



КонсультантПлюс
надежная правовая поддержка

"Электронная коммерция в
России и за рубежом:
правовое регулирование"
(2-е издание)
(Савельев А.И.)
("Статут", 2016)

Документ предоставлен **КонсультантПлюс**

www.consultant.ru

Дата сохранения: 07.03.2018

ЭЛЕКТРОННАЯ КОММЕРЦИЯ В РОССИИ И ЗА РУБЕЖОМ: ПРАВОВОЕ РЕГУЛИРОВАНИЕ

2-е издание

А.И. САВЕЛЬЕВ

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

ПРЕДИСЛОВИЕ КО ВТОРОМУ ИЗДАНИЮ

За более чем два с половиной года с момента подготовки текста первого издания произошел ряд важных событий: были установлены новые законодательные требования к субъектам электронной коммерции; по ряду ключевых вопросов появилась новая судебная практика; приобрели более явные очертания новые тренды в развитии электронной коммерции, которые нельзя не отразить в работе, посвященной заданной теме. Кроме того, в ходе обсуждений с коллегами и студентами магистратуры НИУ ВШЭ по направлению "Право в сфере IT/IP", где я имею честь преподавать курс по электронной коммерции, отдельных идей, высказанных в первом издании, был выявлен ряд положений, требующих корректировки или дополнительного обоснования. Все это и обусловило подготовку второго издания, общий объем дополненного и переработанного контента в котором составил порядка 40% по сравнению с [первой книгой](#).

Следует обозначить основные новеллы,

нашедшие свое отражение в отдельных главах книги.

Глава 1. Понятие электронной коммерции.

Откорректировано понятие "электронная коммерция" и обновлено описание основных подходов к ее определению, а также основных особенностей сети Интернет, влияющих на правовое регулирование процессов, происходящих в ней. Кроме того, данная глава пополнилась подразделом, посвященным основным трендам развития электронной коммерции (экспансии мобильного сегмента электронной коммерции, "Интернета вещей", технологий добавленной реальности, аналитики данных о пользователях и персонализации коммерции, а также появления новых бизнес-моделей, основанных на экономике совместного использования (**sharing economy**), сопровождающегося обозначением основных правовых вызовов, которые они влекут).

Глава 2. Юрисдикционные аспекты электронной коммерции.

Введены новые подразделы о порядке определения юрисдикции в сфере законодательства о защите персональных данных в Европейском союзе и Российской Федерации, что обусловлено масштабными изменениями, происходящими в указанной области: финализацией процесса подготовки общеевропейского регламента о защите персональных данных и недавно принятыми положениями о локализации отдельных процессов обработки персональных данных на территории РФ. Добавлен анализ вопросов, касающихся использования третейского разбирательства в спорах с участием потребителей. Обновлена судебная практика по остальным вопросам, относящимся к юрисдикции в сети Интернет, а также учтены нововведения в Гражданский процессуальный кодекс РФ по вопросам расширения

правомочий судов общей юрисдикции в отношении споров с участием иностранных лиц.

Глава 3. Договорные аспекты электронной коммерции. Отражены изменения в Гражданском кодексе РФ и иных законах, внесенные за последние два года и влияющие на договорно-правовое регулирование отношений, возникающих в сети Интернет. Приведена новая судебная практика, в частности по спорам, связанным с заключением **click-wrap**-соглашений. Более четкое разграничение получили различные способы заключения договоров в электронной среде: посредством обмена электронными документами и посредством акцепта оферты конклюдентными действиями. Кроме того, данная глава пополнилась рассмотрением проблемных аспектов, связанных с реализацией потребителем права на односторонний отказ от договора купли-продажи товаров, заключенного дистанционным способом.

Глава 4. Процессуальные аспекты электронной коммерции. Глава была дополнена с учетом изменений, внесенных в законодательство о нотариате в части, касающейся обеспечения доказательств в сети Интернет.

Глава 5. Веб-сайт как основной инструмент электронной коммерции. В главе нашли свое отражение новые положения об организаторе распространения информации в сети Интернет в части их возможного применения к различным интернет-сервисам. Более четко структурированы и проанализированы положения о правовой природе интернет-сайта и ответственности его владельца как информационного посредника с учетом изменений, внесенных в часть четвертую Гражданского кодекса РФ.

В **параграф** про доменные споры была добавлена характеристика двух иных процедур рассмотрения споров в указанной области, кроме UDRP - URS и PDDRP.

Глава 6. Цифровой контент и виртуальная "собственность". Глава пополнилась новой судебной практикой, касающейся правового статуса цифрового контента, в том числе анализом известного спора компании **Mail.ru** с налоговыми органами. Были обновлены параграфы про исчерпание прав на цифровой контент с учетом новой европейской судебной практики. Добавлена новая судебная практика по вопросам лицензирования программного обеспечения и предоставления удаленного доступа к его функционалу (**SaaS**). Кроме того, появился **параграф**, посвященный проблемам применения законодательства о защите прав потребителей к отношениям, связанным с потреблением цифрового контента.

Глава 7. Электронные платежи в сфере электронной коммерции. Данная **глава** подверглась наиболее радикальному изменению: был добавлен текст о рассмотрении процесса осуществления платежа в сети Интернет с использованием банковских карт, а также проведен анализ вопросов, связанных с использованием процедур **chargeback**, существенным образом переработаны параграфы, посвященные электронным деньгам и правовому статусу криптовалют на примере **Bitcoin**.

Глава 8. Реклама в сфере электронной коммерции. Учтены положения четвертого антимонопольного пакета, законодательства о маркировке информационной продукции и сделан ряд

других изменений. В части рассмотрения вопросов контекстной (поисковой) рекламы было проведено разграничение правовых режимов законодательства об интеллектуальной собственности, о недобросовестной конкуренции и о рекламе в части ее регулирования и ответственности за нарушения. **Параграф** о спаме был дополнен материалом о рассмотрении вопросов правового регулирования СМС-сообщений и иных адресных уведомлений. Кроме того, был добавлен **параграф**, посвященный анализу правового статуса рекомендаций (отзывов) о товарах или продавце, размещаемых пользователями на различных интернет-сайтах.

Глава 9. Персональные данные в сфере электронной коммерции. Существенным образом был переработан материал про понятие персональных данных: описаны возможные подходы к его определению, отечественная судебная практика и зарубежный опыт. Добавлен подраздел, посвященный анализу новых положений о локализации отдельных процессов обработки персональных данных с учетом разъяснений правоприменительных органов. В этой **главе** также представлен новый материал о соотношении средств защиты, предоставляемых законодательством о персональных данных, законодательством об информации в части "права быть забытым" и обновленными нормами Гражданского **кодекса** РФ о защите чести, достоинства и деловой репутации. Обновлен **параграф** об ответственности за нарушение законодательства о персональных данных с учетом новых законопроектов в указанной сфере, а также существующих положений о блокировках интернет-ресурсов.

Как известно, одним из преимуществ создания

следующей версии ранее написанного текста является возможность внести уточнения, обновить устаревшие данные, заново сформулировать ошибочные или противоречивые утверждения, предложить более подходящие примеры, а также улучшить общую структуру изложения материала. Остается выразить надежду, что данные цели в определенной степени были достигнуты в новом издании.

Конечно, не обошлось и без "жертв". Во имя сохранения общего объема книги на приемлемом уровне пришлось удалить некоторые материалы, касающиеся компаративных, исторических и иных аспектов той или иной проблемы. Однако их отсутствие вполне может быть восполнено посредством обращения к первому изданию книги.

Автор будет признателен за конструктивные комментарии и отзывы, которые могут быть отправлены по электронной почте на адрес: **garantus@rambler.ru**.

Тексты правовых актов даны по состоянию на 1 марта 2016 г.

ПРЕДИСЛОВИЕ К ПЕРВОМУ ИЗДАНИЮ

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.

<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>.

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

<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 конъюнктурно-научный характер.

В **главе 1** книги рассматривается 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, 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 правовых порядков или, наоборот, при желании ограничить риски, связанные с подпаданием под их юрисдикцию. К тому же доктрина и законодательство данных правовых порядков по вопросам юрисдикции отличаются высоким уровнем развития и нередко заимствуются российским законодателем, в связи с чем всегда полезно знать "исток".

В **главе 3** рассматриваются 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 **click-wrap-** и **browse-wrap-** соглашениями 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](#) "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 ограничены. 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 9**, 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 неблагоприятный термин с точки зрения поиска его дефиниции. В отсутствие сформулированного в российском законодательстве определения данного понятия <1> приходится довольствоваться теми дефинициями, которые содержатся либо в зарубежном законодательстве и международных актах, либо в отечественной и зарубежной доктрине.

<1> Данный термин, хотя и без дефиниции, все же употребляется в российских правовых актах. См., например: [Постановление](#) Правительства РФ от 19 марта 2002 г. N 169 "О Федеральной целевой программе "Экономическое и социальное развитие

Дальнего Востока и Забайкалья на 1996 - 2005 и до 2010 года" // СЗ РФ. 2002. N 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. N 990 "Об утверждении Положения о Министерстве экономического развития и торговли Российской Федерации" // СЗ РФ. 2001. N 1 (ч. II). Ст. 125.

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 <1>.

<1> Васильева Н.М. [Электронная коммерция как правовая категория](#) // Юрист. 2006. N 5; 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.

Здесь хотелось бы выделить три основных подхода к определению понятия электронной коммерции.

Первый подход основан на Типовом [законе ЮНСИТРАЛ](#), в руководстве к которому под электронной коммерцией предлагается понимать осуществление торговых сделок с использованием различных электронных средств передачи данных (передачи электронных сообщений стандартизированного формата между компьютерами (**EDT**), сети Интернет,

телекса, телефакса, факсимильных сообщений и пр.) <1>. При этом отмечается, что такой широкий подход во многом обусловлен идеологией данного Типового **закона**: чем более широка сфера его применения, тем в большей степени достигаются его цели <2>.

<1> См.: Типовой **закон** об электронной торговле и Руководство по принятию. ЮНСИТРАЛ 1996 г. С. 17 - 18. URL: http://www.uncitral.org/pdf/russian/texts/elect-com/05-89452_Ebook.pdf. Следует отметить, что в русскоязычной версии Типового **закона** термин "electronic commerce" переведен как "электронная торговля", что вряд ли можно считать удачным переводом, учитывая сложившееся в русском языке понимание понятия "торговля" (см. далее).

<2> **Там же**. С. 18.

Второй подход характеризуется тем, что понятие электронной коммерции ограничивается лишь сделками, которые заключены **посредством сети Интернет**. В подобном ключе электронная коммерция рассматривается, 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; данный термин также включает предоставление доступа к Интернету" <1>. 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**" <2>. Как следует из вышеуказанных определений, основным конститутивным признаком электронной коммерции является транзакция (сделка), совершенная с использованием Интернета.

<1> Section 1104 (3). The Internet Tax Freedom Act, 1998.

<2> 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.](#)

Третий подход представляет собой специализированный вариант второго. Под электронной коммерцией предлагается понимать покупку или продажу товаров (услуг) посредством компьютерных сетей с помощью средств, **специально предназначенных для размещения или получения заказов**. Здесь ключевое значение имеет используемый технический способ заключения договора: это должен быть специально приспособленный для таких целей механизм, например форма заказа на интернет-сайте или специализированное приложение смартфона. При этом так же, как и во втором подходе, из понятия электронной коммерции исключаются договоры,

заключенные посредством телефонного звонка, телекса или факса. Кроме них здесь также исключаются договоры, заключаемые посредством обычной электронной почты.

Рассматриваемый подход используется такими международными организациями, как Всемирная Торговая Организация (ВТО) и Организация по Экономическому Сотрудничеству и Развитию (ОЭСР) <1>. Во многом он предопределяется стремлением привести понятие электронной коммерции к общему знаменателю для статистических и экономических целей. Хотя он находит определенное отражение и на уровне законодательства и практики отдельных стран <2>.

<1> E-Commerce in Developing Countries: Opportunities and Challenges for Small and Medium-Sized Business. World Trade Organization. URL: https://www.wto.org/english/res_e/booksp_e/ecom_brochure_e_e.pdf; OECD Glossary of Statistical Terms. Electronic Commerce. OECD Guide to Measuring the Information Society, 2011. URL: <https://stats.oecd.org/glossary/detail.asp?ID=4721>.

<2> Так, в решении Верховного суда Филиппин было отмечено, что филиппинское законодательство об электронной коммерции не охватывает случаи заключения договоров по телефаксу, телексу, телеграммам и иным подобным средствам связи, из чего, по мнению суда, усматривается намерение законодателя ограничить применение норм об электронной коммерции исключительно к случаям обмена электронными сообщениями посредством сетей связи. MCC Industrial Sales Corporation v. Ssangyong

Corporation. 17 October 2007. Цит. по.: Unlocking the Potential of E-commerce for Developing Countries. United Nations Conference on Trade And Development. N.Y., 2015. P. 69.

Оценивая приведенные подходы к определению электронной коммерции, хотелось бы отметить следующее.

Во-первых, факсы, телексы, телефаксы и другие подобные средства связи, несмотря на наличие в них электронной составляющей, вряд ли 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 для передачи информации (например, звук или видео с их помощью не передашь), не позволяют осуществлять одновременное общение и содержат ряд иных недостатков. Кроме того, данные ограничения обуславливают тот факт, что многие актуальные вопросы электронной коммерции просто не возникают при использовании подобных технических средств из прошлого века: конфликт юрисдикций вследствие общедоступного характера 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?

В конечном счете сфера электронной коммерции получила свое масштабное развитие только с приходом Интернета <1>. Именно сочетание развития рынка в сфере интернет-услуг, технологий в области дизайна веб-сайтов и новых вычислительных технологий в итоге и привело к появлению нового поколения коммерции - электронной коммерции <2>. 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 <3>. Доступ к современным телекоммуникационным системам признавался в ВТО ключевым элементом понятия "электронная коммерция" еще в далеком 1998 г. <4>. При этом особо подчеркивалось, что именно сеть Интернет позволяет осуществлять все этапы транзакции в электронной форме <5>. Таким образом, не отрицая исторической значимости иных электронных видов связи, приходится сделать вывод о том, что они не играют той роли в современной структуре электронной коммерции, которая обуславливала бы целесообразность их включения в ее понятие. Напротив, такое включение будет "размывать" понятие электронной коммерции, поскольку им, по сути, будет охватываться любая сделка, заключенная не в устной форме и не на бумаге, что явно не соответствует существу данного понятия.

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

<2> См.: Faye Fangrei Wang. Internet Jurisdiction and Choice of Law: Legal Practices in the EU, US and China. Cambridge, 2010. P. 3.

<3> Юрасов А.В. Основы электронной коммерции. М., 2008. С. 27 - 28.

<4> WTO Declaration on Global Electronic Commerce. 20 May 1998 WT/MIN(98)/DEC/2. § 5.

<5> Ibid. § 20.

Во-вторых, признавая прогрессивность третьего подхода, следует отметить, что он не позволяет в полной мере охватить все формы электронной коммерции, которые используются на практике и могут представлять интерес для юридического анализа. Имеются в виду, в частности, случаи, когда интернет-сайт используется для информационной поддержки традиционного офлайн-бизнеса, а договор заключается посредством обмена электронными письмами с использованием контактных данных, полученных на таком сайте. Возникающие в связи с этим юрисдикционные, договорно-правовые, процессуальные вопросы заслуживают внимания не в меньшей степени, чем при заключении договора с использованием автоматизированных средств размещения заказа онлайн.

С учетом вышеизложенного представляется, что целям настоящей работы лучше всего отвечает следующее определение понятия электронной

коммерции (основанное на втором подходе):
"Электронная коммерция - совокупность отношений, возникающих в связи с заключением сделок посредством сети Интернет, а также при продвижении товаров, работ, услуг и иных объектов гражданских прав в сети Интернет <1>. Таким образом, ядром понятия электронной коммерции является сделка, совершенная посредством Интернета. При этом необязательно, 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.

<1> Данное определение не отвечает признакам технологической нейтральности, так как прямо упоминает определенную технологию (Интернет) в качестве конститутивного признака. Признавая справедливость этого аргумента, полагаю, что можно было бы усовершенствовать данную дефиницию, используя 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.

Кроме того, принимая во внимание, 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 целесообразно включить в понятие электронной коммерции. В таких случаях налицо тесная взаимосвязь между преддоговорным и договорным аспектами, которая обуславливает не только наличие специального регулирования преддоговорного аспекта <1>, но и целесообразность совместного и целостного рассмотрения данных вопросов в рамках работы, посвященной электронной коммерции.

<1> См., например: Федеральный [закон](#) от 13 марта 2006 г. N 38-ФЗ "О рекламе" (далее - Закон о рекламе); [ст. ст. 9, 10](#) Закона РФ от 7 февраля 1992 г. N 2300-1 "О защите прав потребителей" (далее - Закон о защите прав потребителей) о праве потребителя на достоверную информацию о товаре (услуге) и контрагенте (изготовителе (продавце)).

Следует отметить, что по сравнению с [первым изданием](#) настоящей книги, понятие электронной коммерции претерпело некоторые уточнения <1>. Во-первых, из него ушло указание на связь соответствующих отношений с предпринимательской деятельностью. Данный подход представляется более корректным, учитывая общепринятый характер выделения C2C сегмента электронной коммерции, а также развитие экономических моделей, построенных на началах "совместного использования" (**sharing**

economy) (см. далее). Во-вторых, более четко артикулирован основной конститутивный признак электронной коммерции - наличие сделки, заключенной посредством Интернета, и (или) деятельности по продвижению бизнеса в сети Интернет. Таким образом, не всякое действие, связанное с осуществлением предпринимательской деятельности с использованием Интернета, должно относиться к электронной коммерции **per se**, а лишь то, которое предполагает использование данной сети для извлечения прибыли от действий правомерного характера. Совершение акта недобросовестной конкуренции посредством распространения ложных сведений на интернет-ресурсе о конкурирующей компании, безусловно, имеет связь и с предпринимательской деятельностью, и с сетью Интернет, но, разумеется, не должно в силу этого признаваться электронной коммерцией.

<1> Дефиниция **первого издания** книги звучала следующим образом: "Электронная коммерция представляет собой совокупность отношений, возникающих в связи с ведением предпринимательской деятельности в сети Интернет, в частности, при совершении сделок, а также продвижении товаров, работ, услуг и иных объектов в сети Интернет.

Наконец, необходимо сказать несколько слов о термине "электронная торговля". Представляется, что он не является заменой понятия "электронная коммерция" <1>, а выступает лишь одной из разновидностей последней. Под торговлей обычно принято понимать виды экономической деятельности по осуществлению купли-продажи товаров, обмену ими, а также связанные с ними процессы подготовки товаров к продаже, их хранению, доставке и т.п. В российском

законодательстве под торговой деятельностью понимается вид предпринимательской деятельности, связанный с приобретением и продажей товаров <2>. Иными словами, в основе понятия торговли лежит товар, в качестве которого, с точки зрения российского гражданского законодательства, может выступать не любой объект гражданских прав, а лишь вещь (п. 1 ст. 455 ГК РФ). Исходя из системного подхода к применению законодательства, понятие электронной торговли можно определить как деятельность по приобретению и продаже товаров посредством сети Интернет. При таком подходе понятие электронной торговли не включает в себя деятельность по реализации услуг и цифрового контента в Интернете, а сводится, по сути, к интернет-ритейлу. Это представляет собой неоправданное сужение сферы электронной коммерции и входит в противоречие с общепринятым подходом, исходя из которого в качестве объекта электронной коммерции могут выступать любые оборотоспособные объекты гражданских прав. Во избежание терминологической путаницы представляется нецелесообразным использование термина "электронная торговля" в качестве синонима электронной коммерции.

<1> Об использовании понятия "электронная торговля" в законопроектной деятельности см. [первое издание](#) данной книги. С. 17 - 19.

<2> См.: Федеральный закон от 28.12.2009 N 381-ФЗ "Об основах государственного регулирования торговой деятельности в Российской Федерации" (п. 1 ст. 2). В соответствии с Общероссийским классификатором видов экономической деятельности ОК 029-2001 (ОКВЭД) к электронной торговле относится

розничная торговля, осуществляемая через телемагазины и компьютерные сети, включая Интернет (код по ОКВЭД [52.61.2](#)).

В завершение 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 <1> 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. Таким образом, **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

ТСР/IP тоже направлен на унификацию "языка общения" между различными сетями и компьютерами в их составе. Так или иначе, с появлением сети Интернет большинство компаний, желающих заниматься электронным бизнесом, перешли на использование Интернета в качестве средства коммуникаций с бизнес-партнерами <2>.

<1> 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. N 20-П).

<2> Prins C. et al. Trust in Electronic Commerce. Kluwer Law International, 2002. P. 12.

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 <1>. 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 <2>. Поэтому представляется целесообразным там его и оставить, не упоминая без особой надобности при рассмотрении правовых аспектов электронной коммерции.

<1> В соответствии с п. 11.1 ст. 2 Федерального закона от 27 июля 2006 г. N 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.

<2> См., например: распоряжение Правительства РФ от 6 мая 2008 г. N 632-р "О Концепции формирования в Российской Федерации электронного правительства до 2010 года"; Постановление Правительства РФ от 6 сентября 2012 г. N 890 "О мерах по совершенствованию электронного документооборота в органах государственной власти" и ряд других документов.

§ 2. Классификация отношений, возникающих в сфере электронной коммерции

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

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 и прочие инструменты получения обратной связи от потребителей. Обычно такая информационная поддержка сопровождается размещением рекламы в Интернете (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 (см. таблицу): 1) **Business-to-Consumer (B2C)**; 2) **Business-to-Business (B2B)**; 3) **Consumer-to-Consumer (C2C)**; 4) **Business-to-Government (B2G)** <1>.

<1> Schneider G. Electronic Commerce. Course Technology. Mass. 9th ed. 2011. P. 7.

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 <1>



<1> [Глава 3.1](#) Федерального закона от 21 июля 2005 г. N 94-ФЗ "О размещении заказов на поставки товаров, выполнение работ, оказание услуг для государственных и муниципальных нужд".

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

<1> См. [п. 5](#) Постановления Пленума ВАС РФ от 22 октября 1997 г. N 18 "О некоторых вопросах, связанных с применением положений Гражданского кодекса Российской Федерации о договоре поставки".

<2> Федеральный [закон](#) от 21 июля 2005 г. N 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. N 44-ФЗ "О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд").

В рамках данной работы будут рассмотрены вопросы, характерные для отношений, возникающих в сфере электронной коммерции в **B2B-** и **B2C-**секторах. **C2C-** и **B2C-**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 потребуются детальный анализ правовых аспектов возникающих в связи с этим отношений.

В любом случае, к какому сегменту ни 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. Основные тенденции развития электронной коммерции

Рассмотрев понятие электронной коммерции и ее основные виды, целесообразно остановиться на кратком описании основных направлений ее развития.

Это связано с тем, что многие актуальные проблемы, формирующие повестку дня правового регулирования электронной коммерции (по крайней мере, в большинстве развитых стран), заданы перспективными направлениями развития электронной коммерции, которые в свою очередь предопределяются направлениями развития информационно-коммуникационных технологий <1>. К основным трендам электронной коммерции можно отнести следующие.

<1> Общее представление о направлениях развития информационных технологий в России и мире на ближайшие 15 лет можно получить в кн.: Прогноз научно-технологического развития России: 2030 г. Информационно-коммуникационные технологии / Под ред. Л.М. Гохберга и И.Р. Агамирзяна. М.: НИУ ВШЭ, 2014. URL: https://prognoz2030.hse.ru/data/2014/12/25/1103939133/Pr ognoz_2030_final.pdf.

1. Разрастание мобильного сегмента. Аудитория мобильного Интернета за декабрь 2013 - 2014 г. выросла на треть. Доля пользователей, выходящих в Интернет в этот же период со смартфонов, составила около 39%, с планшета - 25%, в то время как около 10% пользователей выходит в Интернет исключительно с мобильных устройств (телефонов) <1>. Все это влечет возрастание роли мобильных телефонов в качестве основного средства аутентификации пользователей в сети Интернет. Кроме того, это обуславливает необходимость учета и адаптации классических требований законодательства о защите прав потребителей, законодательства о персональных данных к специфике мобильных

устройств (ограниченному объему воспринимаемой пользователем информации, ограничениям трафика и пр.).

<1> По данным издания "Интернет в цифрах". Март-апрель 2015 г. // www.in-numbers.ru.

2. Увеличение роли социальных сетей в процессах, связанных с электронной коммерцией. Количество пользователей социальных сетей достигло 91% всех пользователей сети Интернет (98% - молодежная аудитория) <1>. При этом аудитория пользователей в сегменте 12 лет - 24 года большую часть времени, проведенного в Интернете (29%), отводит именно социальным сетям. В ряде стран этот показатель еще выше. Так, в Индонезии 9 из 10 пользователей, имеющих доступ к Интернету, обладают также аккаунтом в социальной сети, а, столица Индонезии - Джакарта носит неофициальное наименование мировой столицы Facebook'a (около 17 млн. пользователей Сети) <2>. Увеличение количества времени, проведенного в социальных сетях, влечет возрастание количества информации, оставляемой пользователем, а следовательно, большие возможности использования данных аналитики для адресного продвижения товаров, работ и услуг. В условиях перегруженности пользователя информацией его внимание становится основной ценностью. Без средств аналитики данных и повышения посредством нее вероятности того, что предложение товара (услуги) является действительно востребованным, интернет-компании не смогут обеспечивать свой рост. Сложившаяся ситуация повышает "нагрузку" на законодательство о персональных данных (с которой, как будет показано в [гл. 9](#) настоящей книги, оно уже не

справляется) и рекламе, а также на средства контроля над прозрачностью и справедливостью соглашений, заключаемых в сети Интернет в полуавтоматическом режиме (click-wrap, browse-wrap-соглашения).

