).

---

[1] См. подробнее: *Лукацкий А.* Надо ли применять сертифицированные средства защиты персональных данных? // http://www.slideshare.net/lukatsky/ss-14591225; См. также: Материалы круглого стола «Персональные данные – год после новой редакции закона» // http://www.youtube.com/watch?v=9KyP1sa6RO8

[2] Пункт 1 Положения о Федеральной службе по надзору в сфере связи, информационных технологий и массовых коммуникаций, утв. Постановлением Правительства РФ от 16 марта 2009 г. № 228.

[3] http://pd.rkn.gov.ru/operators-registry/operators-list

Конечно, указанные исключения дают определенную свободу действий субъектам хозяйственной деятельности, которые неизбежно вынуждены иметь дело с персональными данными. Однако данные исключения носят весьма ограниченный характер, поэтому, опираясь только на них, на комфортную обработку персональных данных рассчитывать не придется. В связи с этим любому интернет-магазину или онлайн-сервису, который рассчитывает на установление длительных отношений со своими клиентами (пользователями), целесообразно подать такое уведомление.

Содержание уведомления регламентировано в ч. 3 ст. 22 Закона о персональных данных. Помимо сведений об операторе оно должно содержать данные об обрабатываемых категориях и видах персональных данных, целях обработки, принимаемых организационно-технических мерах по защите и пр. Также необходимо иметь в виду рекомендации, изданные Роскомнадзором по вопросам заполнения формы уведомления[1].

2.5. Соблюдение особых требований к трансграничной передаче данных

Наличие особых требований к трансграничной передаче данных является составной частью практически любого современного законодательного акта, посвященного персональным данным.

Регулирование данных вопросов начало появляться в 70-е гг. прошлого века в Европе. К примеру, законы Австрии[2], Швеции[3] требовали наличия согласия от уполномоченного органа на передачу персональных данных за пределы страны. Закон о персональных данных Финляндии требовал наличия специального согласия субъекта персональных данных на их передачу в другие страны[4].

Во времена, когда указанные акты принимались, практика трансграничной передачи данных не имела повсеместного характера и носила характер исключения[5]. Основной причиной появления положений о трансграничной передаче данных стали опасения европейских законодателей по поводу возможности обхода законодательных положений о защите персональных данных путем «вывода» процесса их обработки

[1] Приказ Роскомнадзора от 19 августа 2011 г. № 706 «Об утверждении Рекомендаций по заполнению образца формы уведомления об обработке (о намерении осуществлять обработку) персональных данных».

[2] Österreichisches Datenschutzgesetz vom. 18.10.1978. § 32, 34.

[3] Swedish Data Act of 1973. Article 11.

[4] Finnish Personal Data File Act and Personal Data File Decree. 30 April 1987. § 22.

[5] *Kuner C.* Transborder Data Flows and Data Privacy Law. Oxford University Press, 2013. P. 26–28.

в иные юрисдикции, что могло повлечь появление «информационных офшоров» (*data havens*). Данные опасения являются основным объяснением существования данных положений и поныне[1].

Другой причиной введения ограничений на свободный обмен информацией между разными странами являются опасения утраты государством контроля над своим информационным суверенитетом[2]. В качестве примера реальной ситуации, где такие опасения материализовались, можно привести случай с американской корпорацией *Dresser*, французское подразделение которой имело контракт с СССР на поставку оборудования для газопровода из Урала в Западную Европу. Впоследствии выяснилось, что данный договор противоречил экспортному законодательству США, в связи с чем головная компания корпорации *Dresser* отказалась его выполнять и в ответ на требования французского правительства о его исполнении отключила своему французскому подразделению доступ к корпоративной сети, по которой осуществлялся доступ к программному обеспечению, необходимому для реализации договора[3].

В особенности опасения за свой информационный суверенитет свойственны развивающимся странам. Так, в резолюции, принятой на латиноамериканской конференции регуляторов в сфере информации 1982 г., отмечалось непосредственное влияние вопросов трансграничной циркуляции информации на национальный суверенитет и рекомендация о включении в национальные законы о защите информации ограничений на ее хранение и обработку за границей, что должно способствовать развитию национальной информационной инфраструктуры[4]. Однако и иные страны выражают опасения по поводу возможности попадания персональных данных своих граждан в руки иностранных правоохранительных органов, преимущественно США[5].

---

[1] Hague Conference on Private International Law, Cross-Border Data Flows and Protection of Privacy (13 March 2010) // http://www.hcch.net/upload/wop/genaff2010pd13e.pdf

[2] *Gotlieb A. et. al.* The Transborder Transfer of Information by Communications and Computer Systems: Issues and Approaches to Guiding Principles // American Journal of International Law. No 68. 1974. P. 246–247.

[3] *Schoonmaker S.* High-Tech Trade Wars: US– Brazilian Conflicts in the Global Economy. University of Pittsburgh Press, 2002. P. 46–47.

[4] Recommendation Directly Pertaining to Transborder Data Flows Adopted by the Third Conference of Latin American Informatics Authorities, Recommendation Number 12. *Schoonmaker S.* Op. cit. P. 48.

[5] Так, в некоторых провинциях Канады был введен запрет на аутсорсинг персональных данных, в результате которого они могут оказаться под юрисдикцией США. Information & Privacy Commissioner for British Columbia, Privacy and the USA Patriot Act: Implications for British Columbia Public Sector Outsorcing. October 2004 // http://www.

Напротив, США рассматривают свободную циркуляцию информации в качестве одной из основ национального суверенитета. Как отметил один американский политик, одним из способов атаки на США, в высокой степени зависящей от информационно-телекоммуникационных технологий, может выступить ограничение свободы обращения информации, которое может повлечь изоляцию территориальных подразделений трансграничных компании от ее штаб-квартиры[1].

В последнее время опасения за сохранность информационного суверенитета стали вновь высказываться в связи с развитием облачных технологий и перспектив попадания данных под юрисдикцию государств, предусматривающих широкие полномочия правоохранительных органов по доступу к ней[2]. В связи с этим установление дополнительных ограничений на обработку персональных данных за рубежом является вполне удобным инструментом для обеспечения под прикрытием защиты прав граждан на сохранность информации об их личной жизни более «высоких» интересов.

Положения об условиях допустимости передачи данных содержатся в ряде документов: в Основных положениях ОЭСР о защите неприкосновенности частной жизни и международных обменах персональными данными от 23 сентября 1980 г. (ст. 15–18)[3], Конвенции о защите физических лиц при автоматизированной обработке персональных данных (ст. 12 и ст. 2 дополнительного протокола к Конвенции от 2001 г.), Директиве № 95/46/ЕС «О персональных данных» (ст. 25–26) и большинстве национальных актов о защите персональных данных[4].

Директива № 95/46/ЕС «О персональных данных» содержит общую презумпцию запрета трансграничной передачи данных. Такая передача возможна лишь при соблюдении общих условий обработки данных (в частности, при наличии законного основания для такой обработки), а также специальных условий, установленных для транс-

---

oipc.bc.ca/special-reports/1271. Сообщество всемирных межбанковских финансовых телекоммуникаций (*SWIFT*) также заявило об изменении технической архитектуры обработки данных внутриевропейских транзакций для предотвращения их выхода за пределы Европы и возможного попадания под юрисдикцию США. См.: SWIFT Board approves messaging re-architecture. 4 October 2007 // http://www.swift.com/about_swift/legal/swift_board_approves_messaging_re_architecture?rdct=t

[1] *Schoonmaker S.* Op. cit. P. 51.

[2] *Irion K.* Government Cloud Computing and The Policies of Data Sovereignty. September 2011.

[3] OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. 1980.

[4] Подробный их перечень и изложение соответствующих положений на английском языке см.: *Kuner C.* Op. cit. P. 189 ff.