<1> Исследование "Пользование социальными сетями в России. 2012 - 2015 гг." // <http://adindex.ru/news/researches/2015/05/21/123757.phtml>

.

<2> Unlocking the Potential of E-commerce for Developing Countries. United Nations Conference on Trade And Development. N.Y., 2015. P. 27.

3. **Появление и экспансия экономики нового типа и связанных с ней бизнес-моделей - экономики "совместного использования".** Данный вид экономики получил различные наименования в иностранной литературе (**sharing economy, renting economy, collaborative economy, ICT-enabled economy, digital platform economy**) <1>. В самом общем виде ее суть сводится к тому, что при посредничестве интернет-платформ формально незнакомые люди находят друг друга и делятся друг с другом определенными активами, происходит так называемый процесс разобладания (**disowner-ship**), при котором брать что-либо в пользование гораздо выгоднее приобретения его в собственность. Наиболее успешными примерами компаний, имплементировавших бизнес-модели, основанные на "новой экономике", являются **Uber** (компания из Сан-Франциско, создавшая одноименное мобильное приложение для поиска, вызова и оплаты такси или частных водителей) <2>, **Airbnb** (онлайн-площадка для размещения, поиска и краткосрочной аренды частного жилья по всему миру),

Lyft (компания из Сан-Франциско, позволяющая пользователям находить с помощью интернет-сайта или мобильного приложения водителей, сотрудничающих с сервисом и готовых подвезти их за умеренную плату). Фактически в основе данных бизнес-моделей лежит организация коммуникаций экономических субъектов с минимальными издержками, которая обеспечивается интегрированием инноваций последних лет (геолокации, мобильных платежей, удаленного менеджмента людей посредством программного продукта, выступающего интерфейсом между физическим и онлайн-мирами). Новый тип экономики извлекает стоимость из социальных связей между чужими друг другу людьми, в связи с чем фактор доверия является ключевым для ее жизнеспособности. Например, пользователи компании **Lyft** доверяют свою жизнь незнакомым водителям, подвозящим их, куда нужно, а пользователи компании **Airbnb** полагаются на владельцев жилья, у которых останавливаются, находясь в дороге. Фактор доверия в большинстве своем обеспечивается средствами саморегулирования и морального контроля, действующими через набираемые в онлайн-сообществе баллы репутации и подтверждение идентичности по профилям в социальных сетях. Как следствие, экономика совместного использования функционирует на таких условиях, при которых ответственности и риски непрозрачны и распределены неравномерно <3>. При этом нередко определить, кто из пользователей таких платформ выступает потребителем, а кто предпринимателем, весьма непросто, учитывая, что одно и то же лицо может одновременно выступать в обоих качествах. Кроме того, не понятна возможная степень ответственности самих интернет-платформ за действия своих пользователей: должна ли она наступать, и если да, то при каких условиях? Подпадают ли представляемые ими сервисы под действие

законодательства о защите прав потребителей? Все эти вопросы, на которые нет пока удовлетворительных ответов, иллюстрируют необходимость существенной адаптации действующих правовых норм, а при ее невозможности (о которой может свидетельствовать, в частности, значительная социальная напряженность вокруг сервиса "Uber", выливающаяся порой в массовые беспорядки) - выработки новых правил регулирования отношений между субъектами - экономики совместного использования.

<1> New Forms of Work in the Sharing Economy. OECD Working Party on Measurement and Analysis of the Digital Economy. DSTI/ICCP/ISS(2015) 3. For Official Use.

<2> В определенный момент времени капитализация компании Uber составила 50 млрд. долларов. См.: Kosoff M. Uber is officially a \$50 billion company // Business Insider, 31 July 2015. URL: <http://goo.gl/MOQBil>. В связи с этим в деловом обороте часто используется термин "уберизация экономики" как синоним термина "экономика совместного использования".

<3> Essays on the sharing economy by Shehzad Nadeem, Juliet B. Schor, Edward T. Walker, Caroline W. Lee, Paolo Parigi, and Karen Cook. February 23, 2015. URL: <http://contexts.org/articles/on-the-sharing-economy/>.

4. Развитие Интернета вещей. Традиционное понимание Интернета как средства коммуникации пользователей между собой будет постепенно вытесняться использованием Сети для взаимодействия различных устройств между собой. К 2020 г. ожидается, что к сети Интернет будет подключено более 50 млрд.

"умных" устройств <1>. Если сейчас большую часть покупок в Интернете делает пользователь, то в перспективе значительная часть таких покупок может осуществляться самими устройствами в соответствии со специальными алгоритмами. Концепция "умного" холодильника, который отслеживает запасы еды и сроки годности и сам размещает заказы на еду в близлежащем супермаркете, уже давно не является фантастикой. Потенциал Интернета вещей не исчерпывается исключительно потребительским сегментом, большие перспективы открываются и в индустриальном Интернете, где физические устройства промышленного назначения, оснащенные сенсорами и интегрированные с интеллектуальными системами, могут оперативно размещать заказы на недостающие детали или ремонт поврежденных компонентов. Физический мир постепенно превратится в разновидность информационной системы. Интернет вещей приводит к распространению полностью автоматизированных договоров, заключаемых электронными агентами. Право должно определить условия действительности таких договоров и пределы ответственности сторон за ошибки, допущенные их электронными агентами. Другой проблемой, возникающей в связи с развитием "Интернета вещей" является информационная безопасность: кто будет контролировать данные, полученные с таких устройств, и как они будут использованы? Учитывая, что многие устройства, подключенные к сети Интернет, могут оказывать влияние на жизнь и здоровье их обладателя (от устройств медицинского назначения до различного рода автомобилей и промышленных устройств), вопросы информационной безопасности начинают тесно переплетаться с физической безопасностью <2>. Неясно, однако, кто должен нести ответственность за возможный ущерб и вред здоровью, причиненный устройством: производитель самого устройства,

производитель программного обеспечения, провайдер сервиса (например, спортивный клуб, который выдал фитнес-трекер клиенту для оптимизации процесса тренировок)? А если еще учесть имеющуюся в ряде случаев возможность установления пользователем соединения между различными IoT-устройствами, то возможность предвидения последствий таких действий сильно ограничена <3>. Пока на данные вопросы вразумительных ответов не дано ни в России, ни за рубежом.

<1> The Internet of Things: How the Next Evolution of the Internet Is Changing Everything. Cisco White Paper. April 2011. P. 3.

<2> Следует отметить, что Интернет вещей не является возможным апогеем эволюции развития Интернета. На подходе уже Интернет индивидуумов (Internet of Persons), при котором человек посредством имплантированного микрочипа с подключением к сети Интернет, по сути сам становится частью инфраструктуры Интернета. См.: Klitou D. Privacy-Invasive Technologies and Privacy by Design: Safeguarding Privacy, Liberty and Security in the 21st Century. Springer; Leiden, 2014. P. 160 ff.

<3> The Internet of Things: An Overview. Understanding the Issues and Challenges of a More Connected World. Internet Society. October 2015. P. 57.

5. Внедрение технологий "добавленной реальности" (Augmented reality) в электронную коммерцию. В самом общем виде данные технологии представляют собой соединение реального и виртуального миров, при котором восприятие человеком

реального мира расширяется за счет цифровых данных, поступающих в реальном времени в форме, доступной для непосредственного восприятия человеком (на экран мобильного телефона или планшета, лобовое стекло автомобиля, изображение в очках и пр.) <1>. Уже сейчас существуют приложения, которые позволяют при наведении смартфона на определенный объект получить информацию о нем <2>. Эти технологии обеспечивают возможность пользователя получить необходимую информацию о товарах с минимальными затратами времени и сил. В частности, они предоставляют пользователю возможность ознакомления с виртуальным 3D-аналогом товара, используя лишь смартфон (планшет) и специальное программное приложение. Все эти технологии позволяют в определенной степени выровнять информационный дисбаланс между потребителем и предпринимателем, на котором зиждется существующее законодательство о защите прав потребителей, и по-новому взглянуть на концепцию дистанционной купли-продажи товаров.

<1> Kipper G., Rampolla J. Augmented Reality: An Emerging Technologies Guide to AR. Syngress, 2013. P. 1.

<2> Smalley E. Your Phone will Soon Recognize Things it Sees (<http://www.cnet.com/news/your-phone-will-soon-recognize-things-it-sees>). В качестве примера можно указать приложение Layar (<https://www.layar.com>) - браузер расширенной реальности, предоставляющий информацию об объекте, местонахождение которого определяется с помощью GPS-приемника и цифрового компаса, при наведении на него камеры смартфона.

6. **Развитие технологии "Блокчейн" (Blockchain).** Данная технология, впервые реализованная в криптовалюте **Bitcoin** (см. § 4 гл. 7 настоящей книги), иногда именуется второй по значимости после Интернета <1>. В самом общем виде **Блокчейн** можно определить как децентрализованную распределенную базу данных ("учетную книгу") всех подтвержденных транзакций, совершенных в отношении определенного цифрового актива, в основе функционирования которой лежат криптографические алгоритмы. Данная технология позволяет: а) фиксировать достоверные данные о принадлежности существующего в цифровой форме актива определенному лицу без необходимости привлечения какого-либо специализированного посредника, в силу чего является сильным фактором дезинтермедиации экономики; б) обеспечить возможность непосредственной передачи такого актива другому лицу. Таким образом, в перспективе она способна осуществить значительную дезинтермедиацию (устранение посредников) в экономике: банки, нотариусы, депозитарии реестров данных становятся лишними в условиях, когда их работа может быть заменена надежными и устойчивыми к изменениям математическими алгоритмами. Однако наиболее революционные изменения технология **Блокчейн** может осуществить в договорном праве. Она может быть использована для создания так называемых умных контрактов (**Smart contracts**) - полностью автоматизированных, запрограммированных контрактов, т.е. таких соглашений, которые могут заключаться и исполняться без участия человека. По сути, "умные" контракты представляют собой альтернативу целой правовой системе и потребуются немало усилий для того, чтобы "прописать" их в существующие каноны договорного права, адаптировав понятия "обязательство", "обязанность", "кредитор",

"должник" и ряд иных к новым реалиям.

<1> Martin Hiesboeck. Blockchain is the most disruptive invention since the Internet itself - not just in finance. 6 April 2016. Digital Doughnut. URL: <https://goo.gl/9jSYF8>.

Безусловно, данный обзор трендов электронной коммерции не претендует на исчерпывающий характер, однако эти направления будут в значительной степени определять ее дальнейшее развитие, в том числе влиять на правовое регулирование в указанной сфере. В последующих главах книги будут раскрыты отдельные вопросы, связанные с обозначенными трендами. Однако большая часть базовых проблем правового характера, возникающих в сфере электронной коммерции, в основной массе является следствием "архитектуры" сети Интернет, что обуславливает целесообразность рассмотрения отдельных технических аспектов ее функционирования.

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

Особенности технической "архитектуры" сети Интернет в большинстве своем предопределены историческими особенностями разработки и создания данной сети. В итоге то, что изначально рассматривалось как неоспоримое преимущество Интернета с технической точки зрения, на определенном этапе ее развития создало проблемы, с которыми классическое, "аналоговое" право оказалось не в силах справиться.

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. Вера американцев в свои армию, науку, технологии, политическую систему и даже в свои фундаментальные ценности была подорвана. Как отмечается, "никогда еще столь малый и безобидный объект не вызывал столько ужаса" <1>. 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 <2>. 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.

<1> Кин Э. Ничего личного: Как социальные сети,

поисковые системы и спецслужбы используют наши персональные данные. М.: Альпина Паблишер, 2016. С. 28.

<2> Ryan J. A History of Internet and the Digital Future. London, 2010.

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. Таким образом, история Интернета началась не столько с инноваций, сколько со страха.

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 <1>. К тому же реализация данного проекта позволяла Агентству не только приобщиться к решению вопросов общенационального масштаба, но и решить собственные проблемы: все компьютеры, используемые американскими университетами и подрядчиками, приобретались за счет Агентства, и оно было постоянно завалено запросами на приобретение новых компьютеров, поскольку вычислительной мощности 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 <2>. Это позволило

бы объединить географически разрозненных ученых вместе, создав сообщество талантов, работающих над решением определенной проблемы <3>.

<1> Таким образом, говорить о том, что Интернет является проектом ЦРУ, можно, но только при готовности погрешить при этом против истины.

<2> Внимательный к современным технологиям читатель увидит здесь прообраз популярной ныне концепции "облачных" вычислений (**Cloud Computing**).

<3> 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 в наши дни движения **open source**, высказывались еще в середине 60-х гг. XX в. и были положены в основу создания сети Интернет.

В 1969 г. была создана сеть, построенная на принципах децентрализации (по принципу "от пользователя к пользователю", а не "от центра к центру") и пакетной передачи данных (сообщение отправлялось не как единое целое, а по частям, которые передавались по Сети от узла к узлу в произвольном порядке с последующим воссоединением на компьютере адресата, что защищало сообщение от шпионажа), соединившая четыре компьютера, расположенные в Калифорнийском университете в Лос-Анджелесе (**UCLA**), Калифорнийском университете в Санта-Барбаре, Университете штата Юта и Стэндфордском научно-исследовательском институте. 29 октября 1969 г. первое сообщение с компьютера на

компьютер было направлено из университета **UCLA** в Стэнфордский научно-исследовательский институт, однако вместо планированного слова "login" удалось переслать только буквы "lo", после чего сеть дала сбой, однако через час уже была восстановлена и сообщение было передано целиком. Так появилась сеть **ARPANET**, которую обычно считают прародительницей современного Интернета <1>.

<1> 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.

Но **ARPANET** еще не был Интернетом в его современном понимании. Для появления Интернета необходимо было разработать универсальный протокол, который бы позволил разнородным сетям взаимодействовать друг с другом. И такой протокол 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. В силу существенных различий таких сетей необходимо было выработать новые подходы к организации взаимодействия между ними. Так появилась программа Интернет (от англ. **Internetwork** - сеть между сетями). 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 и плотного надзора со стороны военного ведомства. 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>.

<1> В качестве примера можно привести сеть "GLORIAD", запущенную 12 января 2004 г. и объединяющую научно-исследовательские центры России, США, Китая и еще целого ряда 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. 2007. N 5. P. 469. Гениальная идея основной сети, соединяющей остальные, заключалась в "инкапсуляции". Как сказал Винстон Серфф, "мы считали это конвертами". "Инкапсуляция" означает упаковку информации из локальных сетей в этакий "конверт", который объединенная сеть сможет распознать и переправить дальше. Это можно сравнить с почтовыми службами разных государств, которые договорились писать названия стран по-английски, даже если местный адрес - на японском или хинди. См.: Tim Wu. The Master Switch: The Rise and Fall of Information Empires. N.Y., 2011. P. 198.

Управление связи Министерства обороны США, осуществляющее функции оператора сети, обрадовалось появлению нового протокола и установило жесткие требования по миграции существующих сетей на него, которую надо было завершить к январю 1983 г. Те, кто не успел осуществить переход на **TCP/IP** к указанному сроку, были просто отключены от сети <1>. Режим пользования разросшейся сетью также 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. А 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.

<1> Abbate J. Op. cit. P. 141.

Но со временем эра **ARPANET** приходила к концу. Сеть, возраст которой уже переваливал 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 **"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. Соответственно, любая организация, которая подавала запрос на подключение к **NSFNET**, должна была подписать Правила допустимого использования, ограничивавшие ее использование исследовательскими и образовательными целями <1>. Нетрудно догадаться, что столь жесткий подход не приветствовался пользователями, число которых с каждым годом все возрастало, в том числе среди коммерческих организаций <2>. 30 апреля 1995 г. **NSFNET** была окончательно расформирована, а 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 включал в себя 22000 иностранных сетей <3>. 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.

<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> Abbate J. Op. cit. P. 210. В их числе был и российский сегмент сети Интернет. В декабре 1993 г.

образованная в 1990 г. на базе Курчатовского университета сеть "Relcom" была зарегистрирована в опорной сети США - NSFNET, что ознаменовало получение полного доступа к сети Интернет из России. 7 апреля 1994 г. была зарегистрирована доменная зона "ru", что ознаменовало появление рунета - российского сегмента сети Интернет.

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, использующем специальную программу - браузер <1>. Благодаря **WWW** Интернет стал мультимедийным: графическое и звуковое сопровождение стало неотъемлемой частью многих ресурсов сети.

<1> Yee Fen Lim. Cyberspace Law: Commentaries and Materials. Oxford, 2002. P. 11 - 13.

WWW позволила использовать Интернет не только преимущественно как средство общения, но и как источник информации. Недаром 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 с 1995 г.) можно говорить о начале новой эпохи сети Интернет - эпохи электронной коммерции. Многие коммерческие компании (**Dell, Cisco** и др.) открывают свои веб-сайты в сети Интернет и

начинают их активно использовать в коммерческой деятельности. Регистрация доменных имен приобретает платный характер. 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**). Потенциал Интернета в сфере электронной коммерции был значительно усилен появлением первой поисковой системы **AltaVista**, которая "понимала" естественный язык <2>. Можно долго перечислять все последующие инновации, которые произошли в сети Интернет с тех пор, но все они (или по крайней мере большая часть) связаны с развитием ее коммерческого потенциала, поэтому для целей обозначения фундаментальных архитектурных особенностей сети Интернет можно уже сейчас обозначить некоторые выводы.

<1> Reno v. ACLU, 521 U.S. 844, 853 (1997).

<2> В 2003 г. данная поисковая система была поглощена компанией "Yahoo!" и в 2013 г. прекратила работу.

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. А когда ученым предоставляют свободу, они способны придумывать удивительные вещи. Реализованная в итоге по заказу военных 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 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. Эта структура в целом устраивала и "заказчика" - военные ведомства США, которые без труда и особых адаптаций "встроили" ее в уже существующие системы формальных правил.

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".

Персональный компьютер стал прямой противоположностью мейнфреймов IBM System 360, которые стоили миллионы долларов и занимали место размером с комнату. По сути, персональный компьютер

взял всю вычислительную мощь, в то время сконцентрированную у государства, в крупных компаниях и институтах, и отдал ее в руки отдельных людей. Такая демократизация технологической силы практически не имеет прецедентов. В те времена подобное казалось почти невыносимым: обычное устройство сделало простых людей властелинами информации благодаря компьютерным технологиям, которые они могли использовать для личных нужд <1>.

<1> См.: Tim Wu. The Master Switch: The Rise and Fall of Information Empires. N.Y., 2011. P. 270.

В свою очередь **WWW**, сделав Интернет более "дружелюбным" для среднестатистического пользователя, а также обеспечив возможность отображения графических изображений, создала благоприятные условия для электронной коммерции, что предопределило постепенный процесс трансформации Интернета в нечто все более и более регулируемое <1>. Пространство для "инноваций без разрешения" в среде Интернета начало становиться все меньше и меньше.

<1> Lessig L. Code. Ver. 2.0. Basic Books. N.Y., 2006. P. 61.

Таким образом, историю становления сети Интернет можно разделить на два периода. Первый период (начало 60-х гг. XX в. - 1994 г.) характеризуется некоммерческой направленностью и прямым управлением Сети государственными структурами США,

обусловленными восприятием данной технологии через призму соображений национальной безопасности и общественных интересов. Второй период (1994 г. - н.в.) характеризуется активной "коммерциализацией" сети Интернет новыми видами технологических компаний (**Amazon, Netscape, eBay, Yahoo** и др.) <1>. Интернет, пройдя путь от запрета коммерции во всех проявлениях до коммерциализации практически всего, включая частную жизнь пользователей, вызвал одно из крупнейших "накоплений богатства" в истории человечества.

<1> В американской литературе приводится достаточно любопытная параллель: "подобно тому как окончание холодной войны привело к схватке российских финансовых олигархов за покупку государственных активов, так и приватизация Интернета в конце холодной войны вызвала среди новых технологических олигархов в Соединенных Штатах гонку за приобретением первичного онлайн-пространства". См.: Кин Э. Указ. соч. С. 42.

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

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 <1>. Данные в Интернете циркулируют благодаря "сотням тысяч коммутируемых компьютеров и телефонных сетей" <2>.

<1> American Civil Liberties Union v. Janet Reno, Attorney General of the United States (ACLU v. Reno) (1996): Yee Fen Lim. Op. cit. P. 4.

<2> Post D. Anarchy, State and the Internet: An Essay on Law-making in Cyberspace. 1995. P. 2.

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 "езде" и "нигде конкретно", в связи с чем бывает невозможно привязать их к конкретному географическому месту. 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: определение юрисдикции, защита персональных данных пользователей, защита прав потребителей в сети Интернет, защита интеллектуальной собственности. Более подробно они 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, а также локализации информационных процессов территорией отдельно взятой страны.

<1> Johnson D., Post D. Law and Borders - The Rise of Law in Cyberspace // Stanford Law Review. 1996. N 48. P. 1370.

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 <1>. 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.

<1> Reed C. Internet Law: Cases and Materials. Cambridge University Press. 2004. P. 2.

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 повреждены 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. "Загнать" процессы обработки и передачи персональных данных в рамки территории отдельно взятого государства практически невозможно при одновременном сохранении преимуществ, предоставляемых сетью Интернет.

<1> United States v. Kammersell (1999): Kerr O.S. The problem of perspective in Internet law (доступно на сайте www.heinonline.org, последнее посещение - 15 декабря 2006 г.).

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 <1>. Поэтому традиционное придание отечественными правоприменительными органами некой особой силы оригиналам документов утрачивает какой-либо смысл применительно к договорам, заключенным в сети Интернет.

<1> Reed C. Internet Law: Cases and Materials. P. 15.

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 данной Сети такое устройство, но не позволяет произвести однозначную идентификацию лица, которое его использует. Максимум, что можно установить, это факт передачи информации с определенного устройства определенным интернет-провайдером либо получения 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). При этом в ходе передачи информация может быть перехвачена и изменена, равно как могут быть изменены сведения об источнике такой информации посредством использования прокси-серверов.

<1> Volker Haug. Grundwissen Internetrecht. Stuttgart, 2005. S. 8.

<2> Якушев М.А. Интернет и право // Законодательство. 1997. N 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.

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 оборота 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.

Зависимость отношений между участниками сети Интернет от интернет-провайдеров (4) является еще одной фундаментальной чертой "архитектуры" сети Интернет. Интернет-провайдеры предоставляют доступ к Интернету (**Access-providers**), обеспечивают возможность размещения в Сети информации и обмена ею (**Hosting-providers**). Как следствие, они располагают данными, позволяющими идентифицировать пользователей Интернета, а также техническими возможностями по влиянию на происходящие информационные процессы <1>. Тот, кто владеет проводами и радиоволнами, может, по сути, управлять

Интернетом, потому что последний существует и работает только благодаря линиям связи. Недаром интернет-провайдеров нередко именуют "хранителями врат" Интернета (**Internet "gatekeepers"**), в связи с чем они становятся основными проводниками политики государства в отношении Интернета. Именно через них в большинстве случаев находят свое практическое воплощение нормы об ограничении доступа или распространения информации, которую государство считает нужным заблокировать. Таким образом, информационные посредники являются своего рода "инструментом суверенизации" Интернета. Кроме публично-правовой сферы информационные посредники защищают права участников оборота в частноправовой сфере: обладая необходимыми техническими ресурсами, они могут пресекать правонарушения в сети Интернет (нарушение исключительного права, распространение диффамационной информации и пр.), обеспечивая тем самым куда более эффективную защиту нарушенного права, нежели традиционные средства защиты, применяемые непосредственно против нарушителей.

<1> Savin A. EU Internet Law. Edward Elgar: Cheltenham. 2013. P. 104.

Наконец, необходимо отметить, что протоколы сети Интернет "заточены" на максимальную открытость любому передаваемому контенту и способны работать практически с любым оборудованием. Эта его особенность - **нейтральность по отношению к передаваемому контенту или "сетевой нейтралитет"** (5) - стала благословением для одних компаний (типа **Google, Amazon, Netflix**) и проклятием для других,

основанных на моделях передачи информации прошлого века (при помощи традиционных операторов связи, звукозаписывающих компаний, печатных СМИ и пр.). Поскольку одним из эффективных средств защиты от подрывной силы инноваций <1> является введение чрезмерного регулирования, не вызывающего удивления попытки компаний, сдающих позиции перед силой новой технологии, защитить свои интересы посредством привлечения на свою сторону государства. Это во многом объясняет те процессы, которые происходят в сфере законодательства, регулирующего Интернет, например, появление различного рода антипиратских законов, попытки введения лицензирования провайдеров **VoIP** <2> в качестве операторов связи и пр.

<1> Как известно, все инновации можно разделить на две группы: "поддерживающие" (**sustaining**) и "подрывные" (**disruptive**). Это различие лучше всего описано исследователем инноваций Клейтоном Кристенсеном. "Поддерживающими" инновациями называются улучшения, которые совершенствуют товар, но не угрожают рынку. "Подрывные" инновации, напротив, предвещают полное вытеснение продукта, создавая новые рынки. Christensen C. The Innovator's Dilemma: When New Technologies Cause Great Firms to Fail. Boston, Massachusetts, USA: Harvard Business School Press. 1997. Интернет является ярким примером "подрывной" инновации или "созидательного разрушения", по Йозефу Шумпетеру.

<2> **VoIP** - построенная на базе протокола IP технология передачи речи по сетям с пакетной коммутацией. Используется для экономии средств при

междугородных и международных звонках. Технология допускает интеграцию речи и данных. Одним из известных примеров приложений, использующих данную технологию, является Skype.

Итак, "архитектура" сети Интернет отличается следующими особенностями: **отсутствие географических границ; особая децентрализованная процедура доставки сообщений; сложность идентификации пользователей; зависимость происходящих в Интернете процессов и отношений от интернет-провайдеров, нейтральность по отношению к передаваемому контенту.** Указанные особенности всегда следует учитывать при рассмотрении той или иной проблемы, связанной с регулированием отношений в сети Интернет, воздерживаясь от попыток механического распространения на них решений, выработанных для "офлайнового мира".

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>.

<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. N 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".

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 <1>. Иногда под юрисдикцией понимают право, применимое к определенному отношению (**governing law**) <2>. Весьма часто юрисдикция определяется как компетенция судов конкретного государства по рассмотрению и вынесению решений по данному спору <3>.

<1> См., например: Scassa T., Currie R. New First Principles? Assessing the Internet's Challenges to Jurisdiction // Georgetown Journal of International Law. N 42. 2011. P. 1023.

http://papers.ssrn.com/sol3/papers.cfm?abstract_id=211636
4.

<2> Yee Fen Lim. Op. cit. P. 18.

<3> Collier J.G. Conflict of Laws. 3rd ed. Cambridge University Press, 2001. P. 71.

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

<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.

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 <1>.

<1> Данная классификация отражена в положениях Третьего свода норм США о праве международных отношений (Restatement 3rd. of the Foreign Relations Law 1987 г. (§ 401 ff). Она также нашла свое отражение в некоторых правительственных документах Европейского союза. См., например: Recommendation N 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.

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 <1>.

<1> См.: Молодцов С.В. Некоторые вопросы территории в международном праве // Советское государство и право. 1954. N 8. С. 63.

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

<1> Black's Law Dictionary 9th ed. 2011. Thomson West. P. 927.

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. Как отмечалось ранее, одной из фундаментальных архитектурных особенностей Интернета 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.

<1> См.: Бабкин С.А. Интеллектуальная собственность в сети Интернет. С. 222.

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 определенной 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.

<1> См., например: Dodge W.S. Extraterritoriality and Conflict-of-Laws Theory: an Argument for Judicial Unilateralism // Harvard International Law Journal. 1998. N 39. 101.

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 данной Сети.

Приведу несколько резонансных дел, которые наглядно иллюстрируют обозначенные проблемы.

1. **Dow Jones & Co. Inc. v. Gutnik** <1>. Данное дело дошло до Верховного суда Австралии и представляет собой ставший 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, при том что на территории Австралии было распространено только пять бумажных экземпляров издания. Интернет-версия насчитывала порядка 550000 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 "езде", 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, возлагаемому 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.

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

2. Дело **Yahoo! Inc. v. LICRA** <1> 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 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!"** подала заявление 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. **LICRA** сделала заявление об отсутствии у американского суда юрисдикции в отношении ее. Калифорнийский 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".

<1> Yahoo! Inc. v. La Ligue Contre Le Racisme et L'Antisemitisme 145 F. Supp. 2d 1168 (N.D. Cal. 2001).

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**). Кроме того, как покажет дальнейший анализ, данные виды юрисдикции являются взаимосвязанными и в ином плане. Возможность признания и принудительного исполнения судебного решения на территории иностранного государства (принудительная юрисдикция) напрямую зависит от наличия у принявшего соответствующее решение органа судебной юрисдикции, а у государства, к которому относится такой суд, - права регулировать соответствующие отношения с участием ответчика (предписывающей юрисдикции).

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>.

<1> Graham Smith. Internet Law and Regulation. London: Sweet & Maxwell, 2007. P. 665.

В США общий алгоритм рассмотрения вопросов, связанных с юрисдикцией суда по рассмотрению определенного спора, является следующим <1>.

<1> 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>.

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 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

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 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 тыс. 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>.

<1> Black's Law Dictionary. 9th ed. 2011. Thomson Reuters. P. 929.

<2> Ibid. P. 931.

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 <1>. 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 <2>.

<1> Jack H. Friedenthal et al. Civil Procedure. 2nd ed. 1993. § 2.1; Charles Wright. The Law of Federal Courts. 5th ed. 1994. § 42.

<2> 28 U.S.C. § 1391(d). Brunette Mach. Works, Ltd v. Kockum Indus., Inc., 406 U.S. 706, 714 (1972).

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 территории, 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.

<1> Black's Law Dictionary. 9th ed. 2011. Thomson West. P. 1519.

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: а) **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; б) положение о полном доверии и уважении (**The Full Faith and Credit Clause**, **разд. 1 ст. IV**), предусматривающее проявление всеми штатами США доверия и уважения к официальным актам и судебным документам любого другого штата; в) принцип верховенства Конституции (**The Supremacy Clause**, **ст. VI**); г) принцип недискриминации (**The Privileges and Immunities Clause**, **разд. 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 законодательства, 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 (к) 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 его <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**. Примером служит законодательство штата Нью-Йорк <4>.

<1> Black's Law Dictionary. 9th ed. 2011. Thomson West. P. 1027.

<2>

http://en.wikisource.org/wiki/United_States_Code/Title_28/Appendix/FederalRules_of_Civil_Procedure/Rule_4.

<3> Детальный анализ 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. 1997. N 23.

<4> См., например: New York Civil Practice Law. § 302.

3. **Единообразный торговый кодекс (ЕТК).**
Первый его официальный текст был принят в 1952 г.,

второй (ныне действующий) - в 1990 г. ЕТК 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 ЕТК, кроме штата Луизиана, находящегося в силу исторических причин под сильным влиянием континентально-правовых традиций (преимущественно французского права), где была принята усеченная редакция ЕТК, не включающая гл. 2 о купле-продаже.

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

<1> См.: Ward Classen. A Practical Guide to Software Licensing for Licensees and Licensors. ABA Publishing, 2008. P. 212.

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

1. Третий Свод норм США о праве международных отношений 1987 г. (**Restatement 3d of Foreign Relations Law**). Указанный документ, равно как и иные подобные своды норм, 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 выражению известного американского судьи Бенджамина Кардозо, "свод нормы проникнуты особым авторитетом, позволяющим не повелевать, но убеждать" <1>. Данный Свод норм представляет собой квинтэссенцию положений международного права, применимого к США, положений федерального законодательства США, отдельных штатов, а также судебной практики, имеющей довольно сильное влияние на внешнюю политику США или иные существенные международные последствия (§ 1 указанного Свода). В контексте рассматриваемой проблематики основной интерес представляет часть 4 указанного Свода, посвященная вопросам регулирования различных видов юрисдикции, иммунитетов и международного сотрудничества в указанной сфере.

<2> Cardozo B. The Growth of the Law. Yale University Press, 1924. P. 9.

2. Свод норм коллизионного права (Restatement of Conflict of Laws). 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) <1>. 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)). Произшедшие изменения в американской доктрине коллизионного права, заклеившей 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 <2>. 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.

<1> Freiheit J. Proskauer on International Litigation and Arbitration: Ch. 7 Choice of Law Issues. Selecting the Appropriate Law // www.proskauerguide.com/litigation/7/IV.

<2> Symeonides S. Choice of Law in the American Courts in 2006: Twentieth Annual Survey // American Journal of Comparative Law. 2006. N 54. P. 697, 712.

3. **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 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>.

<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.

4. **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 <1>. 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).

<1> ALI Principles of the Law of Software Contracts.
Proposed Final Draft, 2009. P. 2.

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: 1) проживание или учреждение ответчика на территории штата, где расположен суд; 2) согласие ответчика с юрисдикцией, выраженное в договоре либо посредством участия в инициированном процессе (кроме целей оспаривания юрисдикции); 3) нахождение имущества ответчика на территории штата при наличии связи такого имущества с предъявленным требованием; 4) осуществление регулярной деятельности на территории такого штата; 5) совершение действия на

территории такого штата, послужившее основанием для предъявления требования; 6) действие было совершено за пределами штата, но имело существенный, непосредственный и предвидимый эффект на территории штата <1>.

<1> См. детальный перечень в § 423 Restatement 3d of Foreign Relations Law, § 27 Restatement Second on Conflict of Laws.

В случае, если ответчиком выступает иностранное лицо, суд, в который предъявлен соответствующий иск, должен рассмотреть вопрос о том, насколько установление юрисдикции в отношении такого лица является допустимым с точки зрения положений **long-arm 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>.

<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.

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 его юрисдикции судом такого штата <1>. 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.

<1> 95 U.S. 714 (1877).

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" <1>. 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.

<1> 326 U.S. 310 (1945).

Анализ существующих контактов ответчика с территорией штата будет различным в зависимости от того, какой тип персональной юрисдикции 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>.

<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. 1966. N 79.

<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).

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 <1>. Указанное дополнительное требование направлено на защиту интересов ответчика, минимизируя неопределенность, которую могут вызвать его случайные, произвольные 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**

<2>, в котором молодая пара, проживающая в Нью-Йорке, приобрела автомобиль в данном штате и попала в аварию, проезжая по территории штата Оклахома в направлении 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.

<1> Данное правило впервые сформулировано Верховным судом США в деле *Hanson v. Denckla*, 357 U.S. 235, 252 (1958).

<2> 444 U.S. 286 (1980).

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>.

<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. 2006. N 52. P. 155.

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 <1>.

<1> Mass. Sch. of Law at Andover, Inc. v. Am. Bar. Ass'n, 107 F. 3d, 1026, 1042 (3d Cir. 1997).

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 <1>. 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" <2>. Решая вопрос о

возможности отказа в рассмотрении спора со ссылкой на **forum non conveniens**, суды обычно последовательно используют следующие критерии (**three-part test**):

<1> § 84 Restatement Second on Conflict of Laws; Barett Edward. Doctrine of Forum Non Conveniens // California Law Review N 35. 1947.

<2> Gulf Oil Corp. v. Gilbert, 330 U.S. 501, 506-07 (1947).

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 **временных** 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>;

<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).

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 <1>. Однако политическая нестабильность может выступать в качестве фактора для признания альтернативного места рассмотрения спора неадекватным <2>. 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** <3>;

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

<2> 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).

<3> Blanco v. BancolIndus. de Venezuela, S.A., 997 F. 2d 974 (2nd Cir. 1993).

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 <1>. 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> 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.

<1> См., например: Johnson D., Post D. Op. cit.

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 Интернете, 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 Интернета, игнорирующих эти положения, не могла не вызвать попыток "подчинить" ее соответствующим локальным законодательным положениям.

Один из первых подходов, достаточно быстро отвергнутых последующей практикой <1>, был отражен в решении по делу **Inset Systems, Inc. v. Instruction Set, Inc** <2>. 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 его. 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 с этим рисков и обременений, к числу которых относится возможность предъявления иска к компании за пределами ее родного штата.

<1> В литературе его даже именуют аномалией в мире киберюрисдикции. См.: Yvonne Beshany, Sean Shirley. Cyber-Jurisdiction: When Does Use of the Internet

<2> 937 F. Supp. 161 (D. Conn. 1996).

Данному подходу нельзя отказать в определенной логике <1>. 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 Интернете. 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 доинтернетную 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.

<1> Данный подход был реализован и в иных судебных решениях того периода. См., например: *Maritz, Inc. v. Cybergold*, 947 F. Supp. 1328, 1330-33 (E.D. Mo. 1996). В данном деле расположенная в Калифорнии компания, предоставлявшая услуги рекламы по

электронной почте, была признана подпадающей под юрисдикцию суда в Миссури, поскольку ее веб-сайт был доступен на территории указанного штата и на него было осуществлено порядка 300 запросов с его территории.

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 штата <2>. 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.

<1> 952 F. Supp. 1119 (W.D. Pa. 1997).

<2> 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.

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 семь контрактов с интернет-провайдерами на территории штата Пенсильвания. Как следствие, суд отверг аргумент ответчика о случайном характере его контактов с территорией данного штата <1>. Если бы ответчик хотел избежать юрисдикции 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.

<1> Суд не поленился при этом привести пример случайного контакта, транслированного на матерью сети Интернет: ситуация, когда житель штата Калифорния взял с собой в путешествие компьютер и использовал его на территории штата Пенсильвания для получения доступа к сервисам ответчика.

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>.

<1> Toys "R" Us, Inc. v. Step Two, S.A., 318 F.3d 446, 452 (3d Cir. 2003).

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

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 <1>. 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.

<1> См., например: Kevin McMunigal. Desert, Utility and Minimum Contracts: Toward a Mixed Theory of Personal Jurisdiction // Yale Law Journal. N 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. 2003. N 74. 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 очевидный 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>.

<1> Yokoyama D. You Can't Always Use the Zippo Code: The Fallacy of a Uniform Theory of Internet Personal Jurisdiction // DePaul Law Review. 2004 - 2005. N 54. P.

<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*. 2004. Vol. 98. N 2.

<3> *Edelson v. Ch'ien* 352 F. Supp. 2d 861 (N.D. Ill. 2005).

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 установлении общей юрисдикции <1>. Как отмечалось ранее, для этого необходимо, чтобы контакты носили продолжительный, систематический и существенный характер, что отнюдь не эквивалентно 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 <2>. 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** <3>.

<1> 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).

<2> Mink v. AAAA Dev. LLC, 190 F.3d 333 (5th Cir. 1999); MJC-A World of Quality, Inc. v. Wishpets Cp., Ltd, N 00 C 6803 (N.D. Ill. Aug. 27, 2001).

<3> Yokoyama D. Op. cit. P. 1194.

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 <1>. Как указал один из судов, "персональная юрисдикция не может быть установлена, если только ответчик не совершает чего-то большего, что бы свидетельствовало о направленности его действий по отношению к клиентам в штате Западная Вирджиния" <2>. Аналогичные подходы встречаются во многих других решениях <3>.

<1> См. обзор подходов по федеральным окружным судам США: Trammel A., Bambauer D. Personal Jurisdiction and the "Interwebs" // Cornell Law Review. Vol. 100. 2015. P. 1150.

<2> Williams v. Advertising Sex (N.D. W.Va. 2007).

<3> 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).

Лучше всего суть нового подхода демонстрирует дело **Toys "R" Us, Inc. v. Step Two, S.A.** <1>. 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 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.

<1> 318 F.3d 446, 451 (3d Cir. 2003).

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>.

<1> Viz Commc'ns, Inc. v. Redsun N 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).

При определении направленности веб-сайта на территорию определенного штата суд может принимать во внимание следующие факторы: 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>.

<1> Rustad M. Internet Law in a Nutshell. St. Paul:

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 <1>. 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, независимо 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. <2>.

<1> Intellectual Property: Principles Governing Jurisdiction, Choice of Law, and Judgments in Transnational Disputes. ALI, 2007. P. 93.

<2> 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: а) 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; б) национальность истца и ответчика; в) осуществление ответчиком определенной деятельности на территории государства суда, не связанной с предъявленным требованием; г) вручение повестки на такой территории; д) 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.

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

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 <1>. Для этого необходимы еще и соответствующие технические решения (использование специальных технологий, позволяющих блокировать запросы от пользователей с определенных территорий; отсутствие возможности совершения платежей резидентами таких штатов; отсутствие доставки товара в указанный штат) <2> либо инкорпорированная в онлайн-договор юрисдикционная оговорка <3>.

<1> Euromarket Designs Inc. v. Crate & Barrel Ltd.,
96 F. Supp. 2d 824 (N.D. Ill. May 16. 2000).

<2> Toys "R" Us, Inc. v. Step Two, S.A. 318 F.3d
446, 451 (3d Cir. 2003).

<3> Graham Smith. Op. cit. P. 682.

В завершение необходимо указать на наличие в американском процессуальном праве так называемого правила агрегации (**rule of aggregation**). Согласно правилу **4k** 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** <1> 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 **4k** 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.

<1> (N.D. Cal. 1999).

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**) <1>. Разумеется, в данной работе не представляется возможным осветить подходы в выборе 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) <2>.

<1> Klaxon Co. v. Stentor Elec. Mfg. Co., 313 U.S. 487, 496 (1941).

<2> Smith Gregory. Choice of Law in the United States // The Hastings Law Journal. 1987. N 38. 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 **большую** 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>.

<1> Асосков А.В. **Коллизионное регулирование договорных обязательств**. М., 2012. С. 396.

Гораздо **большой** 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: а) потребности межгосударственных и межштатовых взаимоотношений; b) соображения правовой политики штата по месту рассмотрения спора; с) 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.

Таких ограничений два. Во-первых, выбранное право должно быть связано либо 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.

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

<2> § 187 (2) Restatement (Second) on Conflict of Laws.

Если выбранное сторонами право не будет соответствовать указанным ограничениям, то оно может быть проигнорировано <1> 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.

<1> Правда, оно все же может иметь некоторое значение для толкования договора как выражающее волю сторон.

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 отношениями и выбранным правом порядком (§ 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>.

<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.

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 <1>. 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 договором правовым порядкам <2>.

<1> Scoles E., Hay P., Borchers P. Symeonides S. Conflict of Laws. 4th ed. St. Paul. MN. 2004. P. 975.

<2> Ibid. P. 976.

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 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 ЕТК была предпринята попытка внесения изменений в том числе и в данную статью. В соответствии с положениями § 1-301 ЕТК, призванного заменить § 1-105 ЕТК, 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.

<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\(2001\)](http://www.uniformlaws.org/ActSummary.aspx?title=UCC%20Article%201,%20General%20Provisions%20(2001)).

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

<1> 2006 Uniform Commercial Code Survey: Introduction // The Business Lawyer. August 2007. N 62. P. 1555 - 1558. Единственной территорией, имплементировавшей новую редакцию § 1-301 ЕТК, были Американские Виргинские острова.

Таким образом, необходимость наличия разумной связи между выбранным правом и правоотношением продолжает составлять одну из наиболее принципиальных особенностей американского коллизионного права <1>, 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 <2>.

<1> Специалисты в области международного частного права отмечают, что схожее правило содержится лишь в коллизионном праве Польши, Макао (административной единицы Китая с особой правовой системой), Анголы и Мозамбика. См.: Асосков А.В. [Указ. соч.](#) С. 264.

<2> Rühl G. Party Autonomy in the Private International Law of Contracts: Transatlantic Convergence and Economic Efficiency // Conflict of Laws in a Globalized World / Ed. by E. Gottschalk, R. Michaels, G. Rühl, & J. von Hein. Cambridge University Press. 2007. P. 163.

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. Однако такая свобода допускается лишь в договорах, сумма которых превышает 250000 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. 1997. N 15. 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.

<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. 2009. N 24. P. 256 - 261.

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 о принадлежности исключительного права 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 определению последствий нарушения авторского права и доступных средств защиты, то суд использовал коллизионную привязку из сферы деликтного права - **lex**

loci delicti и применил Закон 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" <1>. Отсутствие детальной проработки проблематики выбора права в трансграничных спорах в сфере интеллектуальной собственности во многом обусловлено тем фактом, что американские суды не любят рассматривать требования, связанные с нарушением исключительных прав за рубежом, если это сопряжено с применением иностранного права <2>.

<1> **ITAR-TASS Russian News Agency v. Russian Kurier, Inc.**, 153 F.3d 82, 88 (2d Cir. 1998).

<2> 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**. 2001. N 49. P. 440.

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 имела место и в таком штате. Как видно из данных презумпций, в качестве применимого права в таких случаях выступает право штата, где, как предполагается, репутация 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 (домицию) истца <1>. Таким образом, если американский суд найдет основания для установления юрисдикции в отношении ответчика - 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.

<1> 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).

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, § 481 Restatement 3d of Foreign Relations Law**).

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 имеют 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. 1979. N 18.

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>.

<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. N 415 (1993).

<2> Berner M. Recognition and enforcement in Switzerland of US judgments containing an award of punitive damages // International Business Lawyer. 1994. N 22. P. 272.

Условия и пределы допустимости признания и принудительного исполнения иностранных судебных решений на территории США определяются в соответствии с законодательством соответствующего штата. Федеральные суды по общему правилу также применяют положения законодательства того штата, где они расположены <1>. Решение суда по вопросам признания и принудительного исполнения иностранного судебного решения не может быть оспорено в Верховном Суде США, за исключением случаев, когда такое решение имеет конституционно-правовой аспект (например, затрагивает вопросы обеспечения надлежащей правовой процедуры либо представляет собой вмешательство в вопросы внешней политики США).

<1> Erie Railroad Co. v. Tompkins, 304 U.S. 64 (1938); Restatement 3rd Foreign Relations law. § 481a (1987).

Условия исполнения иностранных судебных решений обозначены в § 98 **Restatement 2nd on Conflict of Laws** и § 481 - 382 **Restatement 3d of Foreign Relations Law**. В них предусматривается общее правило о допустимости признания и принудительного исполнения действительных решений иностранных судов, вынесенных в пределах их компетенции в рамках справедливого состязательного процесса. Наличие соответствующего международного договора США с государством, на территории которого вынесено решение, не является обязательным условием признания и принудительного исполнения такого решения на территории США.

Данные положения нашли свое отражение в известном прецеденте **Hilton v. Guyot** <1>, в котором стоял вопрос о признании и исполнении на территории США решения 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 <2> 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 <3>. 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" <4>.

<1> 150 U.S. 113, 202 (1895).

<2> При этом американский суд может проанализировать обоснованность установления юрисдикции над ответчиком в соответствии с доктриной "минимальных контактов". См.: *Koster v. Autmark Industries, Inc.*, 640 F.2d 77 (7th Cir. 1981).

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

<4> *Loucks v. Std. Oil Co.* 120 N.E. 198, 201 (N.Y. Ct. App. 1918).

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 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>.

<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. См. также: Reporters notes N 1 to § 481 Restatement 3d of Foreign Relations Law.

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 <1>. 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 юрисдикции 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. <2>.

<1> 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.

<2> 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.

Что же касается признания и принудительного исполнения в США решений российских судов, то такие случаи встречаются, но их немного и они не связаны с электронной коммерцией. В основном они касаются вопросов семейного права <1>.

<1> Bliss v. Bliss, 733 A. 2d 954 (D.C. App. 1999); Asanov v. Hunt, 914 So. 2d 769 (Ct. App. Miss. 2005).

Суды США по общему правилу вправе не признавать иностранные судебные решения, касающиеся взыскания налогов или штрафов, имеющих не компенсационную, а карательную направленность (**§ 483 Restatement 3d of Foreign Law Relations**). Данное положение основано на устоявшемся правиле коллизионного права США, согласно которому суд одного государства не обязан признавать и

принудительно исполнять судебное решение, вынесенное на основании норм налогового или публичного законодательства другого государства (§ 89 **Restatement Second on Conflict of Laws**).

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 закреплённой в I поправке к Конституции США свободе слова <1>. В связи с этим в США в 2010 г. был принят отдельный Закон о защите конституционного наследия США <2>, 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 <3>. Ранее подобные законы были приняты в отдельных штатах США (Нью-Йорк, Калифорния, Флорида, Иллинойс и некоторых других).

<1> Yahoo! Inc. v. La Ligue Contre Le Racisme et L'Antisemitisme 145 F. Supp. 2d 1168 (N.D. Cal. 2001).

<2> Securing the Protection of our Enduring and Established Constitutional Heritage (SPEECH) Act, 2010. Pub. L. 111 - 223.

<3> 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.

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 Интернете контент <1>. 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 <2>.

<1> *InvestorsHub.com v. Mina Mar Group* (N.D. Fla. 2011).

<2> См. подробнее § 4 гл. 5 настоящей книги.

Наконец, необходимо отметить, что **jurisdiction to enforce** не ограничивается исключительно вопросами принудительного признания и принудительного исполнения решения суда. В некоторых случаях решения государственных органов США могут

обеспечиваться неюрисдикционными мерами. В частности, отказом иностранному лицу в совершении экспортных или импортных операций с американскими лицами или технологиями; запретом на участие в процедурах государственных закупок; запретом на отчуждение или перевод активов и т.д. <1>. Данные способы обеспечения актов государственных органов США принудительной силой особенно актуальны в случаях с обеспечением соблюдения экономических санкций. Так, в зависимости от содержания положений соответствующей санкционной программы в отношении иностранного лица могут быть приняты следующие меры: запрет на доступ к банковской системе США (заккрытие корреспондентского счета в банке США, блокирование активов такого лица, в случае их прохождения через американский банк); введение визовых ограничений в отношении акционеров или сотрудников такой иностранной организации <2>.

<1> Comment "c" to § 431 Restatement 3d of Foreign Relations Law.

<2> См. подробнее: Савельев А.И. Односторонние экономические санкции США: взгляд со стороны американского и российского права // Закон. 2015. N 5.

В качестве некоторого обобщения характеристик 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 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>;

<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. N 26. P. 96.

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. Гагской **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 достижения результата, предписанного директивой. Директива ЕС служит инструментом гармонизации национального права государств-членов (т.е. сближения способов и методов правового регулирования, направленных на создание схожих, но не обязательно единообразных норм).

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>.

<1> См. подробнее: Кашкин С.Ю., Четвериков А.О. **Европейский союз**: основополагающие акты в редакции Лиссабонского договора с комментариями // СПС "КонсультантПлюс". 2007.

3.1. Основные источники регулирования вопросов юрисдикции в Европейском союзе

1. **Регламент ЕС от 22 декабря 2000 г. N 44/2001** "О юрисдикции, признании и исполнении судебных решений по гражданским и торговым делам" (Брюссель I) <1>. 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.