граничной передачи в ст. 25–26. К таким специальным условиям относится:

1) наличие адекватной защиты персональных данных в принимающей стране, либо

2) наличие одного из оснований, указанных в ст. 26 (1) (согласие субъекта персональных данных на такую передачу, осуществление такой передачи во исполнение договора, заключенного с субъектом, необходимость защиты жизненно важных интересов субъекта персональных данных и др.), либо

3) наличие одобренных национальными органами по защите персональных данных адекватных защитных механизмов (*adequate safeguards*) в виде специальных условий, включенных в договор между компаниями – «экспортером» и «импортером» персональных данных, или так называемых обязательных корпоративных правил (*binding corporate rules, BCR*)[1]. В таких случаях защита прав субъектов персональных данных обеспечивается не средствами законодательства страны – «импортера» персональных данных, а личной ответственностью субъекта – «экспортера» персональных данных за возможные нарушения, которые могут произойти в стране – «импортере».

Следует отметить, что данные правила применяются и к последующей трансграничной передаче данных (*onward transfers*), например, в случаях, когда персональные данные сначала передаются провайдеру услуги за границу, который в свою очередь пересылает их в другую страну на аутсорсинг[2].

Процесс признания Европейским союзом третьей страны в качестве предоставляющей адекватный уровень защиты прав субъектов персональных данных является достаточно длительным и сложным. По состоянию на 1 октября 2013 г. такими странами признаны Андорра, Аргентина, Австралия, Канада, Швейцария, Израиль, США

[1] Данное исключение предназначено для транснациональных компаний, которые могут использовать свои внутренние корпоративные политики по защите персональных данных в качестве достаточной гарантии адекватной защиты персональных данных, передаваемых в рамках своих подразделений, в том числе расположенных в странах, законодательство которых не предоставляет адекватной защиты персональных данных. См.: Overview on Binding Corporate rules // http://ec.europa.eu/justice/data-protection/document/international-transfers/binding-corporate-rules/index_en.htm. См. также: Working Document on Frequently Asked Questions (FAQs) related to Binding Corporate Rules. Article 29 Working Party. 24 June 2008.

[2] См.: ст. II (i) Решения Европейской комиссии 2004/915/EC // http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2004:385:0074:0084:en:PDF; First Orientations on Transfers of Personal Data to Third Countries – Possible Ways Forward in Assessing Adequacy. Article 29 Working Party. 26 June 1997.

(в части передачи персональных данных пассажиров авиатранспорта и соглашений *Safe Harbor*), Новая Зеландия, а также ряд островов: Фарерские острова, острова Гернси, Мэн, Джерси[1]. Россия, по мнению Европейского союза, не относится к числу стран, обеспечивающих адекватный уровень защиты прав субъектов персональных данных. Как следствие передача персональных данных из стран Европейского союза в Россию возможна лишь при наличии на то специальных оснований либо в российские подразделения трансграничных компаний на основании *CBR*.

Учитывая существующие положения об ответственности за нарушение законодательства о персональных данных и состояние отечественной правоприменительной практики по данному вопросу[2], такой подход европейских коллег можно рассматривать как вполне заслуженный и обоснованный. Одного только копирования положений европейского законодательства недостаточно для того, чтобы полученный результат соответствовал европейским стандартам. А учитывая, что Россия завершила процесс ратификации Конвенции о защите физических лиц при автоматизированной обработке персональных данных 1981 г. только спустя восемь лет с момента принятия Федерального закона о ее ратификации, отношение российских государственных органов к проблематике защиты персональных данных становится вполне очевидным.

Российский Закон о персональных данных рассматривает в качестве стран, *a priori* обеспечивающих адекватную защиту персональных данных, все государства, являющиеся сторонами Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных[3]. Иные страны могут быть отнесены к категории «адекватных» специальным перечнем, который утверждается Роскомнадзором, «при условии соответствия положениям вышеуказанной Конвенции действующих в соответствующем государстве норм права и применяемых мер безопасности персональных данных» (ч. 1, 2 ст. 12).

---

[1] http://ec.europa.eu/justice/data-protection/document/international-transfers/adequacy/index_en.htm#h2-11

[2] См. далее.

[3] Примечательно, что какой-либо дополнительной проверки в отношении стран – участниц Конвенции для определения степени адекватности защиты ими персональных данных не требуется. Поэтому, формально говоря, тот факт, что соответствующие положения законодательства о персональных данных не применяются на практике или систематически нарушаются при попустительстве уполномоченных органов, не влияют на статус такой страны для целей применения положений ст. 12 Закона о персональных данных.

Данный перечень по состоянию на 1 октября 2013 г. включает следующие страны: Австралия, Аргентина, Израиль, Канада, Марокко, Малайзия, Мексика, Монголия, Новая Зеландия, Ангола, Бенин, Кабо-Верде, Южная Корея, Перу, Сенегал, Тунис, Чили, Гонконг, Швейцария[1].

Оператор обязан убедиться в том, что иностранным государством, на территорию которого осуществляется передача персональных данных, обеспечивается адекватная защита прав субъектов персональных данных до начала осуществления трансграничной передачи персональных данных (ч. 3 ст. 12 Закона о персональных данных). Систематическое толкование положений ст. 12 дает основание для вывода, что оценка степени адекватности защиты персональных данных в той или иной стране является предметом компетенции Роскомнадзора и не является предметом усмотрения оператора. Все, что он должен сделать, – это ознакомиться с соответствующим перечнем и определить, может ли он передавать персональные данные в такую страну в отсутствие специальных оснований, предусмотренных в Законе. Представляется, что данный подход является правильным, поскольку иной подход создавал бы почву для последующих споров между регуляторами и операторами относительно того, насколько оправданным было суждение последнего об адекватности степени защиты персональных данных в стране-«импортере».

При отсутствии оснований для отнесения иностранного государства к категории обеспечивающих адекватную защиту прав субъектов персональных данных трансграничная передача персональных данных, обработка которых осуществляется в соответствии с общими требованиями Закона о персональных данных, может осуществляться в случаях:

1) наличия согласия в письменной форме субъекта персональных данных на трансграничную передачу его персональных данных. При этом в соответствии с ч. 4 ст. 9 Закона о персональных данных равнозначным письменной форме является электронный документ, подписанный электронной подписью. Учитывая, что новый Закон об ЭП ввел понятие простой электронной подписи, которая подтверждает факт ее формирования посредством использования кодов и паролей, проставление галочки на веб-сайте или принятие условий *click-wrap*-соглашения, сделанное определенным лицом из личного кабинета,

[1] Приказ Роскомнадзора от 15 марта 2013 г. № 274 «Об утверждении перечня иностранных государств, не являющихся сторонами Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных и обеспечивающих адекватную защиту прав субъектов персональных данных».

доступного после введения логина и пароля, может рассматриваться как письменное согласие при условии соблюдения положений ч. 2 ст. 6 Закона об ЭП;

2) предусмотренных международными договорами Российской Федерации;

3) предусмотренных федеральными законами, если это необходимо в целях защиты основ конституционного строя Российской Федерации, обеспечения обороны страны и безопасности государства, а также обеспечения безопасности устойчивого и безопасного функционирования транспортного комплекса, защиты интересов личности, общества и государства в сфере транспортного комплекса от актов незаконного вмешательства;

4) исполнения договора, стороной которого является субъект персональных данных;

5) защиты жизни, здоровья, иных жизненно важных интересов субъекта персональных данных или других лиц при невозможности получения согласия в письменной форме субъекта персональных данных.

В связи с неизбежным наличием иностранного элемента при рассмотрении вопроса трансграничной передачи данных возникает вопрос об определении юрисдикции и применимого права. К вопросам юрисдикции применимы те соображения, которые высказаны ранее в главе, специально посвященной рассмотрению вопросов юрисдикции в сети Интернет. Очевидно, что суды и регуляторы страны, где домицилирован субъект персональных данных, будут считать себя компетентными по вопросам рассмотрения споров, связанных с зарубежной обработкой данных такого субъекта нерезидентом. Ключевой вопрос в таком случае заключается в наличии реальной возможности исполнения решений такого суда (регулятора), что имеет место при наличии каких-либо активов на территории страны суда (регулятора).