<1> Council Regulation (EC). N 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.

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** <1>. Основные изменения заключаются в упразднении экзекватуры (промежуточного судебного решения о признании и принудительном исполнении иностранного судебного решения), за исключением некоторых категорий споров (в частности, диффамации); расширении сферы действия **Регламента** в отношении иностранных лиц, не domiciliрованных в ЕС; гармонизации положений, регламентирующих соглашения о подсудности с положениями Гаагской **конвенции** в отношении соглашений о выборе суда 2005 г. <2>. Новая версия **Регламента** Брюссель I (EC N 1215/2012) применяется с 10 января 2015 г. При дальнейшем упоминании в тексте настоящей работы **Регламента** Брюссель I, его положения и нумерация соответствующих статей будут приводиться в соответствии с новой редакцией.

<1> Council Regulation (EC) N 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. L351/1. 20.12.2012.

<2> 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. **Луганская конвенция 2007 г.** <1>. 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 <2>. 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 **N 44/2001** и **1215/2012**. Луганская конвенция открыта для присоединения других государств при условии наличия единогласного согласия всех ее участников.

<1> Council Decision 2007/712/EC of 15 October 2007 // Official Journal of the European Communities. L 339. 21.12.2007.

<2> См.: Section 6 Preamble to Council Regulation (EC). N 1215/2012 of 12 December 2012.

3. **Регламент ЕС N 593/2008 от 17 июня 2008** "О праве, применимом к договорным отношениям" (Рим I) <1>. Данный документ пришел на смену подписанной 19 июня 1980 г. Римской **конвенции** 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> Regulation EC N 593/2008 of 17 June 2008 "On the Law Applicable to Contractual Obligations" (Rome I) // Official Journal of the European Communities. L177/6. 04.07.2008.

4. **Регламент ЕС N 864/2007 от 11 июля 2007 г.** "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.

<1> Regulation EC N 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). N 4. P. 414 - 424, 2008 // <http://ssrn.com/abstract=1314749>.

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 domicilia ответчика. Домициль истца не имеет значения, равно как не имеет значения национальность ответчика.

Домициль (домицилий) ответчика - физического лица определяется судом, в который предъявлено соответствующее требование, в соответствии с его национальным законодательством ([ст. 62\(1\)](#) Регламента Брюссель I), а domicili ответчика - юридического лица определяется самим Регламентом: местом учреждения компании, местом нахождения ее центральных органов либо местом нахождения основного коммерческого

предприятия (ст. 63 Регламента Брюссель I). Таким образом, у юридического лица может быть несколько доomicилей, каждый из которых в равной степени может выступать 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, доomicилированное 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 в случаях, когда ответчик доomicилирован во Франции и отсутствуют иные основания, указанные в Регламенте, для предъявления к нему иска в Англии <1>. Если же ответчик не имеет доomicилия в государстве - члене ЕС (например, российская компания), то для определения допустимости установления юрисдикции в отношении его применяется национальное процессуальное законодательство.

<1> Goode R. Commercial Law. 3rd ed. London. 2004. P. 1079.

Суд по месту доomicилия ответчика обладает **общей юрисдикцией** в отношении его 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 domicilia 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. 7 (1)(a) Регламента Брюссель I). В договорах купли-продажи таким местом обычно считается место, куда товары были доставлены или должны были быть доставлены; в договорах оказания услуг - место, где услуга была оказана или должна была быть оказана (ст. 7 (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 <1>. Однако согласно позиции Европейского суда договор, по которому правообладатель предоставляет другому лицу на возмездной основе право использовать объект

интеллектуальной собственности, не является договором оказания услуг <2>. Кроме того, позиция, согласно которой цифровой контент, предоставляемый не на материальном носителе, не является ни товаром, ни услугой, нашла свое отражение в Директиве ЕС N 2011/83/EU "О правах потребителей" (п. 19 преамбулы) <3>. Соответственно в отношении договоров на предоставление цифрового контента применяется общее правило ст. 7(1)(a) Регламента Брюссель I о возможности предъявления иска в суд по месту исполнения такого договора. Для этого необходимо осуществить квалификацию договорного обязательства, затем определить применимое к такому обязательству право (в соответствии с Регламентом Рим I) и только после этого - место исполнения обязательства в соответствии с применимым правом <4>. В литературе в качестве места исполнения обязательства по предоставлению цифрового контента предлагается считать местонахождение получателя <5>. Однако данный подход может варьироваться в зависимости от применимого права.

<1> 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.

<2> Falco Privatstiftung and Thomas Rabitsch v. Gisela Weller-Lindhorst [2009] ECR, C-533/07.

<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> Gie Groupe Concorde and Others [1999] ECR. C-440/97.

<5> 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. 2008. N 3.

Другим исключением из общего правила об установлении юрисдикции по domicilio ответчика, применимым к договорным отношениям, является заключение соглашения о подсудности (ст. 25 Регламента Брюссель I). Данное соглашение подчиняется нормам Регламента Брюссель I при условии, что оно (1) устанавливает юрисдикцию определенного суда или судов государства - члена ЕС по рассмотрению споров, связанных с конкретным правоотношением, и (2) не является недействительным в соответствии с правом страны такого суда. Таким образом, если стороны указали, что споры должны рассматриваться в судах Нью-Йорка, то данное соглашение не подпадает под действие Регламента Брюссель I. На практике это может означать, что при предъявлении иска в нарушение условия пророгационного соглашения о рассмотрении спора в суде Нью-Йорка во французский суд к ответчику, domiciliрованному во Франции, такой суд не будет иметь возможности со ссылкой на ст. 25 Регламента Брюссель I отказать в принятии спора к рассмотрению <1>. Новая редакция Регламента исключила условие о

необходимости заключения пророгационного соглашения между лицами, как минимум одно из которых является домицилированным в государстве - члене ЕС, тем самым существенно расширив сферу применения Регламента и устранив необходимость проверки домицилей сторон такого соглашения судом.

<1> По крайней мере, такая неопределенность существует. См.: *Owusu v. Jackson*, ECJ, Case C-281/02, 2005.

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. 25(2) специально оговаривает возможность существования такого соглашения и в электронной форме, если она обеспечивает надежную фиксацию достигнутых договоренностей.

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.

Долгое время особенностью европейского законодательства в области юрисдикции являлось 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 не совместимых между собой решений.

Таким образом, если в обход существующего соглашения о подсудности, признаваемого в соответствии с Регламентом Брюссель I, иск был сначала подан в иной суд и такой суд не откажет в установлении юрисдикции, то суд, указанный в соглашении, не будет иметь 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 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 Брюссель I являлась 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).

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

<2> Savin A. Op. cit. P. 61.

Свобода усмотрения при определении компетентного суда в соглашениях о выборе подсудности значительно ограничена применительно к договорам, заключенным с потребителями, т.е. лицами, действующими за пределами своей профессии или предпринимательской деятельности <1>. Безотносительно к содержанию такого соглашения потребитель всегда имеет возможность выбора: предъявить иск в суд по своему местонахождению (домицию) или по местонахождению (домицию) предпринимателя. Предприниматель такого выбора лишен и имеет возможность предъявления иска к потребителю только по его местонахождению (ст. 18 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.

<1> В соответствии с устоявшейся практикой

Европейского суда в качестве потребителя может выступать только физическое лицо. *Bertrand v. Ott* [1978] ECR C-150/7.

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. 18 Регламента Брюссель I). Таким образом, в Европейском союзе соглашения о подсудности, 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>.

<1> Savin A. Op. cit. P. 62.

Важно отметить, что под действие данных положений Регламента подпадают не все потребительские договоры, а лишь договоры, заключенные в процессе осуществления направленной (**directed [...] to**) предпринимательской или иной профессиональной деятельности на территории государства, где домицилирован потребитель, при условии, что соответствующий договор связан с такой деятельностью (ст. 17(1)(c) Регламента Брюссель I).

Говорить о наличии направленной деятельности можно в тех случаях, когда потребителю по электронной почте приходит реклама или иная информация от предпринимателя, которая имеет своей целью побудить потребителя заключить договор <1>. Однако наибольший интерес толкование критерия направленности имеет применительно к деятельности, осуществляемой посредством веб-сайтов, где их владелец не выступает инициатором коммуникаций с потребителем.

<1> Foss M., Bygrave L. International Consumer Purchases through the Internet: Jurisdictional Issues pursuant to European Law // International Journal of Law and Information Technology. 2000. N 8. P. 14.

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" <1>. Таким образом, в отсутствие заключенного на основе такой информации контракта или коммуникаций между потребителем и предпринимателем, осуществленных посредством веб-сайта, говорить о наличии направленной деятельности предпринимателя на территории государства, где потребители имеют доступ к его сайту, по общему правилу нельзя <2>.

<1> European Commission, Justice and Home Affairs DG, "Statement on Articles 15 and 73" // http://www.europa.eu.int/comm-/justice_home/unit/civil/justici-v-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).

<2> 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.

Возможные критерии направленности деятельности, связанной с использованием веб-сайта, на территорию определенной страны были указаны Европейским судом в решении по делу **Hotel Alpenhoff** <1>:

<1> 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.

- потенциально международный характер деятельности (в данном случае - 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 <1>.

<1> 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 конвенции, 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.

<1> Rosner N. International Jurisdiction in European Union E-Commerce Contracts / Online Contract Formation

ed. by S. Kinsella and A. Simpson. 2004. P. 486.

В завершение необходимо рассмотреть еще один важный вопрос, возникающий в связи с применением критерия направленной деятельности к потребительским договорам. Из положений [ст. 17\(1\)\(с\)](#) Регламента Брюссель I не следует четкого ответа на вопрос, необходима ли причинно-следственная связь между фактом заключения потребителем договора с предпринимателем из другой юрисдикции и его направленной деятельностью на соответствующей территории. Указанное положение говорит лишь о том, что такой договор должен охватываться направленной деятельностью. Например, если немецкий интернет-магазин продает мобильные телефоны и цифровой контент, при этом мобильные телефоны он продает только в Германии, а цифровой контент - на территории всех стран Европейского союза, то потребитель из Франции, заказавший себе мобильный телефон с доставкой во Францию "обходными путями", не будет иметь возможности предъявить иск, связанный с обнаружением недостатков такого телефона, по месту своего жительства (т.е. во Франции), а должен будет предъявить его по местонахождению ответчика (т.е. в Германии). Однако рассмотрим ситуацию, при которой потребитель из Германии приобрел автомобиль у дилера во Франции по рекомендации своего друга. На веб-сайт такого дилера, доступный на территории Германии, он зашел уже после заключения договора. Веб-сайт содержит контактные данные, включающие помимо французского телефона с указанием кода страны также и немецкий телефон. Возникает вопрос: имеет ли такой потребитель право обратиться в немецкий суд на основании [ст. 17\(1\)\(с\)](#) Регламента Брюссель I, принимая во внимание, что заключенный с ответчиком договор никак не был обусловлен

направленной деятельностью предпринимателя? Европейский суд, рассмотрев дело с подобными фактами, пришел к выводу, что предъявление иска в суд по месту нахождения потребителя возможно и при отсутствии причинно-следственной связи между обстоятельствами, обуславливающими направленную деятельность, и заключенным договором, поскольку возложение на потребителя бремени доказывания наличия такой связи или предоставление предпринимателю возможности ее оспаривания снизит уровень защиты потребителей <1>. Таким образом, для применения критерия направленности требуется только выяснение обстоятельств, касающихся предпринимателя, обстоятельства на стороне потребителя иррелевантны для применения защитных юрисдикционных положений Регламента Брюссель I <2>. Во многом данный подход обусловлен теми целями, которые европейский законодатель преследует введением соответствующего положения: это уже не столько защита потребителя как слабой стороны (концепция защиты "пассивного потребителя" от действий предпринимателя по "выманиванию" его из своей юрисдикции), сколько стимулирование потребителей к участию в трансграничной электронной коммерции и развитие тем самым внутреннего рынка ЕС. Последняя цель достигается предоставлением "активному" потребителю гарантий, обеспечивающих его уверенность в достаточном уровне защищенности при совершении покупок за пределами его страны <3>.

<1> Lokman Emrek v. Vlado Sabranovic, ECJ, C-218/1210. 17 October. 2013.

<2> Данный тезис также озвучен в решении Европейского суда Справедливости по делу Munhilleitner

v. Ahmad Yusufi and Wadat Yusufi (ECJ, C-190/11. 7 September. 2012).

<3> См. подробнее: Thiede T., Schacherreiter J. The Recent Shift from the Passive to the Active Consumer // Austrian Law Journal. 2015. N 1. P. 21 - 31.

Общие положения об установлении юрисдикции в сфере деликтных отношений содержатся в [ст. 7 \(2\)](#) 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 <1>. Так, например, в соответствии с устоявшейся практикой Европейского суда Справедливости 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) <2>. В связи с этим представляет интерес дело **eDate Advertising GmbH** <3>, которое было связано с нарушением австрийским сайтом личных прав (права на изображение) немецкого истца. Суд, толкуя [ст. 5 \(3\)](#) Регламента Брюссель I, указал, что в случае нарушения личных прав истца контентом, размещенным в Интернете, истец имеет право предъявить 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 domiciliрованным в одном из государств - участников ЕС (иначе [Регламент](#) не будет применяться), он может выступить 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 domiciliрован ни в одной из стран ЕС, то основания для установления юрисдикции будут определяться национальным законодательством страны, в которой был предъявлен иск.

<1> Bier BV v. Mines de Potasse D'Alsace SA [1978] ECR, C-21/76.

<2> Shevill v. Presse Alliance SA [1995] ECR, C-68/93.

<3> eDate Advertising GmbH v. Martinez. ECR. 25 October. 2011. C-509/09.

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>.

<1> Savin A. Op. cit. P. 60.

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 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. Правда, как и в деле **eDate Advertising GmbH**, Европейский суд указал, что юрисдикция такого суда ограничена лишь ущербом, который был причинен стране, где расположен этот суд <1>.

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

Не следует забывать о возможности

предъявления иска в суд по месту domicilia ответчика - нарушителя исключительного права при условии, если domicilia 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](#) <1> (в части договорных обязательств) и [Регламент Рим II](#) <2> (в части внедоговорных обязательств).

<1> Regulation EC N 593/2008 of 17 June 2008 "On the Law Applicable to Contractual Obligations" (Rome I) // Official Journal of the European Communities. L177/6. 04.07.2008.

<2> Regulation EC N 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.

Право, применимое к договорным обязательствам

[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 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. 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.

<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.

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, 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 свехимперативными 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 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](#).

<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.

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>.

<1> Gillies L. Op. cit. P. 104.

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\(1\)\(с\)](#) 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 законодательством о защите прав потребителей страны своего проживания).

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 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.

Право, применимое к деликтным обязательствам

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. Следует отметить, что применимость данного Регламента не ставится в зависимость от наличия у ответчика domicilia на территории ЕС или от факта причинения вреда на территории ЕС. Имеет значение лишь то, что спор рассматривается судом страны - члена ЕС, обладающим юрисдикцией в отношении такого спора. Кроме того, на применимость положений Регламента ЕС не влияет возможность применения права страны, не являющейся членом ЕС. Как указано в [ст. 3](#) Регламента Рим II, любое право, определенное в соответствии с данным [Регламентом](#), подлежит применению, даже если оно не является правом страны - члена ЕС.

Главным принципом определения права является **lex loci damni**, в соответствии с которым применяется **право страны, где наступил вред**. При этом неважно, 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.

<1> Bogdan M. Torts in Cyberspace. The Impact of the New Regulation Rome II // Masaryk University Journal of Law and Technology. 2005. N 2. P. 5.

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 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 domicilia 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>. К определению

юрисдикции по данной категории споров применяется национальное законодательство страны суда, рассматривающего спор.

<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 Noncontractual Obligations (Rome II) COM (2003). 427 final. 22.07.2003.

Порядок определения права, применимого к нарушению исключительных прав, определяется в соответствии с положениями ст. 8 Регламента Рим II. 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.

В отношении иных объектов интеллектуальной собственности применяется принцип **lex loci protectionis** - применение права страны, для которой истребуется защита. Данный подход по большей части основан на положении ч. 2 ст. 5 Бернской конвенции, согласно которой "объем охраны, равно как и средства защиты, предоставляемые автору для охраны его прав, регулируются исключительно законодательством страны, в которой истребуется охрана". Такой страной

выступает страна, где было совершено нарушение. 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 <1>. В случае если речь идет о нарушении исключительного права посредством распространения объектов авторского права в сети Интернет через веб-сайты, доступные на территории стран ЕС, это фактически означает необходимость одновременного применения национального законодательства 27 стран <2>. Ситуация усугубляется тем, что стороны не могут своим соглашением изменить указанное регулирование, договорившись о применении к спору права какой-либо одной страны (ст. 8 (3) Регламента Рим II). Таким образом, Регламент Рим II весьма "недружелюбен" по отношению к трансграничным спорам, связанным с нарушением авторских прав.

<1> 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.

<2> Engelen Th. Jurisdiction and Applicable Law in Matters of Intellectual Property // Electronic Journal of Comparative Law, Vol. 14.3, 2010. P. 14 ff.

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 domiciliрован ответчик <1>. Таким образом, применимое 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 Интернете, являются доступными во многих странах мира, у потерпевшего появляется неплохая возможность выбора удобного правопорядка.

<1> Kunke C. Rome II and Defamation: Will the Tail Wag the Dog // Emory International Law Review. 2005. N 18. P. 1744.

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 ссылки 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>.

<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. 1996. N 9. P. 489, 512.

Одним из самых обсуждаемых английских дел, связанных с выбором наиболее благоприятной юрисдикции для рассмотрения диффамационных исков, является дело **Berezovsky v. Michaels** <1>. 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 этому спору, поскольку в данном случае была затронута репутация истца, сложившаяся в Англии. В результате в пользу истца были присуждены суммы убытков, а ответчик был

обязан опубликовать опровержение. 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% всего тиража данного журнала.

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

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 Интернете, 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.

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

<2> Ehrenfeld R. Funding Evil: How Terrorism is Financed and How to Stop It. Bonus Books. 2003.

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 2012 г. Европейский парламент выдвинул предложение дополнить [Регламент](#) Рим II положениями, содержащими принципы определения права, применимые к данным видам деликтов <1>. По общему правилу предлагается применять 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 возможных последствий своих действий <2>. 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.

<1> Motion for a European Parliament Resolution. With Recommendations to the Commission on the Amendment of Regulation (EC) N 864/2007 on the Law Applicable to Non-contractual Obligations (Rome II) (2009/2170(INI)). 2.5.2012. URL: <http://goo.gl/6mxlku>.

<2> Kunke C. Op. cit. P. 1752.

Право, применимое к отношениям,
возникающим при обработке персональных данных

Сбор и обработка персональных данных в Интернете обуславливают потенциальную одновременную применимость к данному процессу множества законов о персональных данных, существующих в различных правовых порядках, в частности законов по месту нахождения оборудования, используемого для обработки; по месту жительства субъекта персональных данных; по месту учреждения оператора персональных данных и т.д. В Европе данная проблема стоит особенно остро. С одной стороны, в связи с существованием 27 различных законов о персональных данных, которые не в полной мере гармонизированы [Директивой](#) 95/46/ЕС от 24 октября 1995 г. "О защите прав частных лиц применительно к обработке персональных данных и о свободном движении таких данных" (далее - [Директива](#) ЕС 95/46/ЕС "О персональных данных"), а с другой - в связи с необходимостью создания единого рынка, для которого вопрос предсказуемости и единообразия в деле определения применимого к предпринимательской деятельности права является одним из наиболее фундаментальных.

Вопросы определения применимого права к процессам обработки персональных данных

регламентируются в [ст. 4](#) Директивы 95/46/ЕС "О персональных данных". По сути, в ней закреплено два основных критерия: 1) критерий места нахождения оператора и 2) критерий места нахождения оборудования.

Первый применяется к обработке персональных данных оператором, осуществляемой в связи с деятельностью его подразделения (**establishment**). В таком случае применяется законодательство страны - члена ЕС, где расположено такое подразделение. При наличии у оператора нескольких подразделений на территории различных стран ЕС к обработке персональных данных применяется право каждой из таких стран ([ст. 4\(1\)\(a\)](#)).

Второй критерий применяется в отношении иностранных лиц, не имеющих подразделений на территории страны - члена ЕС. В соответствии со [ст. 4\(1\)\(c\)](#) государство - член ЕС применяет свое национальное законодательство о персональных данных, если "оператор учрежден не на территории ЕС и в целях обработки персональных данных использует оборудование, расположенное на территории такого государства - участника ЕС (если только такое оборудование не используется исключительно для целей транзита по территории Сообщества)".

Во-первых, достаточно много споров вызывает понятие "оборудование", которое может выступать в качестве привязки деятельности иностранного интернет-сайта к территории соответствующего государства. Например, Рабочей группой [статьи 29](#) (Working Party Article 29), уполномоченной на толкование [Директивы](#) 96/46/ЕС "О персональных данных", было дано толкование, согласно которому

размещение файлов **cookie** <1> на персональных компьютерах европейских пользователей уже само по себе может толковаться как использование оборудования, расположенного на территории ЕС, для целей применения европейского законодательства.

<1> Под **cookie** понимается небольшой файл, отправленный интернет-сайтом и хранимый на компьютере пользователя с целью аутентификации пользователя, хранения персональных предпочтений и настроек пользователя, отслеживания состояния сеанса доступа пользователя, ведения статистики о пользователях (по данным **Wikipedia**).

Во-вторых, в условиях широкого использования "облачных" сервисов, предполагающих "динамическое распределение" вычислительных мощностей в зависимости от конкретных потребностей заказчика, а также "распределенное хранение" данных в различных дата-центрах, определение местонахождения оборудования, используемого для обработки конкретных персональных данных, весьма проблематично и чревато значительным бременем для надзорных органов.

В-третьих, использование местонахождения оборудования в качестве критерия определения юрисдикции чревато неудовлетворительными результатами еще и потому, что может влечь распространение национального законодательства о персональных данных на отношения, которые никоим образом не затрагивают прав и интересов граждан такого государства. Так, право Голландии может применяться к интернет-сайту, принадлежащему

компании в Сингапуре, которая обрабатывает персональные данные сингапурских граждан, только на том основании, что эта компания использует "облачный" сервис провайдера, дата-центр которого находится также и на территории Голландии. Очевидно, что подобный результат выходит за рамки разумной сферы действия законодательства о персональных данных и свидетельствует о нецелесообразности использования рассматриваемого критерия для определения применимости к иностранному интернет-сайту положений [Закона](#) о персональных данных.

В-четвертых, поскольку для размещения своего интернет-сайта можно выбрать серверы, расположенные в самых разных странах, создаются условия для обхода обременительных требований юрисдикций, где владелец интернет-сайта фактически осуществляет свою деятельность. Возможность искусственного подчинения правоотношения правопорядку другого государства не позволяет придавать критерию места нахождения сервера наибольшее значение.

Приняв во внимание указанные сложности, Рабочая группа [ст. 29](#) Директивы 95/46/ЕС высказала мнение о необходимости реформирования подходов к определению применимого права и юрисдикции национальных уполномоченных органов по защите персональных данных ^{<1>}. Ею было выдвинуто предложение о том, что в отношении операторов персональных данных, зарегистрированных за пределами ЕС, будущим законодательством должна приниматься во внимание их направленная деятельность на индивидов. Это предложение нашло отражение в тексте общеевропейского Регламента о защите персональных данных (**General Data Protection**

Regulation), который был принят 27 апреля 2016 г. В соответствии со ст. 3 Регламента его положения применяются к обработке персональных данных, осуществляемой подразделением оператора или "обработчика" на территории ЕС. Положения Регламента также применяются к процессам обработки персональных данных субъектов персональных данных, находящихся на территории ЕС, операторами, не имеющими подразделений на территории ЕС, в случаях, когда такие операторы: 1) предлагают гражданам свои товары или услуги (безотносительно к тому, взимается ли плата за них); 2) осуществляют мониторинг поведения субъектов персональных данных, находящихся на территории ЕС <2>.

<1> Article 29 Data Protection Working Party. Opinion 8/2010 On Applicable Law. 16 December 2010. P. 31 (IV 2 (e)).

<2> Regulation (EU) 2016/679 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation). Положения данного Регламента должны быть имплементированы странами ЕС в течение двух лет, по истечении которых он будет обладать прямым действием на территории всего Европейского союза.

Впрочем, не дожидаясь формального принятия Регламента, критерий направленной деятельности уже в определенной степени нашел свое отражение в европейском законодательстве о персональных данных посредством расширительного толкования понятия "подразделение" оператора Европейским судом

Справедливости. Так, в известном деле **Weltimmo** Суд указал, что при определении местонахождения "подразделения" для целей применения положений [ст. 4\(1\)\(a\)](#) Директивы 96/46/ЕС "О персональных данных" необходимо использовать гибкий подход, понимая под таким местонахождением не только формальное место регистрации (учреждения) такого подразделения, но и любую "реальную и эффективную деятельность, осуществляемую оператором на территории соответствующей страны - члена ЕС посредством каких-либо стабильных средств". Такая деятельность может осуществляться, в частности, через веб-сайт, ориентированный на пользователей конкретной территории, ведущийся на национальном языке соответствующего государства и касающийся объектов, расположенных на его территории <1>.

<1> Weltimmo s.r.o. v. Nemzeti
Adatvédelmi és Információszabadság Hatóság, ECJ,
Case C-230/14, 1 October 2015.