Что касается применимого права, то общий подход европейского права в настоящее время заключается в том, что национальное право страны – члена ЕС применяется в отношении случаев обработки персональных данных нерезидентом только при использования для такой обработки оборудования, расположенного на территории такой страны, за исключением случаев, когда оно используется исключительно для целей транзитной передачи данных (ст. 4 (1) (*c*) Директивы 95/46/ЕС)[1]. Иными словами, в качестве коллизионной

[1] Данное исключение сделано как раз для того, чтобы учесть специфику маршрутизации информации в сети Интернет. Как отмечалось ранее, протоколы сети Интернет

привязки используется местонахождение оборудования и характер его использования. Данный подход можно считать достаточно устаревшим в условиях современного уровня развития информационных технологий. Во-первых, субъекту персональных данных достаточно сложно определить, где находится оборудование оператора, и тем более то, для каких целей оно используется. Во-вторых, с технической точки зрения такие данные благодаря технологиям облачных вычислений могут находиться на серверах в разных странах и менять свое местоположение в динамичном режиме.

В проекте Общего регламента о защите персональных данных (*GDPR*) предлагается изменить подход к определению оснований для применения национального права. В частности, в отношении операторов, не домицилированных на территории Европейского союза, в качестве основания для применения права ЕС в области защиты персональных данных указан тот же критерий, что и для применения законодательства о защите прав потребителей: направленность деятельности по наблюдению или предложению товаров (услуг) на граждан ЕС. Ожидается, что такой подход обеспечит персональным данным, обрабатываемым за рубежом, тот же уровень защиты, что и в ЕС, а также бóльшую предсказуемость в вопросах определения применимого права для операторов из третьих стран[1]. Таким образом, европейское право в области защиты персональных данных приобретет еще более явно выраженный экстерриториальный характер. К примеру, российское юридическое лицо, которое реализует свои товары или услуги хотя бы в одной из стран Европейского союза и обрабатывает при этом персональные данные хотя бы одного из граждан такой страны, формально подпадет под действие всей совокупности норм европейского права в области защиты персональных данных (включая штрафы за их несоблюдение). Все это дает основания для вывода о том, что нормы о праве, применимом к зарубежной обработке персональных данных, и нормы об условиях допустимости трансграничной передачи данных преследуют одну и ту же цель: распространение национальных защитных норм

осуществляют разделение каждого цифрового сообщения на отдельные пакеты данных, каждый из которых направляется автономным способом адресату. Прохождение таких пакетов сообщений не может нарушать прав субъектов персональных данных, в связи с чем применения специальных норм законодательства к такого рода способам обращения информации не требуется (см.: *Kuner C.* Op. cit. P. 15).

[1] См.: ст. 3(2) проекта Общего регламента о защите персональных данных (*GDPR*). См. также: How will the EU's data protection reform make international cooperation easier? // http://ec.europa.eu/justice/data-protection/document/review2012/factsheets/5_en.pdf

законодательства о персональных данных за пределы территории государства, их принявшего. Иными словами, они направлены на экстерриториальное применение права такой страны. Такой подход не может не вызвать коллизий между предписаниями, существующими в различных правопорядках. Элементарный пример: субъекту электронной коммерции, продающему товары (услуги) в разные страны мира, поступает предписание от правоохранительных органов одной из них (например, США) о раскрытии данных своих клиентов в связи с расследуемым преступлением. Выполнение такого предписания может быть нарушением положений европейского права об охране персональных данных, влекущим наложение штрафа. Оператор в таком случае находится между молотом и наковальней, и какие-либо удовлетворительные правовые способы разрешения данной коллизии отсутствуют[1].

Применение специальных положений о трансграничной передаче данных в сфере электронной коммерции наталкивается на вопрос о том, что понимать под такой передачей. Дефиниция, содержащаяся в Законе о персональных данных («передача персональных данных на территорию иностранного государства, органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу»), мало помогает в таком понимании. В частности, является ли трансграничной передачей данных размещение информации на веб-сайте, сервер которого находится в другой стране? С одной стороны, вроде бы да, поскольку информация, размещенная на веб-сайте *a priori* доступна пользователям со всего мира, а реализация доступа к ней с технической точки зрения представляет собой обмен данными между таким веб-сайтом и компьютером пользователя. С другой стороны, очевидно, что столь широкое понимание трансграничной передачи данных фактически превратит регулирование такой передачи в регулирование процесса обмена информацией в сети Интернет. С практической точки зрения такой подход перечеркнет смысл наличия специальных норм о трансграничной передаче данных: из специальных норм они превратятся в общие и окажутся просто

[1] Безусловно, введение в национальное законодательство специального положения, позволяющего не учитывать отдельные его положения в случаях, когда это необходимо для соблюдения иностранного законодательства, не очень вяжется с концепцией национального суверенитета, но определенные исключения для тех сфер, которые являются предметом международных соглашений и общих интересов (борьба с коррупцией, противодействием отмыванию доходов, полученных преступным путем, борьба с эпидемиями и т.п.), можно было бы сделать, тем более что определенные примеры тому уже есть (см. подробнее: *Kuner C.* Op. cit. P. 181–183).

не в состоянии «переварить» тот объем оборота информации, который имеет место в сети Интернет, превратившись в один из наиболее декларативных компонентов всего законодательства о персональных данных.

В свое время данный вопрос встал перед Европейским судом, который, руководствуясь прагматическими соображениями, признал отсутствие трансграничной передачи данных при размещении персональных данных на веб-сайте, безотносительно к месту расположения сервера, на котором такой веб-сайт расположен. По мнению суда, при размещении информации на веб-сайте отсутствует факт ее автоматической передачи множеству пользователей из разных стран: такая передача происходит по инициативе пользователя, а не лица, разместившего информацию. Суд также указал, что иной подход повлек бы распространение законов ЕС о персональных данных на весь Интернет, что явно не входило в намерения европейских законодателей[1]. Представляется, что данная правовая позиция является актуальной и в российских условиях как минимум в силу схожести исходных регулятивных положений, а как максимум – в силу ее разумности.

Завершая рассмотрение положений о трансграничной передаче персональных данных, необходимо отметить следующее. Лицо, осуществляющее предпринимательскую деятельность в сети Интернет либо отдающее на аутсорсинг те элементы своего бизнеса, которые связаны с персональными данными (*IT*-инфраструктура, бухгалтерия и т.д.), сталкивается с потенциальной трансграничной передачей персональных данных. В связи с этим в политику конфиденциальности и договоры с субъектами персональных данных целесообразно включать условия о согласии на такую передачу, по возможности как можно более конкретно сформулированные. Даже если изначально предполагается, что в качестве страны – импортера данных выступит государство, обеспечивающее с точки зрения ст. 12 Закона о персональных данных адекватный уровень защиты, все равно нельзя быть уверенным в том, что эта информация в силу технических причин или изменившейся коммерческой ситуации не окажется в иной, менее «благонадежной» стране. В случае же с обработкой персональных данных граждан ЕС включение таких положений является практически абсолютной необходимостью в свете усиления регулятивной политики в данном направлении и существенном повышении штрафов.

[1] Bodil Lindquist, ECJ Case C-101/01. 06.11.2003.

§ 3. Ответственность за несоблюдение требований законодательства о персональных данных

В соответствии со ст. 24 Закона о персональных данных лица, виновные в нарушении требований указанного Закона, несут предусмотренную законодательством Российской Федерации ответственность. Поскольку указанная норма является отсылочной, то установление конкретных видов правонарушений и применение соответствующих мер ответственности регулируются иными нормативными актами.