Принцип страны происхождения

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 продолжают дискуссии о

природе принципа "страны происхождения", и многие авторитетные ученые признают за ним значение нормы, регламентирующей применимое право (право страны учреждения провайдера услуги) <1>.

<1> Savin A. Op. cit. P. 71 - 75.

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](#) <1>. 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.

<1> eDate Advertising GmbH v. Martinez, ECR. 25 October 2011. C-509/09.

Ни в коей мере не оспаривая выводы Европейского суда по данному вопросу, полагаю, что принцип "страны происхождения" мог бы быть 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 же свободный "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. Новая редакция [Регламента](#) Брюссель I устранила необходимость прохождения процедуры признания и принудительного исполнения судебного решения, вынесенного на территории другой страны - члена ЕС, судом государства, на территории которого осуществляется исполнение решения. Судебные решения, обладающие юридической силой на территории одного государства - члена ЕС, имеют аналогичную юридическую силу на территории всех остальных государств ЕС. Для инициирования исполнительного производства по такому решению достаточно предъявления его оригинала или надлежащим образом заверенной копии (с переводом при необходимости) и специального сертификата, выдаваемого судом, который вынес решение. Форма такого сертификата приводится непосредственно в [Регламенте](#). Фактически данный сертификат имеет значение исполнительного листа.

Признание судебного решения, вынесенного судом другого государства - члена ЕС, может быть оспорено в специальном суде, который должен был быть обозначен каждым государством членом ЕС до 10 января 2014 г. Такой суд должен незамедлительно рассмотреть соответствующее заявление. Основания

для удовлетворения такого заявления содержатся в [ст. 45](#) Регламента Брюссель I: а) противоречие публичному порядку государства, в котором исполняется решение; б) отсутствие заблаговременного извещения ответчика о начале процесса, что не позволило ему организовать свою защиту; в) наличие противоречащего оспариваемому решению, вынесенного в судах государства, в котором исполняется решение; г) противоречие данного решения вынесенному в судах иных государств решению по тому же предмету между теми же сторонами при условии, что такое решение удовлетворяет критериям, необходимым для его принудительного исполнения. Однако ни при каких условиях суд, рассматривающий вопрос об отказе в признании судебного решения, вынесенного в иной стране - члене ЕС, не вправе пересматривать его по существу ([ст. 52](#) 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.

<1> Regulation EC N 861/2007 of the European Parliament and of the Council of 11 July 2007 establishing a European Small Claims Procedure // OJ 2007. 1199/1.

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.

Наконец, необходимо упомянуть еще два документа, которые имеют непосредственное отношение к рассмотрению споров в сфере электронной коммерции в Европе. Речь идет о Директиве 2013/11/ЕС "Об альтернативном разрешении споров с участием потребителей" (**ADR Directive**), которая должна была быть имплементирована странами - членами ЕС до 9 июля 2015 г., и о Регламенте N 524/2013 "Об онлайн-разрешении споров с участием потребителей" (**ODR Regulation**), который вступил в силу 9 января 2016 г. Появление указанных документов обусловлено стремлением к развитию внутреннего рынка ЕС за счет стимулирования развития трансграничной электронной коммерции. Скорость заключения договора в таких условиях вступает в противоречие с традиционным судебным процессом, сопряженным со значительными временными и

материальными затратами, особенно если он осложняется иностранным элементом.

Основной целью **ADR Directive** является наделение потребителей возможностью удобного, быстрого и низкозатратного рассмотрения спора с предпринимателем за счет использования аккредитованных арбитражных центров, соответствующих указанным в Директиве минимальным стандартам. При этом Директива не предусматривает обязательность для потребителя рассмотрения спора в арбитражном центре.

Арбитражная оговорка необязательна для потребителя, если соглашение заключено до возникновения спора и имеет своей целью лишить потребителя права на рассмотрение спора в судебном порядке (ст. 10 (1)). Правом на обращение в арбитражный центр наделен только потребитель. Предприниматель не вправе инициировать разбирательство в таком суде с целью урегулирования своих претензий по отношению к потребителю (например, в связи с неоплатой товара) (ст. 2(2)(g)). Кроме того, данный механизм рассмотрения споров не может использоваться для урегулирования споров предпринимателей между собой.

ADR Directive устанавливает ряд требований к арбитражным центрам и их арбитрам с целью обеспечения их профессионализма и прозрачности деятельности. Каждый арбитражный центр, претендующий на рассмотрение споров с участием потребителей, обязан обеспечивать раскрытие полной информации о своей деятельности, в том числе в сети Интернет (ст. 7). Помимо необходимой контактной информации нужно также предоставить данные о

процедуре назначения арбитров, процедуре рассмотрения спора, средней продолжительности рассмотрения спора, расходах на рассмотрение споров, общем числе споров и проценте решений в пользу продавца. Арбитражный центр обязан размещать отчеты по рассмотрению им дел, информацию о причинах отказов в иске и часто возникающих проблемах при рассмотрении исков (ст. 19). Данные положения направлены на то, чтобы потребитель мог сделать свободный и обоснованный выбор арбитражного учреждения.

ADR Directive устанавливает предельный срок рассмотрения спора - 90 дней, возможность проведения судебных процедур без личного участия сторон и без обязательного участия представителей-юристов. Максимально широко предполагается использовать функционал современных информационно-телекоммуникационных технологий, в частности интерактивных веб-сайтов.

Разбирательство спора в арбитражном центре должно быть для потребителя бесплатным или сопряжено с уплатой номинальных расходов (ст. 7 (с) **ADR Directive**). По-видимому, с точки зрения европейского законодателя, арбитражные центры в сфере потребительских споров не должны работать на началах самоокупаемости, предполагается их определенное финансирование со стороны государства, которое может окупиться за счет некоторой разгрузки государственной системы судов.

Основной целью принятия **ODR Regulation** является создание организационных и технических условий для имплементации в Европе системы онлайн-разрешения споров, предусмотренных **ADR**

Directive. Регламент включает конкретный механизм обеспечения функционирования арбитражных центров посредством создания единой интернет-платформы, позволяющей потребителю направлять через нее споры, возникающие в сфере электронной коммерции, на рассмотрение конкретных арбитражных центров, соответствующих требованиям Директивы.

§ 4. Юрисдикция в сети Интернет: российский подход

В России компетенция судов по рассмотрению гражданско-правовых споров определяется гражданским процессуальным (ГПК РФ) 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"**). Данные положения применяются **в дополнение** к положениям процессуального законодательства, определяющего подведомственность и подсудность соответствующего спора. Иными словами, для того, чтобы решить вопрос о возможности рассмотрения в суде спора в отношении конкретного иностранного лица, необходимо предварительно положительно решить вопрос о подведомственности и подсудности такого спора по существу (т.е. безотносительно к национальной принадлежности ответчика) данному суду.

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. При этом положения [гл. 44](#) ГПК РФ "Подсудность дел с участием иностранных лиц судам Российской Федерации" имеют приоритет над общими положениями ГПК РФ о подсудности,

содержащимися в [гл. 3 \(ч. 1 ст. 402 ГПК РФ\)](#).

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, и (или) распространяет рекламу в Интернете, направленную на привлечение внимания потребителей, находящихся 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;

10) по делу о защите прав субъекта

персональных данных, в том числе о возмещении убытков и (или) компенсации морального вреда, истец имеет место жительства в Российской Федерации;

11) по делу о прекращении выдачи оператором поисковой системы ссылок, позволяющих получить доступ к информации в информационно-телекоммуникационной сети Интернет, истец имеет место жительства в Российской Федерации.

Особое внимание следует обратить на положение, приведенное в п. 2, согласно которому российский суд общей юрисдикции компетентен рассматривать споры в отношении иностранного лица, которое распространяет в Интернете рекламу, направленную на российских потребителей. Данное положение, равно как и п. 11 данного перечня, было включено в ГПК РФ в рамках имплементации в российское законодательство концепции "права быть забытым", основные положения которой содержатся в ст. 10.3 Закона об информации <1>. Однако положения п. 2 ч. 3 ст. 402 ГПК РФ сформулированы весьма широко и выходят за рамки собственно "обслуживания" первоначальной цели, особенно если их рассматривать вместе с ч. 7 ст. 29 ГПК РФ и ст. 17 Закона о защите потребителей, устанавливающих право потребителя на предъявление иска по месту своего жительства или пребывания <2>. В совокупности данные положения ГПК РФ по существу представляют собой отечественную версию критерия направленности, отраженного в Регламенте Брюссель I. Только в отличие от европейского подхода, не конкретизирующего формы направленности и оставляющего определение факта ее наличия в каждом конкретном случае на усмотрение

правоприменительного органа, при российском подходе формулируется конкретный и единственный критерий: распространение рекламы в Интернете, направленной на российских пользователей.

<1> См.: Федеральный закон от 13 июля 2015 г. N 264-ФЗ "О внесении изменений в Федеральный закон "Об информации, информационных технологиях и о защите информации" и статьи 29 и 402 Гражданского процессуального кодекса Российской Федерации". Подробнее положения о праве лица быть забытым будут рассмотрены в главе о персональных данных.

<2> Представляется, что в соответствии с ч. 1 ст. 402 ГПК РФ положения п. 2 ч. 3 этой же статьи должны рассматриваться в качестве специальной нормы по отношению к ч. 7 ст. 29 ГПК РФ. Они вводят дополнительное условие для установления юрисдикции российского суда в отношении иностранных лиц при распространении ими рекламы, направленной на привлечение внимания российских потребителей. Общее же правило ч. 7 ст. 29 ГПК РФ действует без ограничений применительно к спорам, где в качестве ответчика выступает российское лицо. Иной подход означал бы лишение п. 2 ч. 3 ст. 402 ГПК РФ какого-либо самостоятельного смысла, поскольку безотносительно к факту наличия рекламы, ориентированной на российского потребителя, последний всегда мог бы предъявить иск в суд по своему месту жительства на основании ч. 7 ст. 29 ГПК РФ. Это не только не соответствовало бы системному подходу к толкованию законодательства, в рамках которого каждая норма должна иметь свой смысл, но и противоречило бы основным направлениям развития

юрисдикционных аспектов законодательства о защите прав потребителей, которые отражены в актах международных организаций вроде ОЭСР и в европейском законодательстве. См., например: § 20 Consumer Protection in E-commerce: OECD Recommendation, OECD Publishing, Paris. URL: <http://dx.doi.org/10.1787/9789264255258-en/>.

Выработать критерии направленности рекламы в Интернете на российских пользователей еще только предстоит. Однако уже сейчас можно ожидать, что в числе основных критериев будет изложение такой рекламы на русском языке, а также распространение соответствующей рекламы на веб-сайтах рунета, т.е. зарегистрированных в доменной зоне ".ru", ".рф", ".su" и иных доменах, тесно связанных с территорией РФ, например ".moscow" <1>. По всей вероятности, в качестве возможного ориентира могут быть использованы подходы, выработанные применительно к определению сферы действия законодательства о персональных данных (см. далее).

<1> Данный критерий уже давно используется ФАС РФ для целей определения сферы применения [Закона](#) о рекламе в Интернете ([письмо](#) ФАС России от 3 августа 2012 г. N АК/24981 "О рекламе алкогольной продукции в Интернете и печатных СМИ"). См. подробнее [гл. 8](#) настоящей книги.

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 Интернета.

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. 7 \(1\) Регламента Брюссель I](#)) 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 место нахождения (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.

<1> Все остальные перечисленные в данной статье варианты явно не подходят к рассматриваемым отношениям.

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 РФ о защите прав потребителей](#) иск может быть предъявлен 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>. Как отмечалось ранее, с недавних пор российское процессуальное законодательство ввело критерий направленности деятельности в виде распространения рекламы в Интернете, рассчитанной на российских пользователей, как условия установления компетенции российского суда в отношении иностранного лица. Таким образом, для обоснования юрисдикции российского суда в отношении иностранного интернет-магазина необходимо доказать факт распространения таким интернет-магазином рекламы в Интернете, направленной на российских пользователей. Такая реклама может распространяться в форме баннеров, сообщений электронной почты, поисковой (контекстной) рекламы. Как отмечалось ранее, пока практикой не выработано конкретных критериев направленности, однако, как представляется, о ее наличии могут свидетельствовать факты распространения рекламы на русском языке и (или) на веб-сайтах рунета.

<1> [Пункт 22](#) Постановления Пленума Верховного Суда РФ от 28 июня 2012 г. N 17 "О рассмотрении судами гражданских дел по спорам о защите прав потребителей"; [п. 7](#) информационного письма Президиума ВАС РФ от 13 сентября 2011 г. N 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".

Необходимо отметить, что в силу древности российских законов о защите прав потребителей отношения, связанные с распространением цифрового контента, при излишне формальном толковании таких

законов могут "выпасть" из-под сферы их применения, а вместе с ними - и положения о возможности предъявления иска по месту жительства потребителя (см. подробнее § 7 гл. 6 настоящей книги). Однако даже при самом пессимистичном сценарии - нежелании российского суда распространять нормы законодательства о защите прав потребителей на отношения, связанные с приобретением цифрового контента, - у потребителя сохраняется возможность в некоторых случаях "затащить" иностранное лицо в российский суд в случае перекалфикации спора с потребительского на спор о незаконной обработке персональных данных. Такая возможность существует в силу того, что большая часть зарубежных интернет-магазинов осуществляет обработку персональных данных своих клиентов, и при нарушении условий договора со стороны предпринимателя (например, непредоставлении цифрового контента или блокировании аккаунта пользователя) можно сослаться на нарушение законодательства о персональных данных (требований к получению согласия, локализации процессов обработки данных и пр.), при условии, что на отношения по обработке персональных данных будет распространяться российское законодательство <1>.

<1> Данный вопрос будет подробнее рассмотрен далее.

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) или арбитража (арбитражная оговорка), в котором подлежат

рассмотрению споры, возникающие из такого договора. В связи с этим 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 зарубежными аффилированными лицами российских компаний.

<1> [Пункт 1](#) информационного письма Президиума ВАС РФ от 9 июля 2013 г. N 158 "Обзор практики рассмотрения арбитражными судами дел с участием иностранных лиц".

Российская судебная практика выработала ряд положений, направленных на обеспечение баланса интересов сторон при заключении пророгационных соглашений. Так, такие соглашения не могут носить "асимметричный" 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 <1>. Как отмечается, в основу этой правовой позиции были положены [ст. 1](#) ГК РФ, закрепляющая принцип равенства, а также [ст. 168](#) ГК РФ, согласно которой признается ничтожной сделка, не соответствующая требованиям закона <2>. Позиция ВАС РФ по данному вопросу представляется небесспорной, тем более что подходы к решению вопроса о правомерности применения асимметричных арбитражных оговорок различаются в разных странах <3>. Возможно, в силу отсутствия в указанном [Постановлении](#) ВАС РФ четкой и убедительной аргументации приведенной позиции в последнее время стали появляться судебные решения, в которых российские арбитражные суды признают действительной такую асимметричную юрисдикционную оговорку, если она допустима в соответствии с правом, применимым к договору <4>. Но в любом случае можно утверждать, что подобного рода оговорки находятся в зоне риска возможного непризнания их российским судом.

<1> [Постановление](#) Президиума ВАС РФ от 19 июня 2012 г. N 1831/12.

<2> Егоров А.В. [Асимметричные оговорки о разрешении споров](#) судебная практика заменяет на симметричные // Вестник международного коммерческого арбитража. 2012. N 2. С. 187.

<3> См. обзор, подготовленный юридической фирмой Clifford Chance: Unilateral Option Clauses in Arbitration: a Survey as to their Effectiveness. 2013. URL: <http://goo.gl/w35K5M>. См. также: Зенькович Д.И. Асимметричные арбитражные соглашения в России и за

рубежом // Отрасли права. 02.06.2015. URL: <http://отрасли-права.рф/article/8077>.

<4> См.: [Постановление](#) Пятнадцатого апелляционного арбитражного суда по делу N А53-17338/2014 от 12 марта 2015 г. В нем суд указал, что право выбора между арбитражем и государственным судом, предоставленное истцу по договору, не противоречит законодательству, так как оно является допустимым в соответствии с английским правом, применимым к соответствующему договору.

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>.

<1> Пункт 6 информационного письма Президиума ВАС РФ от 9 июля 2013 г. N 158 "Обзор практики рассмотрения арбитражными судами дел с участием иностранных лиц".

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).

Что же касается арбитражных оговорок, то они не

вызывают каких-либо особых проблем в предпринимательских договорах, напротив, наличие специального международного соглашения о признании и приведении в исполнение иностранных арбитражных решений, участниками которого являются 156 стран, включая Россию, существенно облегчает рассмотрение вопросов принудительного исполнения решения, вынесенного арбитражем на территории разных стран мира <1>. Правда, необходимо проявлять достаточную степень внимательности при формулировании соответствующих арбитражных оговорок, в том числе в части конкретизации споров, которые могут быть переданы на рассмотрение арбитража. В противном случае, как показывает практика, вместо запланированного Лондонского международного арбитражного суда (The London Court of International Arbitration) можно оказаться в Советском районном суде г. Нижнего Новгорода <2>.

<1> [Конвенция](#) о признании и приведении в исполнение иностранных арбитражных решений (Нью-Йорк, 1958 г.) (Нью-Йоркская конвенция).

<2> См.: решение Советского районного суда г. Нижнего Новгорода от 7 декабря 2015 г. по делу N 2-6575/2015. URL: <http://goo.gl/5VxOue>.

Одним из актуальных вопросов является допустимость арбитражных оговорок в договорах с участием потребителей. С одной стороны, законодательство о защите прав потребителей не содержит никаких специальных запретов на рассмотрение споров из потребительских договоров в третейских судах. С другой стороны, подобное

рассмотрение споров может быть сопряжено с дополнительными обременениями для потребителя: необходимостью несения расходов (при рассмотрении спора в государственном суде потребитель освобожден от уплаты госпошлины), поездок к месту рассмотрения спора. Кроме того, существуют риски необъективного рассмотрения спора в случае, если арбитраж каким-либо образом аффилирован с предпринимателем.

По мнению Верховного Суда РФ, арбитражные оговорки в потребительских договорах по общему правилу допустимы <1>. Однако если арбитражная оговорка включена в договор присоединения, то она будет иметь правовое значение, если потребитель впоследствии признает действительность этого условия и будет настаивать на рассмотрении спора именно в третейском суде <2>. Таким образом, арбитражная оговорка, включенная в **click-wrap**-соглашение с потребителем, не лишает его возможности предъявления иска в суд по своему месту жительства, **а предоставляет ему возможность выбора** оптимального места для рассмотрения спора <3>. Если после возникновения спора потребитель подтвердит свою волю на рассмотрение спора в третейском суде, то результаты последующего разбирательства будут иметь юридическую силу и могут быть принудительно исполнены в порядке, установленном [гл. 47 ГПК РФ](#). Правда, следует отметить, что существует практика арбитражных судов, согласно которой включение в потребительский договор, заключаемый по модели присоединения, условия о рассмотрении споров в третейском суде может влечь административную ответственность за включение в договор условия, ущемляющего права потребителя ([ст. 14.8 КоАП РФ](#)) <4>.

<1> Пункт 1 раздела "Судебная практика по гражданским делам" Обзора судебной практики Верховного Суда Российской Федерации за четвертый квартал 2011 г.

<2> Там же.

<3> Данная идея нашла свое отражение и в [Определении](#) Конституционного Суда РФ от 4 октября 2012 г. N 1912-О: "Предоставление заинтересованным лицам права по своему усмотрению обратиться за разрешением спора в государственный суд (суд общей юрисдикции, арбитражный суд) в соответствии с его компетенцией, установленной законом, или избрать альтернативную форму защиты своих прав и обратиться в третейский суд - в контексте гарантий, закрепленных [статьями 45 \(часть 2\) и 46](#) Конституции Российской Федерации, - само по себе не может рассматриваться как их нарушение, а, напротив, расширяет возможности разрешения споров в сфере гражданского оборота".

<4> "Включение в типовой договор с гражданами-потребителями условия о рассмотрении спора в третейском суде лишает потребителя права на выбор по своему усмотрению судебной защиты нарушенных или оспариваемых прав и ущемляет установленные законом права, что образует состав административного правонарушения, предусмотренного [частью 2 статьи 14.8](#) КоАП РФ" ([Постановление](#) Президиума ВАС РФ от 17 сентября 2013 г. N 3364/13 по делу N А65-15588/2012).

Представляется, что подход ВС РФ является

более сбалансированным, чем позиция ВАС РФ, и будет преобладать при рассмотрении вопросов о правовой оценке условий пользовательских соглашений и иных договоров в сфере электронной коммерции. В том числе и потому, что он создает определенные условия для применения в России альтернативных способов разрешения споров в сфере потребительских договоров, хотя до европейского уровня в данном вопросе нам еще далеко.

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.

<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.

В определенной степени данное ограничение по защите прав правообладателей, существующее у судов общей юрисдикции, компенсируется положениями Антипиратского закона <1>. Данный Закон предусматривает исключительную юрисдикцию Мосгорсуда по рассмотрению по первой инстанции споров правообладателей о защите авторских и (или) смежных прав (кроме фотографий) в сети Интернет, если при этом были приняты предварительные

обеспечительные меры в порядке [ст. 144.1](#) ГПК РФ об ограничении доступа к интернет-ресурсам, на которых осуществляется распространение объектов авторского и (или) смежного права без согласия правообладателя или иного законного основания <2>. Причем Мосгорсуд компетентен рассматривать подобного рода споры безотносительно к наличию или отсутствию у правообладателя предпринимательского статуса.

<1> Под Антипиратским законом понимается совокупность норм, введенных в российское законодательство Федеральными законами от 2 июля 2013 г. [N 187-ФЗ](#) "О внесении изменений в законодательные акты Российской Федерации по вопросам защиты интеллектуальных прав в информационно-телекоммуникационных сетях" и от 24 ноября 2014 г. [N 364-ФЗ](#) "О внесении изменений в Федеральный закон "Об информации, информационных технологиях и о защите информации" и Гражданский процессуальный кодекс Российской Федерации".

<2> Комментарий к положениям Антипиратского закона см.: Савельев А.И. [Комментарий](#) к Федеральному закону от 27 июля 2006 г. [N 149-ФЗ](#) "Об информации, информационных технологиях и защите информации" (постатейный). М.: Статут, 2015.

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, регистрацией 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).

<1> [Постановление](#) ФАС Московского округа от 28 ноября 2012 г. по делу N А40-131680/11-51-1187.

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 Интернете 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.

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, формулировка данного пункта - не самая удачная для целей обоснования юрисдикции российских арбитражных судов в отношении споров, связанных с регистрацией доменных имен на территории Российской Федерации. Хотя на практике суды ее активно используют для обоснования юрисдикции российских арбитражных судов по спорам, связанным с запретом использования товарного знака, фирменного наименования в доменном имени, зарегистрированном в зоне ".ru", и о передаче права администрирования доменного имени <2>.

<1> См. подробнее § 5 гл. 5 настоящей книги.

<2> См., например: **Определение** Верховного Суда РФ от 7 декабря 2015 г. N 305-ЭС15-15588 по делу N A40-102183/13: "Суд пришел к выводу о наличии компетенции у арбитражных судов Российской Федерации рассматривать настоящий спор, поскольку спорное доменное имя зарегистрировано в доменной зоне "RU" и его регистрация осуществлялась регистратором (обществом "РСИЦ"), находящимся на территории Российской Федерации"; **Постановление** Суда по интеллектуальным правам от 2 октября 2014 г. N C01-856/2014 по делу N A40-102183/2013: "Поскольку доменное имя, о запрете администрирования которого

ответчиком просит истец, зарегистрировано в доменной зоне ".ru", рассматриваемый спор относится к компетенции арбитражных судов Российской Федерации".

Упоминание в п. 9 ч. 1 ст. 247 АПК РФ 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 Интернете, 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 Интернете 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 Интернете, подлежит исполнению на территории Российской Федерации, то в соответствии с положениями п. 3 ч. 1 ст. 247 АПК РФ иск может быть и так предъявлен по месту исполнения договора безотносительно к использованию Интернета 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 Интернете, 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 круг споров, могущих возникнуть из цивилистических отношений, практически невозможно <2>.

<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. N 11.

<2> 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. N 2.

Анализ небогатой судебной практики, в которой данное основание фигурировало в качестве относительно самостоятельного (а не в качестве "подкрепления" иных оснований, указанных в [ст. 247 АПК РФ](#)), 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 <1>. В одном из споров фигурировал в качестве возможного критерия и русский язык как язык договора <2>. Кроме того, может приниматься во внимание акцессорный характер обязательства, в связи с которым возник спор, по отношению к основному

обязательству, должником по которому является российское лицо <3>. 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. <4>.

<1> **Постановление** Девятого арбитражного апелляционного суда от 18 апреля 2011 г. N 09АП-7645/2011 по делу N А40-116933/09-50-926, оставленное в силе **Постановлением** ФАС Московского округа от 8 августа 2011 г. N КГ-А40/6186-11.

<2> **Определение** ВАС РФ от 28 октября 2011 г. N ВАС-8661/11 по делу N А60-7981/2010-С2.

<3> **Постановление** ФАС Московского округа от 9 октября 2012 г. по делу N А40-51127/12-114-475: "Кроме того, залоговое обязательство является дополнительным (акцессорным) обязательством по отношению к обеспечиваемому им основному обязательству по кредитным договорам, должником по которому также является российская организация... Данные обстоятельства свидетельствуют о наличии тесной правовой связи спорного правоотношения с территорией Российской Федерации".