Основной и наиболее распространенной формой ответственности за нарушение положений законодательства о персональных данных является административная ответственность. КоАП РФ содержит несколько составов, применимых к нарушениям в указанной сфере:

1) ст. 13.11 КоАП РФ: «нарушение установленного законом порядка сбора, хранения, использования или распространения информации о гражданах (персональных данных)», предусматривающая ответственность в виде предупреждения или наложения штрафа на граждан – в размере от 300 до 500 руб.; на должностных лиц – от 500 до 1000 руб.; на юридических лиц – от 5000 до 10 000 руб. В качестве органа, уполномоченного на возбуждение административного правонарушения по данной статье, выступают органы прокуратуры, рассмотрение дела осуществляется судом. Данный состав является основным и применяется к большинству случаев нарушения оператором установленных обязанностей по обработке персональных данных (осуществление обработки данных без получения согласия субъекта персональных данных, передача персональных данных третьим лицам)[1];

2) ст. 5.39 КоАП РФ: «отказ в предоставлении гражданину собранных в установленном порядке документов, материалов, непосредственно затрагивающих права и свободы гражданина, либо несвоевременное предоставление таких документов и материалов, непредставление иной информации в случаях, предусмотренных законом, либо предоставление гражданину неполной или заведомо недостоверной информации», предусматривающая ответственность в виде наложения на должностных лиц штрафа в размере от 1000 до 3000 руб. В качестве органа, уполномоченного на возбуждение административного правонарушения по данной статье, выступают органы прокуратуры, рассмотрение дела осуществляется судом. Данный состав направлен на защиту права субъекта персональных данных на доступ к инфор-

[1] См., например: постановление ФАС Уральского округа от 13 января 2012 г. № Ф09-9061/11.

мации об осуществляемой обработке его персональных данных, предусмотренную ст. 14 Закона о персональных данных;

3) ч. 2 ст. 13.12 КоАП РФ: «использование несертифицированных информационных систем, баз и банков данных, а также несертифицированных средств защиты информации, если они подлежат обязательной сертификации», предусматривающая ответственность в виде штрафа на граждан – в размере от 300 до 500 руб. с возможной конфискацией несертифицированных средств защиты; на должностных лиц – от 1000 до 2000 руб.; на юридических лиц – от 10 000 до 20 000 руб. с возможной конфискацией несертифицированных средств защиты. В качестве органа, уполномоченного на возбуждение и рассмотрение административного правонарушения по данной статье, выступают органы Федеральной службы безопасности. Следует учитывать, что диспозиция данной санкции охватывает случаи, когда осуществляется использование несертифицированных средств защиты информации в то время, как нормативным актом предусмотрена их обязательная сертификация. Сертификация является лишь одной из форм подтверждения соответствия наряду с иными (государственный контроль (надзор), испытания, регистрация, подтверждения соответствия, приемки и ввода в эксплуатацию объекта, строительство которого закончено, и в иной форме – ч. 3 ст. 7 Закона о техническом регулировании. В настоящее время установлено лишь требование о том, что средства защиты информации, используемые в информационной системе, должны пройти процедуру оценки соответствия (п. 4 Приказа ФСТЭК России от 18 февраля 2013 г. № 21). Про то, что такая оценка соответствия должна проводиться исключительно в форме обязательной сертификации, там ничего не говорится. Так или иначе, ранее уже отмечалось, что у ФСТЭК России есть свое видение данного вопроса;

4) ст. 19.7 КоАП: «Непредставление или несвоевременное представление в государственный орган (должностному лицу) сведений (информации), представление которых предусмотрено законом и необходимо для осуществления этим органом (должностным лицом) его законной деятельности, а равно представление в государственный орган (должностному лицу) таких сведений (информации) в неполном объеме или в искаженном виде», предусматривающая ответственность в виде штрафа на граждан в размере от 100 до 300 рублей; на должностных лиц – от 300 до 500 рублей; на юридических лиц – от 3000 до 5000 рублей. Данная статья применима к случаям ненаправления оператором персональных данных уведомления в Роскомнадзор

об обработке персональных данных в тех случаях, когда оно должно было быть направлено[1].

Следует отметить, что в соответствии с ч. 3 ст. 2.1 КоАП РФ в случае совершения юридическим лицом административного правонарушения и выявления конкретных должностных лиц, по вине которых оно было совершено (ст. 2.4 КоАП РФ), допускается привлечение к административной ответственности по одной и той же норме как юридического лица, так и указанных должностных лиц[2].

Однако даже при совокупном наложении штрафа на должностное лицо и юридическое лицо очевидно, что его размер является далеко не самым высоким, что существенно снижает превентивную функцию административной ответственности. Это осознает и Роскомнадзор, который выступил в качестве инициатора внесения изменений в КоАП РФ. С законопроектом можно ознакомиться на сайте Роскомнадзора[3].

Данный законопроект предлагает закрепление дифференцированного подхода к правонарушениям в сфере оборота персональных данных. Так, в отдельные составы могут быть выделены правонарушения оператора персональных данных, обработка персональных данных без согласия субъекта персональных данных, незаконная обработка специальных категорий персональных данных и несоблюдение условий трансграничной передачи персональных данных. Существенно увеличивается размер штрафов, максимальный размер в отношении юридических лиц может составить 700 000 руб. либо в размере 2% совокупного дохода за прошедший отчетный год.

Для того чтобы определить, много это или мало, имеет смысл посмотреть, какой размер штрафов за нарушения законодательства о персональных данных установлен в странах Европы. Так, например, максимальный штраф за серьезное нарушение законодательства о персональных данных в Великобритании составляет 500 000 ф. ст.[4]. Во Франции размер штрафа за единичное нарушение может дости-

---

[1] См.: постановление Двенадцатого арбитражного апелляционного суда от 1 сентября 2011 г. по делу № А06-858/2011.

[2] См.: п. 15 постановления Пленума Верховного Суда РФ от 24 марта 2005 г. № 5 «О некоторых вопросах, возникающих у судов при применении Кодекса Российской Федерации об административных правонарушениях».

[3] http://rkn.gov.ru/docstore/doc1353.htm?print=1. См. также: *Керенский И.В.* Роскомнадзор предлагает в разы увеличить штраф за нарушение правил обработки персональных данных // СПС «КонсультантПлюс».

[4] Information Commissioner's Guidance About the Issue of Monetary Penalties Prepared and Issued Under Section 55C (1) of the Data Protection Act 1998. 2012. Section 5.1.

гать 150 000 евро, за повторное – до 300 000, или 5% годового дохода[1]. В Германии средний штраф составляет 50 000 евро, максимальный штраф – 300 000 евро[2]. Причем Германии есть чем похвастаться в данной области. В октябре 2009 г. к ответственности за нарушение законодательства о персональных данных был привлечен крупнейший оператор железных дорог в Германии, компания *Deutsche Bahn AG*, которой был назначен штраф в размере 1 123 503 50 евро.

В проекте Общего регламента о защите персональных данных предлагается не только унифицировать принятые в отдельных странах ЕС размеры штрафов, но и повысить их. Так, максимальный штраф составит 100 000 000 евро, или до 5% годового мирового дохода[3].

Так, максимальный штраф за непредоставление ответов на запросы субъектов персональных данных или регулятора составит 250 000 евро, или 0,5% годового мирового дохода; за нарушение положений регламента – 500 000 евро, или 1% годового мирового дохода; за нарушение специальных положений регламента – 1 000 000 евро, или до 2% годового мирового дохода[4].

Как видно, предлагаемые в законопроекте Роскомнадзора штрафы за нарушение персональных данных существенно не дотягивают по размерам до среднеевропейских. Про действующие же ныне штрафы вообще говорить смешно. Для многих компаний с традиционным российским менталитетом гораздо проще оставить все как есть и заплатить штраф, чем погружаться в хитросплетения требований законодательства, привлекать специализированные компании и приобретать специальную инфраструктуру. Очевидно, что такое положение вещей ставит субъектов электронной коммерции в неравное положение. Добросовестные участники, которые дорожат своей репутацией, а также те, которые ведут внешнеэкономическую деятельность со странами Европы, будут прилагать усилия по обеспечению соблюдения требований

[1] Art. 47 Loi relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel et modifiant la loi. No 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

[2] § 43 Bundesdatenschutzgesetz 2009.