<4> **Постановление** Девятого арбитражного апелляционного суда от 24 марта 2008 г. N

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. N 12.

И наоборот. Если судом установлено, что заявленные исковые требования вытекали из деятельности иностранной компании за рубежом, исполнение по спорному договору осуществлялось на территории иностранного государства, большинство доказательств расположено на территории иностранного государства, а правом, применимым к договору, было право иностранного государства, то оснований для применения положений [п. 10 ч. 1 ст. 247 АПК РФ](#) нет <1>.

<1> См. [п. 8](#) информационного письма Президиума ВАС РФ от 9 июля 2013 г. N 158 "Обзор практики рассмотрения арбитражными судами дел с участием иностранных лиц".

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. Как отметил суд в одном из своих решений, "сам факт предполагаемого причинения убытков на территории Российской Федерации свидетельствует о наличии тесной связи спорного правоотношения с указанной территорией" <1>.

<1> [Постановление](#) СИП от 2 июля 2014 г. N C01-471/2014 по делу N A40-56928/2004.

Также критерий тесной связи может быть использован применительно к договорам, по которым распространяются электронные 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 место жительства 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 **произведен** (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 (**lexfori**), при решении вопроса о применимом праве суд руководствуется в том числе и правилами коллизионного регулирования, допускающими широкую автономию воли по выбору иностранного права. Установление судом своей юрисдикции в отношении спора само по себе не влечет применения законодательства страны суда к такому спору <3>.

<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. N 668. P. 446. Цит. по: Крохалев С.В. Категория публичного порядка в международном гражданском процессе. СПб., 2006. § 350.

<3> **Пункт 12** информационного письма Президиума ВАС РФ от 9 июля 2013 г. N 158 "Обзор

практики рассмотрения арбитражными судами дел с участием иностранных лиц".

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.

Право, применимое к договорным обязательствам

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 собственно 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 <1>, связь договора с иными договорами, содержащими условие о применимом праве <2>.

<1> Там же.

<2> Асосков А.В. [Указ. соч.](#) С. 126 и сл.

Таким образом, по общему правилу оговорки о применимом праве, сделанные в договорах, заключаемых посредством Интернета, в том числе click-wrap-соглашениях, подлежат признанию со стороны российских судов <1>. Российское гражданское право не ограничивает выбор применимого права требованиями о наличии разумной связи между таким правом и регулируемым им правоотношением, как это отчасти имеет место в США.

<1> Правовой статус и условия действительности подобных соглашений будут подробно рассмотрены далее.

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. 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>.

<1> Федеральный [закон](#) от 30 сентября 2013 г. N 260-ФЗ "О внесении изменений в часть третью Гражданского кодекса Российской Федерации".

<2> Подробный анализ см.: Асосков А.В. [Указ. соч.](#) С. 418 - 437.

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, 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. 2 ст. 1211 ГК РФ такой стороной является исполнитель <1>.

<1> Подпункт "б" п. 12 ст. 3 проекта Федерального закона N 47538-6 "О внесении изменений в части первую, вторую, третью и четвертую Гражданского кодекса Российской Федерации, а также в отдельные законодательные акты Российской Федерации".

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 Интернета, 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 исключительного 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.

<1> См.: Международное частное право: Постатейный [комментарий](#) раздела VI Гражданского кодекса Российской Федерации / Под ред. П.В. Крашенинникова. М., 2010. С. 186 - 187.

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. 447](#) 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 <1>. 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".

<1> Асосков А.В. [Указ. соч.](#) С. 452.

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.

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.

Согласно [ст. 1212](#) ГК РФ в редакции, действующей с 1 ноября 2013 г. <1>, 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.

<1> О содержании предыдущей редакции [ст. 1212](#) ГК РФ и связанных с ней проблемах в сфере электронной коммерции см. первое издание настоящей работы. С. 121 - 124.

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 (как того требует [Директива 2011/83/ЕС "О правах потребителей"](#)), 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](#).

<1> Асосков А.В. [Указ. соч.](#) С. 174.

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. При заключении потребителем договора в отсутствие направленной деятельности профессиональной стороны на территорию его места жительства применимое право определяется по общим правилам [ст. 1211 ГК РФ](#).

Кроме того, необходимо иметь в виду, что критерий направленной деятельности и соответствующие ему защитные положения о применимом праве не применяются в отношении договоров перевозки, а также в отношении договоров на выполнение работ (оказание услуг), если работа или

услуга подлежит выполнению исключительно в иной стране, чем страна места жительства потребителя. Таким образом, положения российского законодательства о защите права потребителей не могут быть применены к отношениям, возникающим при приобретении авиабилетов посредством Интернета, например для целей определения последствий отказа от договора со стороны потребителя <1> или ненадлежащего исполнения договора со стороны перевозчика <2>.

<1> См., например: [Постановление](#) ФАС Волго-Вятского округа от 24 июля 2014 г. по делу N A43-13631/2013.

<2> Апелляционные определения Омского областного суда от 7 октября 2015 г. по делу [N 33-6031/2015](#); Московского городского суда от 18 сентября 2015 г. по делу [N 33-32008/2015](#).

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 Интернете. 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.

<1> См.: Бабкин С.А. Право, применимое к отношениям, возникающим при использовании сети Интернет: Основные проблемы. С. 50.

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 <1>.

<1> См.: Там же. С. 51.

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 Интернете 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 Интернете, могло предполагать возможность причинения ею вреда в стране, где проживает или располагается потерпевший (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.

<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. ст. 14.1 - 14.8 Федерального закона от 26 июля 2006 г. N 135-ФЗ "О защите конкуренции" (далее - Закон о защите конкуренции).

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" <1>. Данная позиция является достаточно традиционной для российского права <2>.

<1> Канашевский В.А. Международное частное право: Учебник. М.: Международные отношения, 2006. С. 458 - 459.

<2> 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.

^{<1>} Progoff S., Halpern M., Feinberg I. Understanding the Intellectual Property License. Practicing Law Institute. 2004. P. 613.

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 <1>. 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 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 <2>. Таким образом, анализ вопросов принадлежности исключительного права российскому автору или его зарубежному работодателю должен осуществляться по нормам ГК РФ (ст. 1295).

<1> Гаврилов Э. Решение вопросов международного частного права в части четвертой Гражданского кодекса Российской Федерации // Хозяйство и право. 2008. N 3.

<2> См.: [Комментарий](#) к части четвертой Гражданского кодекса Российской Федерации (поглавный) / Под ред. А.Л. Маковского. М., 2008. С. 305.

В проекте изменений в ГК РФ предлагалось включить в [разд. VI](#) ГК РФ [ст. 1207.2](#), специально посвященную статусу права интеллектуальной собственности <1>:

<1> 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.

"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 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. Таким образом, предлагавшаяся редакция [ст. 1207.2](#) обладала теми же недостатками, что и соответствующие положения [Регламента](#) Рим II, и никак не учитывала этот факт, впрочем, как и специфику сети Интернет в принципе. Кроме того, в случае принятия данного положения оно создавало бы дополнительные проблемы для российских

правообладателей, которые, защищая свои права от нарушений в сети Интернет в российском суде, были бы вынуждены нести бремя установления содержания права множества различных стран. Все это послужило причиной отклонения данной поправки. Как следствие, **lex loci protectionis** так и не стал частью российского коллизионного права. Вместо него применяются положения [ст. 1231](#) ГК РФ.

Право, применимое к отношениям,
возникающим при обработке персональных данных

Законодательство о персональных данных представляет собой комплексную отрасль, включающую как положения частноправового характера, основанные на принципах автономии воли (например, в части регулирования согласия субъекта персональных данных на обработку его данных, заключения договоров между оператором и лицом, осуществляющим обработку персональных данных по его поручению, и т.п.), так и положения публичного права (например, в части регулирования статуса уполномоченного органа по надзору и контролю в сфере персональных данных, требований к обработке данных и локализации). Кроме того, законодательство о персональных данных играет важную роль в обеспечении национальных интересов в сфере информационной безопасности. Все это обуславливает необходимость определения сферы применения законодательства о персональных данных по кругу лиц и территории в случае обработки персональных данных в сети Интернет. Федеральный [закон](#) от 27 июля 2006 г. N 152-ФЗ "О персональных данных" (далее - Закон о персональных данных) не содержит специальных положений на сей счет. Соответствующие разъяснения ^{<1>} были даны Минкомсвязи России, который является федеральным

органом исполнительной власти, осуществляющим функции по выработке и реализации государственной политики и нормативно-правовому регулированию в сфере обработки персональных данных (п. 1 Положения о Министерстве связи и массовых коммуникаций Российской Федерации <2>). В связи с этим их можно рассматривать в качестве изложения официальной позиции регулятора в сфере законодательства о персональных данных, хотя они формально не являются юридически обязательными для судов.

<1>

<http://www.yaz.ru/personaldata/#1438546529980>

<2> Данное **Положение** утверждено Постановлением Правительства РФ от 2 июня 2008 г. N 418 "О Министерстве связи и массовых коммуникаций Российской Федерации". В соответствии с п. 6.6 указанного Положения Минкомсвязи России имеет право давать государственным органам, органам местного самоуправления, юридическим и физическим лицам разъяснения по вопросам, отнесенным к сфере ведения Министерства.

В соответствии с разъяснениями Минкомсвязи России, при осуществлении деятельности в сети Интернет, которая в силу своего трансграничного, децентрализованного и виртуального характера не позволяет четко обозначить географические границы осуществления такой деятельности, необходимо установить специальные критерии, при которых она может быть отнесена к осуществляемой на территории РФ. Одной лишь доступности интернет-сайта на территории РФ недостаточно для вывода о том, что на него распространяется законодательство РФ, в том

числе о персональных данных, поскольку в таком случае сфера его применения носила бы по существу всемирный характер и делала бы практически невозможным контроль за его деятельностью. В связи с этим, по мнению Минкомсвязи России, необходимо руководствоваться критерием направленной деятельности, который уже нашел свое отражение как в европейском, так и в российском законодательстве.

О наличии направленности интернет-сайта на территорию Российской Федерации могут свидетельствовать следующие обстоятельства: 1) использование доменного имени, связанного с Российской Федерацией или субъектом Федерации (".ru", ".рф.", ".su", ".москва", "moscow" и т.п.), и (или) 2) наличие русскоязычной версии интернет-сайта, созданной владельцем такого сайта или по его поручению иным лицом (использование на сайте или самим пользователем плагинов, предоставляющих функционал автоматизированных переводчиков с различных языков, не должно приниматься во внимание). При этом, поскольку русский язык широко используется в некоторых странах за пределами РФ, для определения направленности интернет-сайта именно на территорию РФ дополнительно необходимо наличие как минимум одного из следующих элементов: возможности осуществления расчетов в российских рублях; возможности исполнения заключенного на таком интернет-сайте договора на территории РФ (договоров доставки товара, оказания услуг или пользования цифровым контентом на территории России), использования рекламы на русском языке, отсылающей к соответствующему интернет-сайту, или иных обстоятельств, явно свидетельствующих о намерении владельца интернет-сайта включить российский рынок в свою бизнес-стратегию.

Таким образом, исходя из приведенной позиции Минкомсвязи России можно выделить два базовых и ряд дополнительных (вторичных) критериев, свидетельствующих о направленности деятельности иностранного интернет-сайта на территорию РФ.

Базовые критерии:

1) использование таким интернет-сайтом доменного имени, связанного с территорией РФ (".ru", ".su", ".рф") и ее регионами (".москва", ".moscow"). При этом необходимо именно фактическое использование такого доменного имени, т.е. "привязка" к конкретному интернет-сайту, в том числе посредством реализации функции "переадресации" (**redirect**) на интернет-сайт, зарегистрированный под функциональными доменами (вроде ".com"). Регистрация доменного имени для целей предотвращения киберсквоттинга, не сопровождающаяся фактическим использованием, не должна приниматься во внимание для решения вопроса о сфере действия законодательства РФ о персональных данных <1>; либо

<1> Представляется, что в некоторых случаях, при наличии иных очевидных факторов, свидетельствующих о направленности на территорию РФ, во внимание может приниматься также и использование доменного имени, зарегистрированного в иных доменных зонах, но с использованием специального раздела ".ru" (например, ".com.ru").

2) наличие русскоязычной локализованной версии такого интернет-сайта.

Вторичные критерии (используются в качестве дополнительных применительно ко второму базовому критерию):

1) возможность заключения договора с российскими пользователями;

2) возможность доставки товара или цифрового контента на территорию РФ;

3) оказание приобретаемой через интернет-сайт услуги на территории РФ;

4) возможность осуществления расчетов в российских рублях;

5) наличие русскоязычной рекламы данного интернет-сайта.

При этом для вывода о направленности деятельности русскоязычного интернет-сайта иностранного происхождения на территорию РФ достаточно установить наличие хотя бы одного из вышеперечисленных вторичных критериев.

Рассмотрим применение данных критериев на примерах.

1. Предположим, что имеется интернет-магазин, принадлежащий зарубежной компании, который использует доменное имя в зоне ".com". Интерфейс данного ресурса выполнен на английском языке, при этом отсутствует русскоязычная версия. Возможность размещения заказа и доставки товара (контента) существует для любых пользователей безотносительно к их национальной или географической

принадлежности. При таких обстоятельствах данный интернет-магазин не подпадает под действие [Закона](#) о персональных данных, поскольку отсутствуют основные критерии направленности деятельности данного сайта именно на российских пользователей.

2. Интернет-магазин использует доменное имя в зоне ".com" и обладает русскоязычной версией. При этом он содержит оговорку о том, что товары и (сервисы) не предоставляются жителям на территории РФ, которая подкреплена иными мерами, явно свидетельствующими об отсутствии намерения осуществлять целенаправленную деятельность на территорию РФ (отказ в приеме к оплате банковских карт, выпущенных российскими банками; использование технологий геолокации с определением географической принадлежности IP-адреса пользователя с блокировкой возможности совершения заказа/доставки товара/получения контента пользователями с IP-адресами российских интернет-провайдеров). При таких обстоятельствах можно сделать вывод о том, что деятельность такого интернет-магазина не направлена на территорию РФ и что на деятельность по обработке персональных данных пользователей такого ресурса не распространяются требования [Закона](#) о персональных данных.

3. Интернет-сайт, представляющий собой социальную сеть, принадлежит иностранной компании и использует доменное имя в зоне ".com". При этом существует русскоязычная версия данного сервиса. Российский пользователь имеет возможность пользования данным сервисом, заключив пользовательское соглашение, которое переведено на русский язык. Кроме того, в иных русскоязычных

интернет-сайтах предоставлена возможность авторизации через аккаунт рассматриваемой социальной сети. При таких обстоятельствах есть основания утверждать, что деятельность указанного интернет-сайта направлена на российских пользователей и в части обработки персональных данных должна соответствовать требованиям [Закона](#) о персональных данных.

4. Интернет-сервис, интерфейс которого выполнен на английском языке, принадлежит иностранной компании и при этом использует доменное имя, зарегистрированное в зоне ".ru", в качестве непосредственного доменного имени интернет-ресурса или для целей переадресации на иной адрес. Рассматриваемый сервис доступен для заказа и использования любому пользователю, безотносительно к его национальной или географической принадлежности. По общему правилу деятельность такого сервиса может рассматриваться в качестве направленной на территорию РФ в силу использования географического доменного имени, непосредственно связанного с Российской Федерацией. При этом используемый на интернет-сайте язык не имеет значения.

Представляется, что критерий направленной деятельности является наиболее сбалансированным для целей применения к отношениям, возникшим в связи с обработкой персональных данных в сети Интернет. С одной стороны, он позволяет вывести из-под сферы действия [Закона](#) о персональных данных те интернет-сайты, которые не имеют какой-либо связи с территорией РФ, с другой - он позволяет владельцам интернет-сайтов предположить возможность применения к ним требований законодательства и

предпринять соответствующие меры. Также данный критерий обладает достаточной гибкостью, позволяющей противодействовать мерам по обходу [Закона](#), который может иметь место при использовании иных критериев (например, месторасположения сервера или места учреждения владельца интернет-сайта).

При этом следует подчеркнуть (хотя это и не отмечено в приведенной позиции Минкомсвязи России), что критерий направленности должен применяться лишь к тем интернет-сайтам, в рамках которых осуществляется какая-либо правомерная деятельность (например, продажа товаров/услуг, не исключенных из оборота). Сбор и обработка персональных данных в таких случаях не являются самоцелью, а осуществляются для целей обеспечения такой правомерной деятельности и как таковые имеют в своей основе какое-либо законное основание (согласие субъекта или основание, предусмотренное [Законом](#)).

Если же в рамках интернет-сайта осуществляется преимущественно противоправная деятельность, а сбор/обработка персональных данных российских пользователей осуществляются в отсутствие их согласия или иного законного основания и сопряжены с массовыми нарушениями их прав (например, такой интернет-сайт распространяет базы с персональными данными российских граждан), то в отношении этого интернет-сайта могут быть приняты меры в соответствии с законодательством РФ вне зависимости от наличия критериев, свидетельствующих о направленности такого интернет-сайта на российских пользователей.

Как будут применяться разъяснения Минкомсвязи России на практике, покажет время. Но в любом случае

они представляют собой достаточно прогрессивный подход к решению проблемы регулирования процессов обработки персональных данных в трансграничной среде Интернета. Остается выразить надежду, что он найдет свое отражение в [Законе](#) о персональных данных, особенно учитывая, что критерий направленной деятельности уже нашел свое отражение не только в [ст. 1212 ГК РФ](#), но и в [Законе об информации применительно к поисковым системам \(ст. 10.3\)](#) и [ГПК РФ](#).

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. N 5105/08 по делу N A40-73830/06-25-349.

<3> [Постановление](#) ФАС Московского округа от 17 февраля 2009 г. N КГ-А40/12786-08-П по делу N A40-7480/08-68-127.

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. N 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>. Иными словами, в настоящее время суды исходят в основном из принципа "фактической взаимности", т.е. из необходимости наличия положительных доказательств фактов исполнения российских судебных решений либо убедительных обоснований исполнимости этих решений в странах, откуда исходят такие судебные решения. В российской судебной практике пока не нашел своего отражения принцип "презюмируемой взаимности", при котором наличие взаимности предполагается, пока отсутствуют конкретные данные, свидетельствующие об отказе в признании российских судебных решений в стране, вынесшей подлежащее принудительному исполнению решение.

<1> [Определение ВАС РФ от 7 декабря 2009 г. N ВАС-13688/09 по делу N А41-9613/09.](#)

<2> **Постановление** ФАС Московского округа от 17 февраля 2009 г. N КГ-А40/12786-08-П по делу N 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. N 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".

Помимо применения в отечественной судебной практике принципа "фактической взаимности", формализм при применении положений **ст. 241** АПК РФ также значительно "смягчается" за счет расширительного толкования понятия "международный договор", когда в качестве такового признаются международные соглашения, в которых отсутствуют непосредственные указания на взаимное признание и принудительное исполнение решений судов сторон таких соглашений. Так, в одном из дел ВАС РФ сослался в качестве дополнительного основания признания решения ирландского суда на наличие

международного акта - Конвенции ООН против коррупции 2003 г., участниками которой являются и Россия, и Великобритания и которая налагает на них обязанность содействовать друг другу в осуществлении мер, направленных на более эффективное и действенное предупреждение коррупции в частном секторе и борьбу с ней (п. 2 ст. 12), в том числе посредством признания контрактов, совершенных под влиянием коррупционных факторов, недействительными (ст. 34). Поскольку в решении ирландского суда были отмечены подозрительность оспариваемого договора и возможное наличие в нем коррупционной составляющей, ВАС РФ счел возможным сослаться на Конвенцию ООН как на международный договор, необходимый для признания и принудительного исполнения иностранного судебного решения на территории Российской Федерации <1>. Данное решение демонстрирует расширительный подход к толкованию понятия "международный договор" для целей признания и принудительного исполнения иностранного судебного решения. Впоследствии ВАС РФ продолжал следовать данному подходу, признав в качестве такого международного договора Соглашение между Правительством РФ и Правительством Соединенного Королевства Великобритании и Северной Ирландии об экономическом сотрудничестве от 9 ноября 1992 г., в котором нет ни слова о взаимном признании и исполнении решений судов, но говорится о предоставлении физическим и юридическим лицам каждой из стран национального режима в судебных процессах на территории другой страны в связи с торговыми сделками (ст. 11) <2>.

<1> Постановление Президиума ВАС РФ от 8 октября 2013 г. N 6004/13.

<2> [Постановление](#) Президиума ВАС РФ от 28 января 2014 г. N 3366/13.

Если суд установит наличие международного договора или фактической 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 большую 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 было 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. N 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". См. также: Куделич Е.А. [Трансграничное исполнение судебных решений](#) в России: в плену устоявшихся стереотипов или поступательное движение вперед? // Закон. 2015. N 5. С. 148 - 151.

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>;

<1> См., например: [Постановление](#) ФАС

Уральского округа от 29 декабря 2003 г. по делу N А71-288/2002-Г10.

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 <1>. По мнению Верховного Суда РФ, под публичным порядком 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 <2>. 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.

<1> 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.

<2> **Определения** Судебной коллегии по гражданским делам Верховного Суда РФ от 25 сентября 1998 г. по делу N 5-Г98-60.

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 <1>. 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.

<1> Информационное письмо Президиума ВАС РФ от 26 февраля 2013 г. N 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).

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 правовой системы, или с несколько иным содержанием, нежели принятое 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.

<1> Пункт 5 информационного письма Президиума ВАС РФ от 26 февраля 2013 г. N 156.

Непривлечение к участию в деле третьих лиц может быть расценено как нарушение их фундаментального права на судебную защиту, препятствующее приведению в исполнение соответствующего иностранного судебного решения со ссылкой на противоречие такого решения публичному порядку Российской Федерации <1>. Однако суд может весьма избирательно подходить к определению наличия или отсутствия такого нарушения в некоторых случаях. Достаточно показательным является дело, рассмотренное Президиумом ВАС РФ, в котором ВАС РФ счел, что права третьих лиц - российских компаний - цессионариев не затрагиваются решением ирландского суда о признании исходного договора недействительным. При этом ВАС РФ сослался на то, что "согласно законодательству Северной Ирландии к судебному разбирательству об оспаривании

действительности сделок в качестве его сторон должны по общему правилу привлекаться стороны таких сделок и, соответственно, надлежащим образом уведомляться о производстве. При этом у суда нет обязанности привлекать к участию в деле в качестве третьих лиц последующих цессионариев (новых кредиторов) и извещать их о ведущемся судебном разбирательстве". Поскольку такие третьи лица не принимали участия в судебном разбирательстве, но полагают свои права и интересы затронутыми, имеется возможность подать самостоятельный иск об оспаривании заключенных ими сделок и обжаловать принятый судебный акт, поскольку "факт принятия иностранным судом решения, затрагивающего права третьих лиц, не может являться основанием для применения оговорки о публичном порядке и отказа на этом основании в признании решения иностранного суда на территории Российской Федерации" <2>. Данный подход открывает достаточно широкие возможности для совершения сторонами первоначального договора злоупотреблений в отношении правопреемников по такому договору (в качестве которых нередко выступают кредиторы таких лиц в результате реструктуризации задолженности), признавая недействительным первоначальный договор в иных юрисдикциях и тем самым фактически лишая правопреемников их имущества без привлечения их в процесс. В рассматриваемом деле содержится и немало иных спорных обстоятельств (обоснование юрисдикции ирландского суда в отношении российских лиц в отсутствие пророгационного соглашения, применение ирландским судом своего национального права к договору между российскими лицами, исполнение которого тесно связано с территорией РФ, и пр.), но они выходят за рамки исследуемого вопроса. Интересующемуся читателю можно порекомендовать ознакомиться с записью заседания Суда по данному делу <3>.

<1> **Постановление** ВАС РФ от 23 октября 2012 г. N 7805/12. В данном споре ВАС РФ указал, что признание кипрским судом недействительным договора купли-продажи доли в уставном капитале, покупателем по которому выступала российская компания, не заключавшая пророгационного соглашения о выборе суда данного государства в качестве компетентного и не дававшая добровольного согласия на участие в судебном разбирательстве в указанном суде, является нарушением публичного порядка Российской Федерации. Такое нарушение было усмотрено судом в том, что право на суд, гарантированное **ст. 6** Конвенции о защите прав человека и основных свобод 1950 г., включает в себя право лица участвовать в тех судебных процессах, в рамках которых решаются вопросы о его правах и обязанностях.

<2> **Постановление** Президиума ВАС РФ от 8 октября 2013 г. N 6004/13.

<3>

https://www.youtube.com/watch?v=72mGp0CQ4_U

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.

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>.

<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. N 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.

Кроме того, представлены и более радикальные мнения о необходимости разработки и принятии международной конвенции, которая установила бы зоны национальной юрисдикции в Интернете по аналогии с Арктикой, космическим пространством, Луной и другими небесными телами <1>. По мнению сторонников данного подхода, Интернет фактически является особой информационной зоной мира и сотрудничества, 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 <2>.

<1> 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 Интернета. М., 2007. С. 86.

<2> 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.

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**) (далее - Конвенция). 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 показала 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 их 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**).

^{<1>} Schulz A. The 2005 Hague Convention on Choice of Court Clauses // ILSA Journal of International and Comparative Law. 2006. N 12. P. 433 - 434.

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 февраля 2016 г. данная **Конвенция** была подписана представителями США, Европейского союза, Сингапура и Мексики, однако ратифицирована только последней <1>. Формально **Конвенция** вступила в силу 1 октября 2015 г. <2>.

<1> Текст **Конвенции** на английском языке: http://www.hcch.net/index_en.php?act=conventions.text&cid=98.

<2> 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.

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 <1>.

<1> См.: Faye Fangrei Wang. Internet Jurisdiction and Choice of Law: Legal Practices in the EU, US and China. P. 20.

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, 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 попадали 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. "с" 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 "с" 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-соглашений**).

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>;

<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.

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 ^{<1>}, относящихся к такому суду (например, стороны обозначили в качестве компетентного суда мировой суд, которому возникший спор не подведомственен в принципе);

^{<1>} Следует подчеркнуть, что автономия воли сторон по заключению пророгационных соглашений не может изменить существующие правила процессуального законодательства, касающиеся предметной юрисдикции, т.е. компетентности суда по рассмотрению споров соответствующего вида в принципе. См. [ст. 5 \(3\)](#) Конвенции.

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 положения договорного права об ошибке, о введении в заблуждение, 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

условиях 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 отношение к [Конвенции](#) со стороны других стран, в частности Китая, Индии, Бразилии и других развивающихся стран, вызвано в том числе и этими соображениями <2>.

<1> Конвенция допускает возможность присоединяющегося государства сделать оговорку о неприменении отдельных положений Конвенции к определенным отношениям при наличии на то "серьезного интереса" (ст. 21).

<2> 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.

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 Интернете <1>.

<1> 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**.

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) <1>. Для реализации 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 обеих форм.

<1> Во многом данные подходы были вдохновлены наработками, полученными в области правового регулирования трансграничного банкротства. См.: UNCITRAL Model Law on Cross-Border Insolvency 1997; American Law Institute's Guidelines Applicable to Court-to-Court Communications in Cross-Border Cases 2001.

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 временные 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 судопроизводства 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 быть принудительно исполнены на территории других государств, как противоречащие Принципам <1>.

<1> Intellectual Property: Principles Governing Jurisdiction, Choice of Law, and Judgments in Transnational Disputes. ALI. 2007. § 403 (2) (c) & (d).

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 исключительного 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 временные 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.

<1> См.: Бабкин С.А. Право, применимое к отношениям, возникающим при использовании сети Интернет: основные проблемы. С. 45.

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 Интернете, 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 Интернета, 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 регулировать такие отношения <1>. Трансграничный и общедоступный характер Интернета 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.

<1> Емкий и краткий анализ на русском языке данного подхода см.: Бабкин С.А. Интеллектуальная собственность в сети Интернет. С. 231 и сл.

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 плавание" абсолютного саморегулирования <1>. 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.

<1> 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.

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 Интернета, но в остальном это все те же "минимальные

контакты", "место исполнения договора", "место совершения правонарушения или наступления его вредоносных последствий".

Критерий направленности осуществляемой в Интернете 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.

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.

Что же касается российского права, то с момента первого издания данной книги произошел ряд изменений, касающихся каждого из трех видов юрисдикции.

В части судебной юрисдикции (**jurisdiction to adjudicate**) можно упомянуть следующие изменения.

Во-первых, конкретизирована юрисдикция судов общей юрисдикции в отношении потребительских отношений с участием иностранных интернет-компаний

за счет добавления возможности предъявления физическим лицом иска к такой компании, если будет установлен факт распространения ею интернет-рекламы, направленной на российского потребителя. (ч. 7 ст. 29 и п. 2 ч. 3 ст. 402 ГПК РФ).

Во-вторых, установлена исключительная юрисдикция Мосгорсуда по рассмотрению в качестве суда первой инстанции споров, связанных с защитой исключительного права на объекты авторских и (или) смежных прав (кроме фотографических произведений), при условии предварительного принятия обеспечительных мер в виде ограничения доступа к соответствующему интернет-ресурсу (ст. 144.1 ГПК РФ).

В части определения права, применимого к соответствующим отношениям (**jurisdiction to prescribe**), произошел ряд изменений, касающихся преимущественно публичного права.

Критерий направленности деятельности как условие установления юрисдикции российского суда или выбора применимого права, изначально применявшийся в российском праве в весьма фрагментарной форме, все чаще используется в российском законодательстве. Помимо положений ст. 1212 ГК РФ он с 2015 г. нашел свое отражение в Законе об информации применительно к определению сферы действия специального регулирования деятельности поисковых сервисов, посвященному "праву быть забытым" (ст. 10.3), а также в разъяснениях Минкомсвязи России по вопросам определения сферы деятельности законодательства о персональных данных.

Что касается юрисдикции, связанной с

обеспечением исполнения судебных решений (**jurisdiction to enforce**), здесь также произошел ряд изменений, ключевым из которых является расширительное толкование судами понятия "международный договор" для целей принятия решения о признании и принудительном исполнении иностранного судебного решения за счет отнесения к таковым практически любых международных соглашений, в которых имеется хотя бы намек на осуществление сотрудничества между Россией и государством, где было вынесено решение, по вопросам, имеющим отношение к проблематике судебного решения.

Еще одним трендом стало все расширение сферы применения механизма блокировки интернет-ресурса, обеспечивающего, по сути, возможность исполнения решений российских правоприменительных органов без необходимости обращения к иностранным органам власти. Такого рода механизм обеспечивает определенный уровень самодостаточности указанных решений и способствует их реализации "своими силами", повышая тем самым информационный суверенитет государства. Безусловно, существует большое количество способов обхода такого рода блокировок, однако, даже несмотря на это, они обеспечивают минимальную техническую исполнимость вынесенных решений в отношении той категории пользователей, которые не применяют специальные средства обхода блокировок.

§ 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 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 обуславливает 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>.

Закключаемые в Интернете 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>.

<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: Ocean 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

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 правовых порядках лишь на основании того факта, что веб-сайт был доступен на их территории.

В завершение необходимо отметить, что в свете происходящих в российском законодательстве и правоприменительной практике изменений, направленных на ужесточение контроля над российским сегментом сети Интернет, при выборе доменного имени и хостингового провайдера для интернет-сервиса или интернет-магазина целесообразно анализировать потенциальные риски, связанные с его возможным подпаданием под российскую юрисдикцию. Как отмечалось ранее, регистрация интернет-ресурса в доменной зоне ".ru" (".рф", ".su" и т.д.) может рассматриваться в качестве обстоятельства, свидетельствующего о наличии направленной деятельности на территорию России, что влечет: 1) возможность предъявления иска к его владельцу в российском арбитражном суде по спорам, связанным с использованием средств индивидуализации в доменном имени, а в некоторых случаях - также по иным спорам по причине тесной связи с территорией России; 2) распространение на такой ресурс российского законодательства о персональных данных и о рекламе;

3) возможность распространения на В2С отношения российского законодательства о защите прав потребителей законодательства (ст. 1212 ГК РФ). Кроме того, не исключено, что доменные имена, контролируемые Координационным центром национального домена сети Интернет, могут впоследствии быть делегированы без решения суда. Появились сообщения о том, что региональная общественная организация "Центр интернет-технологий" (РОЦИТ), занимающаяся защитой прав пользователей российского сегмента Сети, договорилась о совместном противодействии мошенникам с Координационным центром национального домена сети Интернет (КЦ), в частности, о таком, которое позволит КЦ делегировать домены мошеннических интернет-магазинов по жалобе РОЦИТ <1>. Безусловно, все это увеличивает риски, связанные с существованием интернет-ресурса в российском сегменте сети Интернет, и обуславливает целесообразность внимательного подхода к выбору доменного имени.

<1> <http://izvestia.ru/news/602824>

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 (ст. 433 ГК РФ). 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>.

<1> Smith S. Contract Theory. Oxford, 2004. P. 169.

Таким образом, для признания договора заключенным необходимо установить наличие оферты, акцепта, а также соблюсти требования, предъявляемые 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, сделавшего 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>.

КонсультантПлюс: примечание.

Монография М.И. Брагинского, В.В. Витрянского "Договорное право. Общие положения" (Книга 1) включена в информационный банк согласно публикации - Статут, 2001 (3-е издание, стереотипное).

<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.

Указанные требования взаимосвязаны и, по сути, обеспечивают друг друга. Как отмечал Л. Эннексерус, оферта должна быть настолько определенной, 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 определенного лица, но и определенного <1>. 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 <2>.

<1> 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. N 09АП-8366/2012-ГК по делу N А40-131749/11-55-237). Однако, как показано далее, такой подход является неверным, поскольку не учитывает возможности существования публичной оферты.

<2> Брагинский М.И., Витрянский В.В. **Договорное право. Общие положения**. С. 198.

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.

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, витрине и т.п.), демонстрации их образцов или предоставления 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 виртуальную 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 ознакомления покупателя с товаром либо образцом товара при заключении такого договора" <1>.

<1> См.: п. 2 Постановления Правительства РФ от 27 сентября 2007 г. N 612 "Об утверждении Правил продажи товаров дистанционным способом".

Как следует из данной дефиниции, не всякая продажа товара, осуществляемая с использованием Интернета, 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 ими, подобрал товар и продал его покупателю, такой договор не подпадает под понятие дистанционного способа продажи, даже если коммуникации происходили с использованием Интернета, 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 <1>. По мнению некоторых российских судов, 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 <2>. Однако с данным подходом сложно согласиться. Несмотря на то что у покупателя была возможность заранее посмотреть товар "вживую", нет никаких гарантий, что ему доставят именно то, на что он смотрел, в случае заказа данного товара через

интернет-магазин. В равной степени нет никаких гарантий того, что потребителю была предоставлена объективная информация о товаре, под влиянием которой он впоследствии разместил заказ в интернет-магазине. При таких обстоятельствах специальные гарантии, которые предоставляются при дистанционном приобретении товара, приобретают весьма актуальный характер. С формально-юридической точки зрения, поскольку процесс заключения договора происходил не в момент ознакомления с товаром на территории предпринимателя, а в момент размещения заказа на веб-сайте магазина, в указанный момент у покупателя отсутствовала возможность непосредственного ознакомления с товаром, а значит, такой договор может быть отнесен к разряду договоров дистанционной купли-продажи товара. Примечательно, что в [Директиве ЕС "О правах потребителей" 2011 г.](#) данная ситуация прямо обозначена в качестве разновидности договора, заключенного дистанционным способом <3>.

<1> См.: [Постановление](#) Президиума Верховного суда Удмуртской Республики от 21 мая 2010 г., в котором говорится: "...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".

<2> См., например: Апелляционное [определение](#) Московского городского суда от 12 апреля 2012 г. по делу N 11-4108, где сказано: "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".

<3> "Дефиниция договора, заключенного дистанционным способом, охватывает ситуации, при которых потребитель совершает визит в помещения предпринимателя для целей сбора информации о товарах (услугах) и впоследствии заключает договор дистанционным способом" (см. [п. 20 преамбулы](#) Директивы от 25 октября 2011 г. 2011/83/EU "О правах потребителей").

Если же потребитель сделал на сайте интернет-магазина лишь предварительный заказ, а впоследствии оплатил и забрал его в пункте самовывоза, то говорить о заключении договора купли-продажи дистанционным способом также нельзя, поскольку потребитель в таком случае имел возможность непосредственно ознакомиться с товаром в момент его приобретения и принять соответствующее решение по результатам такого ознакомления <1>.

<1> [Определение](#) Красноярского краевого суда от 15 января 2016 г. по делу N 4Г-3130/2015.

Возвращаясь к терминологии российского законодательства, необходимо отметить еще один важный момент. Следует отличать продажу товара

дистанционным способом от продажи товара по образцам. По ранее действовавшему законодательству определить, являлась ли продажа товара посредством Интернета продажей 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.

<1> См.: [п. 2 Постановления Правительства РФ](#)

от 21 июля 1997 г. N 918 "Об утверждении Правил продажи товаров по образцам".

Указанная неопределенность была устранена путем внесения изменений в соответствующие [Правила](#) <1>. 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) <2>.

<1> [Постановление](#) Правительства РФ от 4 октября 2012 г. N 1007 "О внесении изменений в некоторые акты Правительства Российской Федерации по вопросам продажи товаров и оказания услуг".

<2> См., например, понятие розничной торговли в [ст. 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 товаров дистанционным способом: "Предложение товара в его описании, обращенное к неопределенному кругу лиц, признается публичной офертой, если оно достаточно определено 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, 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).

Из указанных положений можно сделать следующий вывод: любое предложение товара в интернет-магазине, содержащее наименование товара и стоимость за единицу, может быть квалифицировано как публичная оферта, 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>. Судебная практика в целом разделяет данный подход <2>. Как отмечено в решении одного из судов, "по своему юридическому значению размещенная на веб-сайте информация о товаре, предназначенная для пользователей Интернета, представляет собой оферту, так как является адресованным одному или нескольким конкретным лицам предложением, которое достаточно определено и выражает намерение лица, сделавшего предложение,

считать себя заключившим договор с адресатом, которым будет принято предложение ([пункт 1 статьи 435 ГК РФ](#))... Оферта считается полученной адресатом, когда посетитель интернет-магазина загрузил на своем компьютере соответствующую страницу" <3>.

<1> См.: [преамбула](#) к российскому Закону о защите прав потребителей; [п. 1 ст. 1212 ГК РФ](#).

<2> См., например: [п. 10](#) "Обзора судебной практики по гражданским делам президиума Нижегородского областного суда за II полугодие 2013 года"; Апелляционное [определение](#) Архангельского областного суда от 8 июля 2013 г. по делу N 33-3981/13.

<3> Решение Промышленного районного суда г. Смоленска от 30 апреля 2015 г. по делу N 2-2013/2015.

В связи с этим возникает вопрос: имеют ли какое-либо правовое значение оговорки, сделанные на сайте, о том, что предложение товара не является публичной офертой? Сразу следует сделать оговорку, что вышеуказанные положения [ст. 494 ГК РФ](#) и правил дистанционной продажи товара касаются лишь случаев продажи **товара** (т.е. физических объектов) посредством сети Интернет. Они не распространяются на случаи реализации через интернет-сайты услуг (например, гостиничных услуг, услуг в сфере перевозок пассажиров и др.) или цифрового контента. В отношении порядка заключения договоров о продаже таких объектов действуют общие правила об оферте и акцепте, соответственно, у оговорок об ознакомительном характере информации на таком сайте и об отсутствии у нее статуса публичной оферты

гораздо больше шансов на "выживание".

С одной стороны, подобная оговорка свидетельствует о том, что в сделанном предложении отсутствует воля лица считать себя связанным акцептом другой стороны, т.е. отсутствует один из существенных элементов оферты. Это дает основание для вывода некоторых судов о том, что размещенная информация является лишь предложением делать оферты <1>.

<1> Решение Димитровградского городского суда Ульяновской области от 24 июня 2014 г. по делу N 2-1525/2014 гласит: "В силу прямого указания о том, что размещенная информация об ассортименте товара не является публичной офертой, сообщение сведений об ассортименте товара является предложением делать оферты. Поскольку ответчик не подтвердил принятие заявки по цене, указанной в заказах, договор купли-продажи не может считаться заключенным". См. также [Постановление](#) Восьмого арбитражного апелляционного суда от 21 апреля 2015 г. по делу N А46-14294/2014, в котором говорится: "Кроме того, указано, что данный интернет-сайт носит исключительно информационный характер и ни при каких условиях не является публичной офертой. Учитывая изложенное, суд апелляционной инстанции соглашается с выводами арбитражного суда о наличии у общества законных оснований для выставления цены за предложенный товар индивидуально каждому клиенту".

С другой стороны, положения [ст. 494](#) ГК РФ и [п. 12](#) Правил продажи товаров дистанционным способом могут рассматриваться в качестве специальных правил,

носящих императивный характер по причине необходимости защиты слабой стороны. Соответственно, одного только наличия существенных условий договора на сайте интернет-магазина достаточно, чтобы признать размещенную информацию офертой. Признак определенности оферты в данном случае более важен, нежели волевой, поэтому оговорки об отсутствии у размещенной информации статуса оферты не имеют юридической силы как противоречащие императивным нормам [ст. 494](#) ГК РФ. Некоторые суды придерживаются этой логики. Как отмечено в одном из судебных решений, "довод ответчика о том, что размещенная на его интернет-сайте www.220-volt.ru информация не является публичной офертой, и поэтому приложенная истцом распечатка подтверждения заказа говорит только о том, что он принят в обработку, является неверным, поскольку самим же ответчиком на своем сайте указано, что размещенные на сайте цены товаров действуют только при оформлении заказа через интернет-магазин www.220-volt.ru" <1>. В другом деле суд не принял ссылку ответчика на то, что размещение на сайте предзаказа на товар, которого нет, является, как указано в пользовательском соглашении, условной сделкой в соответствии со [ст. 157](#) ГК РФ, а следовательно, не порождает прав и обязанностей сторон до поступления товара на склад продавца. Суд счел, что размещенная на сайте информация о товаре достаточна для ее квалификации в качестве оферты, которая была акцептована потребителем посредством размещения заказа <2>. Хотя в данном споре и не фигурировала оговорка об отсутствии у информации на сайте статуса публичной оферты, суть та же: суд не принял во внимание иные сделанные продавцом оговорки, преследующие аналогичную цель - сохранение за собой контроля над моментом заключения договора.

<1> Решение Новодвинского городского суда
Архангельской области от 7 августа 2015 г. по делу N
2-673/2015.

<2> Решение Промышленного районного суда г.
Смоленска от 30 апреля 2015 г. по делу N 2-2013/2015.

Таким образом, четкого ответа на вопрос о юридическом статусе указанных оговорок нет. Если посмотреть на политико-правовую подоплеку данного вопроса, то вырисовывается следующая картина. Практически все судебные споры, где фигурировал вопрос о том, является ли размещенная на сайте интернет-магазина информация офертой и когда именно договор был заключен, связаны с произошедшим в период между размещением заказа и моментом исполнения договора изменением цены товара, которая возрастала в силу различных факторов, в том числе колебаний курса рубля, и владельцу интернет-магазина становилось невыгодно исполнять договор на условиях с первоначально заявленной ценой. В других случаях, куда более малочисленных, речь шла о допущенных работниками интернет-магазина технических ошибках в описании товара или его цены. Поэтому решение вопроса о правовой природе информации, размещенной на сайте интернет-магазина, и оговорок, о ее справочном характере неразрывно связано с ответом на вопрос: кто должен нести риски изменения рыночной стоимости товара или нести ответственность за действия своих работников? Представляется, что ГК РФ дает ответы на данный вопрос в дефиниции понятия предпринимательской деятельности как деятельности, осуществляемой на свой риск, а также в положении об

ответственности должника за действия своих работников (ст. 402). При таком подходе ссылка на императивный характер специальных положений ст. 494 ГК РФ и правил дистанционной продажи товаров будет выглядеть органично. Но в тех случаях, когда из конкретных обстоятельств дела будут очевидны явная недобросовестность потребителя, злоупотребление им своими правами, есть возможность пресечь его действия, ссылаясь на общие положения об оферте, содержащиеся в ст. ст. 435 и 437 ГК РФ.

Вышеизложенное дает основания для следующих выводов.

1. С чисто прагматической точки зрения интернет-магазину выгодно использовать соответствующие оговорки, поскольку они дают ему в руки дополнительный аргумент и ссылки на них отсекают определенное количество споров с теми потребителями, которые не искушены в нюансах договорного права. К тому же основанные на таких ссылках аргументы могут "устоять" и в суде. Но так или иначе, надо отдавать при этом себе отчет в том, что подобного рода дисклеймеры не являются "пуленепробиваемыми" и могут не спасти в случаях, когда поведение интернет-магазина судья сочтет явно несправедливым.

2. При желании подстраховаться от нежелательного акцепта потребителя продавец может использовать классические конструкции договорного права. Как известно, акцепт должен быть полным и безоговорочным (п. 1 ст. 438 ГК РФ), акцепт, сопровождающийся дополнительными условиями, является встречной офертой (ст. 443 ГК РФ), которая, в свою очередь, подлежит акцепту первоначальным оферентом. Таким образом, даже если информация,

размещенная на сайте интернет-магазина, является публичной офертой, действия покупателя по размещению заказа, при осуществлении которых он определяет какие-либо дополнительные условия (порядок оплаты, метод доставки, требования к упаковке и т.п.), представляют собой встречную оферту, которая подлежит акцепту со стороны интернет-магазина. В таком случае у сотрудников интернет-магазина появляется возможность проверить исполнимость заказа и убедиться в коммерческой целесообразности его выполнения на обозначенных условиях. Примеры подобного анализа отношений, возникающих при размещении заказа в интернет-магазине, уже имеют место в судебной практике <1>.

<1> См., например: Апелляционное [определение](#) Архангельского областного суда от 8 июля 2013 г. по делу N 33-3981/13, в котором говорится: "То обстоятельство, что истец сформировал заказ с условием доставки курьером и оплатой товара наличными курьеру, не свидетельствует о заключении между сторонами договора купли-продажи на указанных условиях. Так, в силу [ст. 443](#) ГК РФ ответ о согласии заключить договор на иных условиях, чем предложено в оферте, не является акцептом. Такой ответ признается отказом от акцепта и в то же время новой офертой".

3. Правила дистанционной продажи товаров ([п. 13](#)) прямо допускают возможность определить срок действия оферты. Таким образом, можно определять срок, в течение которого информация о товаре, размещенная на интернет-сайте, является актуальной. При этом необходимо учитывать положения [ст. 190](#) ГК

РФ, устанавливающей допустимые виды сроков: указание календарной даты, периода времени или события, которое должно неизбежно наступить. Так, например, указание на то, что соответствующая цена действительна в течение новогодних праздников, является допустимым ограничением срока действия оферты. А указание на то, что оферта действует, "пока товар есть в наличии", формально не отвечает требованиям [ГК РФ](#) о сроке, так как отсутствие товара по причине его полной продажи не обладает качеством неизбежного события: часть товара может остаться нераспроданной.

Нормы, аналогичные положениям российского законодательства, дающие основания для квалификации предложения о продаже товара на веб-сайте в качестве публичной оферты, хотя и встречаются в иных странах ^{<1>}, но все же воспринимаются не всеми правопорядками.

^{<1>} 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.

Отдельные положения [Директивы ЕС N 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 окончательно 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 считается заключенным в момент, когда покупатель кладет товар в корзину, что повлекло бы ряд неудобств для него самого. Он не сможет поставить товар на полку обратно и выбрать другой, не оплатив первый, поскольку договор в отношении его 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 нередко 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 ф. ст. - 98 фунтов вместо 600 <4>.

<1> Reed C., Angel J. Computer Law: The Law an Regulation of Information Technology. Oxford University Press. 2007. P. 106.

<2> [1953] 1 QB 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/guardian-weeklytechnologysection2>.

Соображения в пользу нецелесообразности признания информации, размещенной на веб-сайте интернет-магазина, в качестве оферты высказываются и в немецкой доктрине <1>, поскольку немецкое право, так же как и английское, не рассматривает выставление товара на витрине и в магазинах самообслуживания в качестве оферты <2>.

<1> Law of E-Commerce in Poland and Germany / Ed. B. Heiderhodd. Sellier. Munchen, 2005. P. 34.

<2> BGH. 16.01.1980. NJW 1980, 1388. Markesinis B. The German Law of Contract. Oxford and Portland.

Таким образом, российский подход отличается определенной жесткостью по отношению к интернет-магазинам, что может быть в определенной степени оправдано частыми проявлениями недобросовестности с их стороны, например, 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 интернета 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 тех благ, о которых говорится в оферте <2>. 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.

<1> [Пункт 58](#) Постановления Пленума Верховного Суда РФ N 6, Пленума ВАС РФ N 8 от 1 июля 1996 г. "О некоторых вопросах, связанных с применением части первой Гражданского кодекса Российской Федерации".

<2> См.: [п. 2](#) информационного письма

Президиума ВАС РФ от 5 мая 1997 г. N 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.

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 Интернете. 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 именно 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 "сообщение о намерении покупателя приобрести товар" и специального правового регулирования в отношении его 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 сообщение 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 <2>; оплату товара с отсутствием возражений со стороны продавца против действий покупателя <3>; размещение заказа на веб-сайте с присвоением ему определенного номера <4>.

<1> [Решение](#) Верховного Суда РФ от 4 октября 2011 г. N 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. N 612", оставленное без изменения [Определением](#) Верховного Суда РФ от 8 декабря 2011 г. N КАС11-675.

<2> См., например: [п. 43](#) Постановления Пленума ВС РФ от 22 июня 2012 г. N 17 "О рассмотрении судами гражданских дел по спорам о защите прав потребителей"; Кассационное [определение](#) Саратовского областного суда от 19 апреля 2011 г. по делу N 33-2062.

<3> Апелляционное [определение](#) Московского городского суда от 22 октября 2012 г. по делу N 11-23085/12 гласит: "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".

<4> В [Постановлении](#) Девятнадцатого

арбитражного апелляционного суда от 15 февраля 2013 г. по делу N А36-6311/2012 говорится: "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 24500 руб. Сообщение о намерении приобрести вышеуказанный товар (заказ), поступившее от потребителя, было принято заявителем, и ему был присвоен номер W0022-03270. 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".

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) <1>.

КонсультантПлюс: примечание.

Учебник "Российское гражданское право: В 2 т." (отв. ред. Е.А. Суханов) включен в информационный банк согласно публикации - Статут, 2011 (2-е издание, стереотипное).

<1> Гражданское право: Учебник: В 4 т. / Под ред. Е.А. Суханова. М., 2005. Т. I: Общая часть; 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). Никакой иной формы договора (например, электронной) гражданское законодательство РФ не предусматривает.