[3] Art. 79 Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) Updated version: http://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/dv/comp_am_art_30-91/comp_am_art_30-91en.pdf

[4] Art. 79 Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) // http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf

законодательства Российской Федерации о персональных данных. Все остальные участники отечественного оборота в большинстве случаев не будут демонстрировать того же рвения. Учитывая избирательный подход отечественных правоприменительных органов к выбору мишеней для проверок, нетрудно догадаться, какие именно компании попадут под их прицел. А принимая во внимание запутанный характер и весьма обтекаемые формулировки отечественного законодательства о персональных данных, найти несоответствия будет не так сложно, даже если оператор приложил максимум усилий для того, чтобы сделать «все по закону». Так что штрафы, конечно, повышать нужно, чтобы хотя бы не было стыдно говорить об их размерах в пересчете на доллары или евро зарубежным коллегам. Но пока не будут решены глобальные проблемы отечественного правоприменения (коррупция, некомпетентность, избирательность), повышение штрафов ляжет бременем на добросовестные компании, не достигая главного источника утечек персональных данных: государственных органов и *no-name* компаний.

Помимо административной ответственности нарушение законодательства о персональных данных может в некоторых случаях влечь и уголовную ответственность. В числе потенциально применимых составов преступления можно указать следующие:

1) ст. 183 УК РФ «Незаконные получение и разглашение сведений, составляющих коммерческую, налоговую или банковскую тайну», которая включает в себя четыре состава:

– часть 1: Собирание сведений, составляющих коммерческую, налоговую или банковскую тайну, путем похищения документов, подкупа или угроз, а равно иным незаконным способом. При этом собирание рассматриваемых сведений путем доступа к охраняемой законом компьютерной информации, если это повлекло уничтожение, блокирование, модификацию либо копирование информации, нарушение работы ЭВМ, системы ЭВМ или их сети, следует квалифицировать по совокупности ч. 1 ст. 183 и ст. 272 УК РФ[1]. За данные деяния предусмотрено наказание вплоть до лишения свободы на срок до 2 лет;

– часть 2: Незаконные разглашение или использование сведений, составляющих коммерческую, налоговую или банковскую тайну, без согласия их владельца лицом, которому она была доверена или стала

[1] Комментарий к Уголовному кодексу Российской Федерации (постатейный) / под ред. А.И. Чучаева. М., 2013. Комментарий к ст. 183.

известна по службе или работе. За данные деяния предусмотрено наказание вплоть до лишения свободы до 3 лет;

– часть 3: Те же деяния, причинившие крупный ущерб (доход или ущерб более 1,5 млн руб.) или совершенные из корыстной заинтересованности. За данные деяния предусмотрено наказание вплоть до лишения свободы до 5 лет;

– часть 4: Деяния, предусмотренные ч. 2 или 3 ст. 183 УК РФ, повлекшие тяжкие последствия. В качестве таких тяжких последствий может выступить, например, самоубийство субъекта, чьи персональные данные были разглашены. За данные деяния предусмотрено наказание вплоть до лишения свободы до 7 лет.

Несмотря на то что положения ст. 183 УК РФ не содержат прямого упоминания о персональных данных, они, учитывая весьма широкое определение понятия коммерческой тайны, могут быть отнесены к таковой при соблюдении условий, указанных в Федеральном законе от 29 июля 2004 г. № 98-ФЗ «О коммерческой тайне» (далее – Закон о коммерческой тайне). Как правило, данные о клиентах организации охватываются режимом коммерческой тайны, введенным в ней[1].

В качестве примера можно привести уголовное дело, в котором лицо, предложившее работнику компании ОАО «ВолгаТелеком» передать ему за вознаграждение сведения об абонентах, было осуждено за покушение на собирание сведений, составляющей коммерческую тайну, путем подкупа (ч. 3 ст. 30, ч. 1 ст. 183 УК РФ)[2];

2) ст. 138 УК РФ «Нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений» содержит обычный состав (ч. 1), и квалифицированный (ч. 2), предусматривающий совершение тех же деяний, но только с использованием служебного положения (например, работниками операторов связи[3]). В последнем случае в числе возможных наказаний предусмотрено лишение свободы. На практике имели случаи привлечения к уголовной ответственности по данной статье лиц, которые регистрировали аккаунты в социальных сетях под именем других граждан, вели от их

[1] Тем не менее нормы, установленные в законодательстве о персональных данных, по общему правилу будут иметь приоритет над нормами Закона о коммерческой тайне при определении их правового статуса (условия использования, порядка распоряжения и т.п.).

[2] Приговор первомайского районного суда г. Кирова по уголовному делу от 30 августа 2011 г. № 1-269/2011 (43902).

[3] См.: Комментарий к Уголовному кодексу Российской Федерации (постатейный) / под ред. Г.А. Есакова. М., 2012. Комментарий к ст. 137.

имени переписку и тем самым знакомились с личной информацией, адресованной таким лицам в письмах от их друзей и знакомых[1], либо которые из неприязненных отношений размещали на таких фальшивых аккаунтах помимо прочих персональных данных ложные сведения о сексуальных предпочтениях потерпевшей[2].

Не исключается возможность квалификации некоторых действий, связанных с незаконной обработкой персональных данных, по совокупности с иными статьями УК РФ, в частности со ст. 272 «Неправомерный доступ к компьютерной информации» и ст. 273 «Создание, использование и распространение вредоносных программ для ЭВМ».

Гражданско-правовая ответственность за нарушение персональных данных может принимать различные формы: возмещение убытков, взыскание неустойки либо возмещение морального вреда. Убытки, как правило, взыскать вряд ли удастся, учитывая весьма строгий подход отечественных судов к доказыванию их размера и причинно-следственной связи между нарушением и размером наступивших убытков. К тому же тесная связь персональных данных с личностью лица в большинстве случаев исключает наличие убытков, носящих экономический характер: расходы, которые лицо, чье право нарушено, произвело или должно будет произвести для восстановления нарушенного права, утрата или повреждение его имущества (реальный ущерб) либо неполученные доходы, которые это лицо получило бы при обычных условиях гражданского оборота, если бы его право не было нарушено (упущенная выгода) (ст. 15 ГК РФ). Что же касается неустойки, то ее взыскание за факт нарушения оператором условий обработки персональных данных возможно только в случаях, прямо предусмотренных договором. Учитывая, что физическое лицо обычно выступает в договоре слабой стороной, а также тот факт, что подавляющее большинство договоров заключается по модели присоединения (особенно в сфере электронной коммерции), рассчитывать на наличие такой неустойки в договоре весьма наивно. Поэтому возмещение морального вреда является наиболее реалистичной мерой гражданско-правовой ответственности из трех перечисленных.

Под моральным вредом понимаются нравственные или физические страдания, причиненные действиями (бездействием), посягающими на принадлежащие гражданину от рождения или в силу зако-

[1] См. приговор Исакогорского районного суда г. Архангельска от 31 января 2011 г., которым была осуждена генеральный директор ООО «Гелиос» по ст. 137 и 272 УК РФ // http://pravo.ru/news/view/47465

[2] См.: приговор Октябрьского районного суда г. Белгорода от 18 августа 2010 г.

на нематериальные блага, такие, как жизнь, здоровье, достоинство личности, деловая репутация, неприкосновенность частной жизни, личная и семейная тайна и т.п.[1] В соответствии со ст. 151 ГК РФ моральный вред может быть взыскан за посягательства на личные неимущественные права или нематериальные блага, а также в случаях, установленных Законом. Положение ч. 2 ст. 24 Закона о персональных данных является как раз таким случаем. В нем закреплено, что «моральный вред, причиненный субъекту персональных данных вследствие нарушения его прав, нарушения правил обработки персональных данных, установленных настоящим Федеральным законом, а также требований к защите персональных данных, установленных в соответствии с настоящим Федеральным законом, подлежит возмещению в соответствии с законодательством Российской Федерации. Возмещение морального вреда осуществляется независимо от возмещения имущественного вреда и понесенных субъектом персональных данных убытков».

Правда, учитывая специфику подхода отечественных судов к определению его размеров, данная форма защиты будет являться во многом декларативной. Так, за неправомерное размещение на официальном веб-сайте районного суда персональных данных потерпевшей (фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация) суд, признав наличие факта нарушения законодательства, взыскал в пользу потерпевшей возмещение морального вреда в размере 200 руб.[2] Такая «щедрость» не вызывает удивления на фоне общей картины взыскания морального вреда российскими судами. Так, сумма, близкая к 100 тыс. руб., считается весьма значительной и присуждается, как правило, в связи с причинением смерти близкому родственнику истца. Тяжкое повреждение здоровья оценивается приблизительно в 2–3 раза ниже, а легкий вред здоровью – соответственно в 10 и более раз ниже. Причем даже эти цифры нигде не фиксированы и суд вполне может назначить компенсацию и в меньшем размере. Минимальный размер суммы компенсации морального вреда законодательно не установлен[3]. В связи с этим субъекту персональных данных, чьи права были нарушены незаконной обработ-

[1] Пункт 2 постановления Пленума Верховного Суда РФ от 20 декабря 1994 г. № 10 «Некоторые вопросы применения законодательства о компенсации морального вреда».

[2] Решение Ленинского районного суда г. Чебоксары Чувашской Республики от 6 июля 2010 г. по делу № 2-2225/2010.

[3] См.: *Кузнецова О.В.* Возмещение морального вреда: практическое пособие. М., 2009.

кой данных, в большинстве случаев целесообразно обратить внимание на административную или уголовную ответственность, не тратя свое время на длительный гражданский процесс о возмещении морального вреда.

В целом гражданско-правовая ответственность является одной из наименее эффективных и перспективных для восстановления нарушенных прав субъекта персональных данных из всех перечисленных в ст. 24 Закона о персональных данных.

§ 4. Перспективы развития законодательства о персональных данных

Лучшим способом рассмотреть возможные перспективы развития законодательства о персональных данных является, пожалуй, анализ основных нововведений, предлагаемых в проекте Общего регламента о защите персональных данных (*GDPR*), поскольку данный документ в случае его принятия имеет все шансы стать «законодателем мод» в этой сфере на ближайшие годы. Некоторые новеллы уже освещались ранее: увеличение штрафов и расширение сферы действия данного закона в отношении нерезидентов ЕС, осуществляющих «направленную» деятельность на граждан ЕС. Однако это далеко не все предлагаемые нововведения. Конечно, здесь нет возможности привести полный перечень таковых, поскольку проект документа состоит из 90 статей и преамбулы почти из 140 пунктов. Однако некоторые основные моменты все же стоит указать.

Во-первых, предполагается расширить существующий набор прав субъекта персональных данных за счет включения в него права на перенос своих персональных данных от одного оператора к другому (*right of portability*) (ст. 18 *GDPR*) и права «быть забытым» (*the right to be forgotten*) (ст. 17 *GDPR*). В первом случае идет речь о предоставлении субъекту возможности получения от оператора своих персональных данных в одном из общераспространенных форматов данных для того, чтобы иметь возможность без затруднений использовать их у другого оператора (типичный пример – смена социальной сети с переносом данных своего аккаунта). Второе право предполагает обязанность оператора удалить персональные данные по достижении цели их обработки, при отзыве субъектом согласия на их обработку или отсутствии иных законных оснований для продолжения их обработки. В тех случаях, когда речь идет о размещении персональных данных на общедоступных ресурсах, данное право предполагает, что оператор должен также предпринять усилия по информированию третьих лиц о поступившем

требовании субъекта об удалении таких данных и ссылок на них. Нетрудно заметить, что основным источником вдохновения для данных прав стали социальные сети и желание законодателей обеспечить их пользователей дополнительными средствами контроля над размещаемыми данными.

Примечательно, что в ходе последующих дискуссий вышеуказанные права претерпели определенный «ребрендинг» и утратили самостоятельный статус, став составной частью более общих прав субъекта персональных данных: право быть забытым стало частью права на удаление персональных данных, а право на перенос данных стало частью общего права на доступ к персональным данным[1].

В соответствии со ст. 17 компромиссного варианта *GDRP* субъект персональных данных имеет право требовать удаления своих персональных данных, недопущения их дальнейшего распространения и удаления третьими лицами ссылок на такие персональные данные. Данная статья содержит ряд условий для реализации данного права, правда, не ограничивает его реализацию только социальными сетями.

В соответствии со ст. 15 (2*a*) компромиссного варианта *GDRP* право на перенос персональных данных теперь включает в себя два элемента: право на получение копии своих персональных данных в общераспространенном формате данных и право на перенос данных, который должен быть осуществлен оператором оператору при условии наличия технической возможности. Правда, до сих пор не ясно, к каким операторам будет применяться данное право: формально его реализация не ограничена исключительно социальными сетями (где ему и место), в связи с чем его введение может скорее навредить, чем принести пользу, поскольку обеспечение реализации данного права возлагает дополнительные издержки на операторов[2].

В целом придумывание законодателями неких новых прав или правомочий в составе имеющихся прав субъектов персональных данных может рассматриваться скорее в качестве показателя кризиса законодательства о персональных данных в условиях современных телекомуникационных и информационных технологий,

[1] С текстом компромиссного варианта *GDRP* можно ознакомиться по следующим ссылкам: http://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/dv/comp_am_art_01-29/comp_am_art_01-29en.pdf (ст. 1–29), http://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/dv/comp_am_art_30-91/comp_am_art_30-91en.pdf (ст. 30–91).

[2] См. подробнее: *Swire P., Lagos Y.* Why the Right to Data Portability Likely Reduces Consumer Welfare: Antitrust and Privacy Critique // Maryland Law Review. No 72(2). 2013. P. 347–349.

чем в качестве показателя его развития. Сталкиваясь с тем, что право не «справляется» в полной мере с защитой персональных данных пользователей сети Интернет, законодатели реагируют путем дальнейшего ужесточения правового режима, повышая тем самым дополнительные риски и издержки, связанные с его соблюдением. Насколько такая политика оправдает ожидания и приведет к повышенной защите прав граждан, покажет время, но определенная дисбалансированность данного законодательства и отрыв от реальности являются очевидными.

Во-вторых, направлением развития законодательства о персональных данных является разработка дополнительных средств защиты прав несовершеннолетних. В частности, подобно тому, как это имеет место в США (*COPPA Act*), обработка персональных данных субъектов в возрасте меньше 13 лет будет требовать согласия их законных представителей (ст. 8 (1) *GDPR*), при этом оператор должен обеспечить разумные средства для определения возраста, в том числе технологические. Предполагается, что эта мера позволит обеспечить дополнительную защиту наиболее уязвимых категорий субъектов персональных данных, которые не могут осознавать характер и последствия совершаемых владельцами популярных веб-ресурсов действий с их персональными данными.

В-третьих, предполагается значительное упрощение процесса информирования субъекта персональных данных о способах использования персональных данных путем применения специальных графических символов, содержание которых интуитивно понятно и наглядно. В данном случае в качестве источника вдохновения выступили идеи свободных лицензий семейства *Creative Commons*, которые помимо юридического текста лицензии используют графические изображения. Статья 13 (*a*) компромиссного варианта *GDRP* содержит детальное описание символов, которые должны использоваться применительно к определенным видам действий с персональными данными. В частности, они должны указывать: осуществляется ли сбор персональных данных в объеме, превышающем минимально необходимый для целей обработки; обрабатываются ли персональные данные после достижения целей их сбора; обрабатываются ли персональные данные для иных целей, кроме тех, ради которых были собраны; предоставляются ли персональные данные третьим лицам, осуществляющим предпринимательскую деятельность; осуществляется ли продажа персональных данных; осуществляется ли шифрование персональных данных.

Для наглядного доведения до сведения субъекта персональных данных указанных сведений предполагается использование трех колонок, первая из которых содержит графическое обозначение соответствующей операции с персональными данными, вторая – пояснения, а третья – зеленую галочку (если соответствующее условие выполняется) или красный крестик (если соответствующее условие не выполняется).

Введение подобной практики преследует цели обеспечить достаточный уровень информированности субъекта, необходимый для эффективной реализации им своих прав, противодействуя тем самым повсеместной практике включения политик обработки персональных данных в состав *click-wrap-* или *browse-wrap*-соглашений, которые мало кто читает и которые написаны малопонятным языком. Причина такого «безответственного» подхода имеет вполне рациональное обоснование: если субъект персональных данных будет тщательно изучать *privacy policies*, размещенные на каждом сайте, на котором он оставляет свои данные, ему не останется времени ни на что другое. Согласно исследованию, проведенному в США, среднестатистический американец должен затратить приблизительно 201 час, в стоимостном выражении составляющих в среднем 3534 долл., на одно только чтение политик конфиденциальности, размещенных на веб-сайтах, которые он посещает[1]. Очевидно, что в условиях гигантского информационного потока, направленного на современного пользователя сети Интернет, обеспечить более-менее осознанный подход к реализации своих прав, в том числе и в сфере защиты своих персональных данных, возможно при условии существенного облегчения восприятия основных условий их обработки; графический способ их подачи является достаточно эффективным решением[2]. Представляется, что это одно из тех изменений в законодательстве о персональных данных, которое способно принести реальную пользу, превышающую издержки, связанные с его соблюдением.

В-четвертых, предлагается облегчить трансграничную передачу данных путем расширения сферы применения Обязательных корпо-

[1] *McDonald M., Cranor L.* The Cost of Reading Privacy Policies // A Journal of Law and Policy. No 540. 2008. P. 562.

[2] Здесь можно провести параллель со знаками дорожного движения, которые в наглядной и интуитивно понятной форме способны довести необходимую информацию до сведения водителя в кратчайшие сроки. Очевидно, что иной подход (использование текстового сообщения вместо графического) абсолютно неприемлем в ситуациях, когда необходимо принимать решение в минимальные сроки. Путешествие по сети Интернет также можно рассматривать в качестве особого рода «вождения», при котором необходимо оперативное принятие решения.

ративных правил (*Corporate Business Rules*) и формализации требований к ним (ст. 43 *GDPR*). Здесь хотелось бы отметить, что, несмотря на все преимущества, которые данные положения несут для трансграничных компаний, они малоприменимы к малому и среднему бизнесу. Так что проблема обеспечения соблюдения дополнительных условий трансграничной передачи данных остается актуальной для большинства компаний.

Некоторые авторы в связи с этим высказали мнение о том, что положения о трансграничной передаче данных устарели в связи с развитием сети Интернет и облачных технологий. Само по себе место обработки данных не обеспечивает необходимого уровня защиты, все зависит от конкретного оператора и принимаемых им мер. В связи с этим ими предлагается сделать такого оператора ответственным в определенном объеме за действия третьих лиц, которые обрабатывают персональные данные за пределами государства, где проживает субъект, переведя географические соображения из первоочередного фактора во второстепенный[1]. Иными словами, суть предложения сводится к тому, чтобы сделать гарантом соблюдения прав субъекта персональных данных не уполномоченные органы и законодательство страны-«импортера», а оператора, который передает такие данные. Фактически речь идет о распространении принципов, заложенных в положениях о *CBR,* не только на внутрикорпоративные отношения, но и на внешние.

Представляется, что данные предложения заслуживают внимания *de lege ferenda*, учитывая, в какую профанацию на практике превращаются требования об «адекватности» защиты персональных данных в соответствующем государстве. Очевидно, что ни факт наличия определенных норм в законодательстве, ни факт ратификации каких-либо конвенций сам по себе ничего еще не дает с точки зрения наличия реальных гарантий защиты персональных данных для конкретного субъекта. Все зависит от тех организационных и технических мер, которые принял конкретный оператор. А стимулировать его их самостоятельно предпринимать, а не просто отправлять обработку персональных данных на аутсорсинг в третьи страны («где подешевле»), будет вероятность ответственности за действия обработчиков и операторов на территории таких стран. Да и субъекту персональных данных будет гораздо проще обеспечить защиту своих прав, общаясь со «своим» оператором, нежели искать удачи в зарубежных юрисдикциях «с адекватным уровнем защиты» персональных данных. Без-

[1] См. подробнее: *Kuner C.* Op. cit. P. 170–174.

условно, ответственность оператора за третьих лиц не должна быть безграничной, необходима конкретизация оснований и пределов такой ответственности. Но само направление развития законодательства в этой части представляется верным.

В завершение необходимо остановиться еще на одной проблеме, которая пока не получает широкого освещения в отечественной юридической литературе, но определенно получит через некоторое время.

Как известно, законодательство о персональных данных во многом обязано своим появлением и развитием технологиям, обеспечившим возможность их автоматизированной обработки. В связи с этим логично предположить, что революционные изменения в технологиях повлекут необходимость их учета законодательством о персональных данных. И такие технологии уже пришли. Речь идет о методиках обработки больших объемов структурированных и неструктурированных данных для выявления новой информации, представляющей ценность для принятия решений. В технической и аналитической литературе соответствующие технологии получили название «Большие данные» (*Big Data*), а результат их применения в отношении конкретных лиц называется профайлингом (*profiling*). Следует оговориться, что данная категория носит многоаспектный характер и заслуживает отдельной статьи, а может быть, и книги[1]. В контексте проблематики персональных данных необходимо отметить следующее. Ранее уже говорилось о том, что внимание пользователей является одной из основных ценностей в мире электронной коммерции. Для того чтобы завоевать это внимание, необходимо иметь максимум информации о потребностях и предпочтениях пользователя. Каждое действие пользователя, совершаемое в сети Интернет, оставляет определенный «цифровой» след – начиная от информации, которую пользователи добровольно размещают в сети Интернет (в социальных

[1] В частности, технологии *Big Data* лежат в основе систем негласного сбора информации вроде нашумевшей *PRISM*. См.: That NSA Thing – Think about the Data for a Minute, Think about It Differently. 13 June 2013 // http://bigdataandthelaw.com/2013/06/13/that-nsa-thing-think-about-the-data-for-a-minute-think-about-it-differently/. Технологии *Big Data* могут использоваться для борьбы с эпидемиями, позволяя оперативно получать информацию о территории распространения заболеваний из различных данных, распространяемых в сети Интернет, в том числе поисковых запросов. Это убедительно продемонстрировал *Google* в период эпидемии вируса гриппа *H1N1*. См.: *Mayer-Schonberger V., Cukier K.* Big Data: A Revolution That Will Transform How We Live, Work and Think. London, 2013. Обобщенную актуальную статистику заболеваемости гриппом можно посмотреть здесь: http://www.google.org/flutrends/

сетях, высказывания на форумах, «лайки» различного рода новостей и высказывания других пользователей, переписка с использованием публичных почтовых сервисов), и заканчивая той, о наличии которой пользователь может и не подозревать (информация о посещенных сайтах, о совершенных покупках, о географическом месторасположении пользователя и пр.). Если обработать всю эту информацию, можно получить весьма точный портрет («профайл») пользователя и использовать его для принятия решений в отношении такого пользователя: от весьма безобидных – вроде направления адресной рекламы до более «чувствительных» – в виде отказа в приеме на работу, определения кредитного лимита или индивидуализированного размера страховой премии.

Закон о персональных данных в ст. 16 вслед за соответствующими положениями Директивы № 95/46/ЕС предусматривает специальные положения, касающиеся порядка принятия решений, затрагивающих права субъекта персональных данных, исключительно на основании автоматизированной обработки персональных данных. По общему правилу это возможно лишь с письменного согласия субъекта персональных данных и при условии разъяснения ему возможных юридических последствий такого решения и предоставления возможности заявления возражений. Казалось бы, данное положение может быть применено к случаям принятия решений на основании данных, полученных с помощью *Big Data*-аналитики. Однако более детальное их рассмотрение позволяет сделать вывод об их бесполезности в данном случае.

Во-первых, посредством технологий *Big Data* обрабатывается огромный массив информации, лишь часть из которой может быть отнесена к категории персональных данных, многие иные данные носят статистический или обезличенный характер. Во-вторых, нельзя говорить о том, что решение принимается исключительно на основании автоматизированной обработки данных. Результаты аналитики обычно являются основанием для принятия решения уполномоченным лицом, а не самим решением. В-третьих, субъект персональных данных и не узнает о том, использовались ли результаты *Big Data*-аналитики при принятии юридически значимого решения в отношении них, а главное, каковы были исходные данные, которые выступали предметом анализа. Очевидно, что именно здесь кроется основная проблема: в настоящее время субъект не может контролировать оборот информации о нем в сети Интернет, а следовательно, иметь реальную возможность требовать ее исключения или корректировки. Рано или

поздно возникнет необходимость выработки принципиально иных правовых норм, которые бы учитывали данные реалии и обеспечивали более эффективную защиту субъектов персональных данных. И одним только правом «быть забытым» и иными нововведениями *GDPR* здесь не обойтись. Очевидно, что в условиях, когда большинство пользователей добровольно размещают большие объемы персональных данных на различных ресурсах, современные технологии сделали процесс получения информации предельно доступным, ужесточение правовых требований к процессу сбора информации (например, различного рода требования к выражению согласия субъекта персональных данных и т.п.) будет в большинстве своем пустой тратой ресурсов. Вместо этого право должно сконцентрироваться на том, как собранная информация используется, стимулируя разработку и имплементацию технологий, которые минимизировали бы возможности бесконтрольного использования следов жизнедеятельности пользователей в сети Интернет. Но самое главное заключается в осознании того факта, что развитие технологий сделало право на неприкосновенность частной жизни в значительной степени устаревшим[1]. По крайней мере существует очевидный конфликт между теми преимуществами, которые предоставляют современные технологии, и правом на неприкосновенность частной жизни. Развитие информационных технологий демонстрирует устойчивую тенденцию к уменьшению степени *физического* контроля владельца над информацией[2]. Эти очевидные факты необходимо признать и отталкиваться от них при конструировании нового правового режима как для персональных данных, так и для права на неприкосновенность частной жизни в условиях всеобщей компьютеризации.

Первые попытки выработки специального правового режима профайлинга были выработаны в *GDPR* и получили дальнейшее развитие в компромиссном варианте данного документа (ст. 20). Вкратце суть предлагаемых положений можно свести к следующему:

1) каждый гражданин имеет право на заявление возражений в отношении факта осуществления такого профайлинга и его результатов;

---

[1] По выражению Хэла Вэриена (*Hal Varian*), главного экономиста Google, «право на частную жизнь – это нечто из прошлого. С технической точки зрения оно устарело». *Stylianou K.* Hasta La Vista Privacy or How Technology Terminated Privacy // Personal Data Privacy and Protection in a Surveillance Era: Technologies and Practices / ed. by C. Akrivopoulou and A. Psygkas. N.Y., 2011. P. 52.

[2] Ibid. P. 49.

2) профайлинг, который может повлиять на права и обязанности субъекта персональных данных, допустим лишь в трех случаях: когда это прямо предусмотрено Законом, когда он осуществляется в связи с заключением или исполнением договора с данным лицом и когда имеется согласие субъекта персональных данных. При этом такой профайлинг должен предполагать возможность вмешательства человека, в том числе для разъяснений субъекту персональных данных причин принятия того или иного решения на его основе;

3) профайлинг не должен приводить к дискриминации, основанной на признаках расы, этнического происхождения, по политическим и религиозным убеждениям, членстве в профсоюзах, гендерным признакам.

Насколько указанные меры будут способствовать эффективной защите прав граждан, покажет время. Но в любом случае они являются неплохой отправной точкой для дальнейших исследований по данной тематике.

Александр Иванович САВЕЛЬЕВ

ЭЛЕКТРОННАЯ КОММЕРЦИЯ В РОССИИ И ЗА РУБЕЖОМ: ПРАВОВОЕ РЕГУЛИРОВАНИЕ

Редактор *Я.В. Бродневская*
Художественное оформление: *В.В. Самойлова*
Компьютерная верстка: *О.Л. Божьева*

Подписано в печать 06.03.2014. Формат 60×90 $^{1}/_{16}$. Бумага офсетная.
Гарнитура Newton. Печать офсетная. Усл. печ. л. 34. Тираж 500 экз.
Заказ №

Издательство «Статут»:
119454, г. Москва, ул. Лобачевского, д. 92, корп. 2;
тел./факс: +7(495) 649-18-06
E-mail: book@estatut.ru
www.estatut.ru

ISBN 978-5-8354-1018-7

МИЛОГОС
юридический институт

ЮРИДИЧЕСКИЕ СЕМИНАРЫ И КОНФЕРЕНЦИИ В МОСКВЕ

РЕФОРМА ГРАЖДАНСКОГО КОДЕКСА РФ:
комментарии к основным новеллам ГК РФ

ЭФФЕКТИВНАЯ ДОГОВОРНАЯ РАБОТА:
актуальные вопросы реформы ГК РФ и судебной практики

ПРАВОВОЙ РЕЖИМ НЕДВИЖИМОГО ИМУЩЕСТВА И СДЕЛОК С НИМ:
реформа ГК РФ, комментарии к судебной практике и анализ актуальных практических вопросов

ПРАВОВОЕ РЕГУЛИРОВАНИЕ КОРПОРАТИВНЫХ ОТНОШЕНИЙ И СДЕЛОК:
реформа ГК РФ, судебная практика и сопровождение корпоративных процедур и сделок

ДОГОВОРНОЕ ПРАВО В СВЕТЕ РЕФОРМЫ ГРАЖДАНСКОГО КОДЕКСА РФ:
комментарии к основным новеллам ГК РФ

ПРАКТИЧЕСКИЕ ВОПРОСЫ ПОДГОТОВКИ И ВЕДЕНИЯ СУДЕБНЫХ ДЕЛ:
актуальные практические и процессуальные вопросы

ЗАКОНОДАТЕЛЬСТВО ОБ ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ:
практика применения и реформа IV части ГК РФ

ПРАКТИКА ПРИМЕНЕНИЯ ЗАКОНОДАТЕЛЬСТВА О БАНКРОТСТВЕ:
анализ актуальных практических вопросов и новелл законодательства

ПРАКТИКА ПРИМЕНЕНИЯ АНТИМОНОПОЛЬНОГО ЗАКОНОДАТЕЛЬСТВА:
анализ актуальных вопросов и судебной практики

ПРАВОВЫЕ АСПЕКТЫ ЭЛЕКТРОННОЙ КОММЕРЦИИ

ЮРИДИЧЕСКИЙ DUE DILIGENCE:
цели, методы и эффективные технологии

ПРАКТИКА ПРИМЕНЕНИЯ ТРУДОВОГО КОДЕКСА РФ:
защита прав работодателя в современных условиях

ОТДЕЛЬНЫЕ ВИДЫ ГРАЖДАНСКО-ПРАВОВЫХ ДОГОВОРОВ В ПРАКТИКЕ ДОГОВОРНОЙ РАБОТЫ:
актуальные проблемы и судебная практика

ГОСУДАРСТВЕННЫЕ И МУНИЦИПАЛЬНЫЕ ЗАКУПКИ:
актуальные правовые и практические вопросы

СТРОИТЕЛЬНО-ИНВЕСТИЦИОННАЯ ДЕЯТЕЛЬНОСТЬ:
актуальные вопросы правового регулирования и судебной практики

НА МЕРОПРИЯТИЯХ ИНСТИТУТА ВЫСТУПАЮТ ВЕДУЩИЕ РОССИЙСКИЕ ЮРИСТЫ, СУДЬИ И ПРЕДСТАВИТЕЛИ ПРАВОВОЙ НАУКИ

тел.: +7 (495) 771-59-27
+7 (495) 772-91-97
e-mail: info@m-logos.ru
http://www.m-logos.ru