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 Интернета 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.

КонсультантПлюс: примечание.

Учебник "Российское гражданское право: В 2 т." (отв. ред. Е.А. Суханов) включен в информационный банк согласно публикации - Статут, 2011 (2-е издание, стереотипное).

<1> Гражданское право: Учебник: В 4 т. / Под ред. Е.А. Суханова. Т. I: Общая часть. С. 462.

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: он может быть написан от руки, напечатан на компьютере или воспроизведен иным способом. Схожим образом понимается письменная (текстовая) форма в европейском праве. В соответствии с **DCFR** текстовая форма означает информацию, изложенную с помощью букв алфавита или иных понятных знаков при помощи средств, обеспечивающих возможность ее прочтения, записи и последующего воспроизведения в материализованной форме (ст. I-1:106 (2) **DCFR**) <1>.

<1> Текст **DCFR** на русском языке см.: **Модельные правила европейского частного права** / Пер. с англ.; науч. ред. Н.Ю. Рассказова. М.: Статут, 2013. С. 109.

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 могут предусмотреть необходимость совершения сделки в квалифицированной письменной форме - нотариальной.

Долгое время законодательство о нотариате не предусматривало специальных положений, регламентирующих порядок совершения нотариальных действий в отношении электронных документов. В связи с этим считалось, что "через Интернет невозможно совершить сделки, требующие нотариального удостоверения, поскольку удостоверительная надпись может быть совершена только на "бумажном" документе" <1>. Однако с 1 июня 2014 г., после вступления в силу поправок в **Основы законодательства Российской Федерации о нотариате** от 11 февраля 1993 г. N 4462-1 (далее - Основы законодательства о нотариате), ситуация изменилась <2>. Появилась возможность совершать не только нотариальные действия на основе электронных документов, но и иные нотариальные действия: "удостоверение равнозначности электронного документа документу на материальном носителе" (ст. 103.8), "удостоверение равнозначности документа на бумажном носителе электронному документу" (103.9). Кроме того, у

нотариуса появилась возможность выступать посредником в передаче электронных документов от одних физических и юридических лиц другим лицам (ст. 86). Для совершения указанных действий нотариус использует усиленную квалифицированную электронную подпись (ст. 11). Однако, несмотря на все эти нововведения, сфера их применения достаточно ограничена: нотариус либо сам создает электронные документы на базе предъявленных ему документов на бумажных носителях, либо совершает действия с электронными документами, **подписанными квалифицированной электронной подписью**, которая в электронной коммерции используется крайне редко. Поэтому рассчитывать на то, что нотариусы станут драйверами развития электронного документооборота в сфере электронной коммерции, вряд ли стоит, но и забывать про них тоже не надо.

<1> Калятин В.О. Право в сфере Интернета. С. 329. На это указывает, в частности, толкование ст. 45 Основ законодательства о нотариате, устанавливающей требования к документам, предъявляемым для совершения нотариальных действий. Например, такое: "В документе, объем которого превышает один лист, листы должны быть прошиты, пронумерованы и скреплены печатью".

<2> Федеральный закон от 21 декабря 2013 г. N 379-ФЗ "О внесении изменений в отдельные законодательные акты Российской Федерации".

Таким образом, принимая во внимание экзотический характер устной формы при заключении договоров посредством Интернета, а также

ограничения, которые сопровождают квалифицированную (нотариальную) письменную форму, основной формой договора в сфере электронной коммерции остается простая письменная форма. При этом, разумеется, 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 общепризнанным 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 <1>. Иными словами, договор не перестает быть договором лишь на том основании, что он заключен при помощи компьютера.

<1> [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 N

2000/31/ЕС "Об электронной коммерции" и др.

В российском законодательстве, к сожалению, отсутствуют положения, аналогичные вышеизложенным <1>.

<1> Но могут появиться в случае ратификации Конвенции ООН об использовании электронных сообщений в международных сделках 2005 г., которая была подписана Россией 25 апреля 2007 г. Закрепленный же в настоящее время в п. 3 ст. 4 Федерального закона от 6 апреля 2011 г. N 63-ФЗ "Об электронной подписи" принцип недопустимости 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, говорит несколько об ином: о недопустимости дискриминации различных технологий создания электронных подписей, а не о недискриминации электронных и бумажных документов в целом.

При этом в отечественной правоприменительной практике и доктрине электронная форма предоставления информации в течение долгого времени рассматривалась, да и сейчас 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 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 до 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 на то 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 об условиях действительности договоров, заключаемых в электронной среде сети Интернет, является наиболее значимым вопросом электронной коммерции, которая имеет в своем основании именно договорные отношения. Во многом этот вопрос зависит от развенчания мифов о наличии в договорах, заключаемых посредством Интернета и не скрепляемых усиленной квалифицированной подписью,

пороков формы.

<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. Так, в [Определении](#) Воронежского областного суда от 4 марта 2010 г. по делу N 33-1144/10 сказано, что "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".

Общее регулирование письменной формы договора содержится в положениях [ст. ст. 160](#) и [434](#) ГК РФ.

Согласно [п. 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 либо иного аналога собственноручной подписи допускается в случаях и в порядке, которые предусмотрены законом, иными актами или соглашением сторон".

Статья 434 ГК РФ конкретизирует способы заключения договора в письменной форме: 1) путем составления одного документа, подписанного сторонами; 2) 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; 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. В связи с этим возникает вопрос: является ли по российскому праву наличие подписи необходимым элементом письменной формы договора?

<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.-практ. **комментарий** (постатейный) / Под ред. А.П. Сергеева. М., 2010 (п. 4 комментария к ст. 420).

Вопрос о необходимости наличия подписи как

обязательного условия признания договора заключенным в письменной форме решается в зависимости от того, какой из трех указанных в [ст. 434](#) ГК РФ способов заключения договора был использован. Так, в соответствии с [п. 2 данной статьи](#) подпись является необходимой в случае составления договора в качестве единого документа. Однако для электронной коммерции данная форма заключения договора не является типичной, так как она предполагает наличие сторон договора в одном месте и в одно время, для того чтобы они смогли проставить свои подписи **в одном и том же** документе. В случае же, когда договор заключается в Интернете, стороны находятся в разных местах и подписывают документ в разное время. Причем документы, в которых проставляется подпись, в таком случае не являются тождественными с технической точки зрения, поскольку при передаче по Интернету, а также в ходе процессов, происходящих на программном уровне компьютера стороны по договору, они представляют собой лишь копии исходного документа (пусть в некоторых случаях и на 100% достоверные). В описанной ситуации более корректно говорить об обмене документами ([п. 2 ст. 434](#) ГК РФ).

В случае заключения договора посредством обмена документами закон устанавливает дополнительное условие соблюдения письменной формы договора - наличие возможности установить, что документ исходит от стороны по договору. Данная возможность будет иметь место в случае, когда соответствующая сторона проставила подпись, юридическая сила которой признается законодательством. Это следует из положений [ч. 4 ст. 11](#) Закона об информации, связывающих 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".

Что же касается третьего способа заключения договора, то здесь закон ничего не говорит о необходимости наличия подписи. Ее отсутствие восполняется совершением конклюдентных действий, т.е. поведением стороны, которое свидетельствует о наличии воли на заключение договора. Условия самого договора при этом изложены в письменной оферте. Поскольку оферта не является сама по себе сделкой, так как не влечет юридических последствий в виде возникновения договорных прав и обязанностей в отсутствие акцепта ^{<1>}, то на нее не распространяются требования [ст. 160](#) ГК РФ о необходимости ее подписания собственноручной подписью или ее аналогом. К тому же информация о товаре (услуге) в интернет-магазине в ряде случаев признается законом и судебной практикой публичной офертой (см. далее) и в отсутствие каких-либо подписей.

^{<1>} См.: Брагинский М.И., Витрянский В.В. Договорное право: Общие положения. М., 1997.

Таким образом, систематическое толкование положений [ГК](#) РФ позволяет сделать вывод, что письменная форма договора будет иметь место при

выполнении двух условий:

1) договор составлен в виде документа или документов, отражающих содержание договоренностей сторон;

2) при заключении договора в форме единого документа (п. 1 ст. 434 ГК РФ) или посредством обмена документами (п. 2 ст. 434 ГК РФ) согласие сторон с условиями договора подтверждается подписанием их собственноручной подписью либо ее аналогом, а при заключении договора посредством акцепта письменной оферты конклюдентными действиями (п. 3 ст. 434 ГК РФ) согласие выражается соответствующим поведением другой стороны.

Рассмотрим теперь способы заключения договора, предусмотренные в п. п. 2 и 3 ст. 434 ГК РФ, подробнее.

3.1. Заключение договора посредством обмена электронными документами (п. 2 ст. 434 ГК РФ)

В соответствии с новой редакцией данного пункта, вступившей в силу с 1 июня 2015 г., допускается заключение договора "путем составления одного документа, подписанного сторонами, а также 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". Внесенные в данный пункт изменения исправили ранее действовавшую не очень удачную формулировку, согласно которой функция удостоверения факта принадлежности сообщения определенному лицу возлагалась не на само содержание документа, а на

используемое средство связи, что несколько противоречило здравому смыслу и сложившейся практике <1>.

<1> Согласно ранее действовавшей формулировке [п. 2 ст. 434](#) ГК РФ "договор в письменной форме может быть заключен путем составления одного документа, подписанного сторонами, а также путем обмена документами посредством почтовой, телеграфной, телетайпной, телефонной, электронной или иной **связи, позволяющей достоверно установить, что документ исходит от стороны по договору** (выделено мной. - **А.С.**)". О проблемах, связанных с толкованием данного положения, см.: Савельев А.И. [Электронная коммерция в России](#) и за рубежом: правовое регулирование. М.: Статут, 2014.

Новая редакция [п. 2 ст. 434](#) ГК РФ также ввела в гражданское законодательство понятие "электронный документ", под которым понимается "информация, подготовленная, отправленная, полученная или хранящая с помощью электронных, магнитных, оптических или аналогичных средств, включая электронный обмен данными и электронную почту". Данное понятие несколько отличается от содержащегося в [Законе](#) об информации, в котором под электронным документом понимается "документированная информация, представленная в электронной форме, то есть в виде, пригодном для восприятия человеком с использованием электронных вычислительных машин, а также для передачи по информационно-телекоммуникационным сетям или обработки в информационных системах". В понятие, используемое в [ГК](#) РФ, не включается необходимость наличия в документе определенных реквизитов в

качестве конститутивного признака электронного документа, в отличие от понятия, содержащегося в [Законе](#) об информации, в котором прямо указывается на "документированный" <1> характер информации, воплощенной в электронном документе. Представляется, что подход [ГК РФ](#) в большей степени соответствует международным нормам. В частности, с 1 августа 2014 г. для Российской Федерации вступила в силу [Конвенция](#) ООН об использовании электронных сообщений в международных договорах (Нью-Йорк, 2005 г.), которая применяется к договорам гражданско-правового характера с участием иностранных граждан или иностранных юридических лиц, а также осложненным иностранным элементом в случаях, когда стороны такого договора договорились о ее применении. Данная [Конвенция](#) содержит иное понятие электронного сообщения. В соответствии с [п. "б" ст. 4](#) Конвенции электронное сообщение означает "любое сообщение, которое стороны передают с помощью сообщений данных". При этом под сообщением данных [Конвенция](#), вслед за Типовым [законом](#) ЮНСИТРАЛ об электронной торговле 1996 г., понимает информацию, подготовленную, отправленную, полученную или хранимую с помощью электронных, магнитных, оптических или аналогичных средств, включая электронный обмен данными, электронную почту, телеграмму, телекс или телефакс, но не ограничиваясь ими.

<1> В соответствии с [п. 11 ст. 2](#) Закона об информации "документированная информация - зафиксированная на материальном носителе путем документирования информация с реквизитами, позволяющими определить такую информацию или в установленных законодательством Российской

Федерации случаях ее материальный носитель".

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 Интернете 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 Интернете некоей особой формы договора под названием "конклюдентно-письменная" <3>: во-первых, **ГК** РФ знает только устную и письменную формы договора, а во-вторых, не очень понятно, чего именно "письменного" содержится в электрических сигналах и электромагнитных импульсах.

<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. Правовые аспекты торговли в сети Интернет // Право и государство: Теория и практика. 2012. N 10/94.

<3> Там же.

Обмен электронными документами как способ заключения договора предполагает определенную степень индивидуализации 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, в ходе которой были согласованы

существенные условия договора, 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 связаны 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.

<1> См.: ст. 11 (3) Директивы N 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. ст. 1369-2, 1369-3 ФГК; ст. II-3:201. См. подробнее: Draft Common Frame of Reference (DCFR), Full Edition. Vol. 1 / Ed. by Christian von Bar and Eric Clive. Sellier. 2009. P. 241 ff.

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.

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 физическом мире, а в ряде случаев и не будут их иметь (если договор не только заключается, но и исполняется в Интернете), вопрос о доверии к личности контрагента выходит на первый план. Данные, получаемые от контрагента посредством Интернета, по общему правилу не несут существенных идентификационных характеристик. IP-адрес, с которого была осуществлена коммуникация, идентифицирует лишь окончное 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.

<1> В Рунете данный сервис реализован, в частности, здесь: <http://www.ripn.net/nic/whois/index.html>.

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 обуславливает возможность проведения почерковедческой экспертизы для решения вопроса о ее подлинности <1>. В условиях электронного обмена данными подлинник сообщения неотличим от копии, не имеет собственноручной подписи и не является бумажным документом. Действия, совершаемые в Интернете, 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 точками и не становится частью самой транзакции, совершаемой в Интернете <2>.

<1> 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.

<2> Lessig Lawrence. Code: Version 2.0. Basic Books. 2006. P. 35.

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 Интернете 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 Интернета, будут 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, 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 сослаться 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 большая часть сделок в сфере электронной коммерции, заключаемых посредством обмена документами, являются действительными. Сомнения в соответствии их письменной формы эффективно устраняются 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>.

<1> Зак А.Ю. **Нарушения прав потребителей** при ненадлежащем исполнении договора дистанционной продажи в Интернете и способы их преодоления // Современное право. 2010. N 8.

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 веб-сайта (**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.

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 имелись 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. Эта 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>.

<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).

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 <1>. Впоследствии действительность **click-wrap**-соглашений уже воспринималась американскими судами как данность <2>.

<1> N C-98 JW PVT ENE, C98-20064JV (N.D. Cal Apr, 1998).

<2> См., например: Caspi v. Microsoft Network, L.L.C 732 A.2d 528, 529 (N.J. Super. Ct. App. Div., 1999).

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

<1>.

<1> 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, о праве провайдера услуг на одностороннее изменение условий соглашений без уведомления пользователя и некоторые другие.

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 N 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.

Договор, заключенный посредством щелчка мышью (**click-wrap**), признается действительным в Англии <1>, Италии <2>, Франции <3>, Германии <4>, Канаде <5> и ряде других стран.

<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 N 206/2001 R.G.A.C. // <http://www.riceragiuridica.com/sentenze/index.php?num=86>
8. В данном деле было признано действительным соглашение о подсудности, включенное в соглашение, возникающее при размещении заказа на веб-сайте.

<3> См.: [ст. ст. 1369-4, 1369-5](#) ФГК, посвященные процессу заключения договора в электронной форме (введены в действие Ордонансом от 16 июня 2005 г. N 2005-674).

<4> BGN, 07.11.2002. 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.

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) действия 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 <1>. 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 пользователем. Также оно обычно содержит необходимые существенные условия соответствующего договора либо непосредственно, либо инкорпорируя их путем отсылки к иным документам.

<1> Дмитрик Н.А. Способы осуществления субъективных гражданских прав и исполнения обязанностей с использованием сети Интернет. С. 18.

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.

Следует отметить, что российские суды обычно признают действительность соглашений, заключенных по модели **click-wrap**. Причем это касается как арбитражных судов <1>, так и судов общей юрисдикции <2>. Особенно успешно на положения **click-wrap**-соглашения ссылаются различного рода интернет-платформы, которые выступают посредниками между сторонами договоров, создавая организационные и технические условия для их заключения. Нередко пользователи впоследствии пытаются предъявить требования, вытекающие из неисполнения или ненадлежащего исполнения таких договоров, подобным платформам, которые, в свою очередь, ссылаясь на положения пользовательских соглашений, подчеркивают справочно-информационный характер своих сервисов <3>.

<1> См., например: [Постановление](#) Десятого арбитражного апелляционного суда от 23 сентября 2014 г. по делу N А41-6880/2014. "По условиям регистрации на указанном сайте истец выразил согласие с пользовательским соглашением, присоединившись к нему при регистрации на сайте. Из содержания разд. 2 пользовательского соглашения, размещенного на сайте www.emex.ru и представленного в материалы дела, следует, что администрация сайта не является для пользователя продавцом товаров, не осуществляет доставку товаров пользователю, не принимает возвраты приобретенных пользователем товаров (п. 2.6

пользовательского соглашения)". **Постановление** ФАС Дальневосточного округа от 1 июля 2013 г. по делу N А51-21472/2012 гласит: "Как установлено судами, для размещения заказа на сайте... необходимо ознакомиться с пользовательским соглашением, а также зарегистрироваться в качестве пользователя. При этом из пользовательского соглашения следует, что исполнитель (ответчик) обязуется приобрести для клиента (истца) от своего имени, но за его счет товар, наименование, ассортимент и количество которого должны быть согласованы сторонами при оформлении заказа, а клиент - принять и оплатить заказ в соответствии с условиями данного соглашения; пунктом 5.2.4 исключена ответственность исполнителя за несоответствие доставленного от продавца на склад исполнителя товара тем характеристикам или фотографиям, которые были заявлены (размещены) продавцом на сайте, исполнитель не является продавцом/производителем товаров, а лишь оказывает посреднические услуги между продавцом/производителем товара и покупателем товаров (клиентом), в связи с чем (пункт 6.1.2) клиент заявляет, что он понимает то, что исполнитель является лишь посредником в отношениях между клиентом и продавцом/производителем товаров".

<2> См., например: Определение Октябрьского районного суда г. Кирова от 14 сентября 2012 г. по делу N АП 11-181/12. В нем отмечается: "Между истцом и ООО "е-коммерс груп" было заключено соглашение о предоставлении услуг на сайте www.molotok.ru, предметом которого (п. 1.1) является предоставление ответчиком возможности размещать информацию о намерении продать или купить различные товары или услуги на сайте www.molotok.ru. Согласно п. 3.1 соглашения моментом его заключения считается

момент нажатия пользователем кнопки "Зарегистрироваться", расположенной в конце страницы регистрации сайта www.molotok.ru. Нажатием кнопки пользователи подтверждают свое согласие со всеми условиями соглашения". В решении Ленинского районного суда г. Нижнего Новгорода от 6 ноября 2014 г. по делу N 2-4413/2014 сказано: "Судом установлено, что с истцом был заключен договор публичной оферты в соответствии со [ст. 437](#) ГК РФ. Акцепт оферты, в частности, подтвержден: а) фактом выписанного счета, т.к. получение реквизитов ООО "Ника" для оплаты счета с момента проставления галочки, акцептирующей оферту, невозможно технически, равно как и невозможна выписка без акцепта оферты (стоит запрет через JS-функцию на чекбоксе, который необходимо отметить галочкой после прочтения оферты и согласия с ее условиями в полном объеме)".

<3> [Постановление](#) Десятого арбитражного апелляционного суда от 23 сентября 2014 г. по делу N А41-6880/2014 (платформа [emex.ru](#)); решение Кунцевского районного суда г. Москвы от 27 января 2015 г. по делу N 2-587/2015 (платформа **ЯндексМаркет**); решение Хорошовского районного суда от 14 августа 2013 г. N 2-2853\2013 (платформа **Anyway-anyday**) и др.

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>.

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.

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 оно могло 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. Соответственно, интерфейс интернет-магазина в процессе размещения заказа должен предусматривать возможность перехода на предыдущие стадии (диалоговое окно "Назад"), а выставленные условия соглашения должны сопровождаться возможностью отказа от них (диалоговое окно "Не согласен" или иное

аналогичное).

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. Только такой подход позволяет устранить одну из главных проблем **click-wrap**-соглашения - проблему доказывания факта принятия его условий конкретным клиентом. Если с технической точки зрения оформление заказа невозможно иным образом, чем принятие его условий клиентом, то возникновение спора по поводу исполнения заказа неизбежно подразумевает, что соответствующий клиент принял условия **click-wrap**-соглашения. При этом техническая невозможность принятия заказа в отсутствие согласия клиента с условиями **click-wrap**-соглашения может подтверждаться, в частности, письмами от организации, разрабатывавшей сайт интернет-магазина <1>, либо заключениями эксперта (специалиста).

<1> См., например: [Постановление](#) ФАС Дальневосточного округа от 1 июля 2013 г. по делу N А51-21472/2012, в котором говорится: "Порядок действий по доступу лиц на сайт в целях последующего оказания им услуг составлен разработчиком сайта - ООО "Экспресс Мобайл", что подтверждается письмом последнего от 06.12.2012, направленным на адрес ответчика".

В-четвертых, учитывая, что при формировании заказа, сопровождающегося заключением **click-wrap-**соглашения, используются автоматизированные средства, на стадии заключения 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 N 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. Такие механизмы могут предусматривать возможность редактирования условий заказа на каждом этапе его формирования, а также внедрение специальных страниц подтверждения с вопросом вроде "Данный заказ представлен верно?". 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

американским <2> правом. 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" <3>, что могло бы быть весьма полезным, учитывая, что такие соглашения имеют тенденцию периодически изменяться предпринимателем в одностороннем порядке.

<1> [Статья 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.

<2> 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.

<3> Leff L., Ahmad I. et al. XML for Click-Through Contracts // International Journal of Law and Information Technology. 2008. Vol. 17. N 2.

В Европе недавно было сформулировано еще

одно условие для подобного рода соглашений. В соответствии со [ст. 8 \(2\) Директивы N 2011/83/EU "О правах потребителей"](#) <1> 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" или "Заплатить сейчас" (**pay now**). Положения указанной [Директивы](#) должны были быть имплементированы в национальные законодательства 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> 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** имеют полное право на существование в рамках российского права <1>. Данные положения укладываются в рамки классического договорного права с точки зрения положений п. 3 ст. 434 и п. 3 ст. 438 ГК РФ. Отечественные суды относятся к ним вполне благосклонно. К тому же российское законодательство давно уже признает действительность предшественника **click-wrap**-соглашения - так называемой оборточной лицензии (п. 5 ст. 1286 ГК РФ <2>), прямо предусматривающей схожий особый порядок заключения договора в отношении программного обеспечения. Если же мы признаем действительность "оборотных" лицензий, где согласие пользователей с их условиями выражено гораздо менее очевидным образом (в форме начала использования программы в соответствии с условиями, изложенными на ее экземпляре, упаковке или в электронном виде), 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.

<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 23 сентября 1992 г. № 3523-1 "О правовой охране программ для электронных вычислительных машин и баз данных".

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 <1>. 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 <2>. С другой стороны, в таких случаях усложняется доказывание того факта, что пользователь был заранее (т.е. до начала использования) ознакомлен с условиями соглашения.

<1> Davidson A. The Law of Electronic Commerce. Cambridge University Press. 2009. P. 70.

<2> 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 (2d Cir N.Y., 2004).

Типичным примером данных соглашений являются различного рода правила использования веб-сайта, ссылки на которые обычно содержатся внизу веб-страницы данного сайта. Эти правила предусматривают, что просмотр или иное использование сайта предполагают 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>.

<1> Sandeen S. The Sense and Nonsense of Web-site terms of Use Agreements // Hamline Law Review. 2003. N 26. P. 525, 528.

Как правило, все условия правил пользования сайтом можно разделить на информационные (содержащие уведомления о правах на интеллектуальную собственность, статусе владельца сайта <1>) 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 <2>.

<1> 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>.

<2> 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.

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.

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 содержанием, нежели 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 отправляет на конкретную страницу или ресурс веб-сайта, а не на его главную 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>.

<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. November 2008. N 64. P. 204.

В настоящее время одним из наиболее цитируемых дел по вопросам **browse-wrap**-соглашений является **Register.com, Inc. v. Verio, Inc.** <1>. 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**-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.

<1> 356 F.3d 393 (2d Cir. 2004).

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.

<1> Указанный подход нашел свое отражение и в других решениях. См.: *Southwest Airlines Co. v. Board First, L.L.C.* N 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).

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" <1>.

<1> The Canadian Real Estate Association v. Sutton (Québec) Real Estate Services Inc., Québec Supreme Court. Case N 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>.

<1> Oberlandesgericht Hamburg. N 3 U 168/00. 13.06.2002.

<2> Netwise v. NTS Computers. 5 December 2002. Computerrecht 2003/02. P. 149.

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 <1>. 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.

<1> Femminella J. Online Terms and Conditions: Bound by the Web // St. John's Journal of Legal Commentary. 2003. N 17. P. 102.

В связи с вышеизложенным можно предложить следующую рекомендацию. Если информация на веб-сайте представляет собой высокую 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 особо критичным 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.

<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. 2005. N 11. P. 165.

§ 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 содержанием. Это могут быть как 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.

<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.

В зависимости от того, какой концепции электронной подписи законодатель отдает предпочтение, можно с определенной долей условности выделить три основные модели регулирования электронных подписей <1>:

<1> 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. N 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, предмет 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 <1>. Стороны сами определяют степень надежности подписи и технологию, используемую для ее создания. Данный подход свойствен для США, Канады;

<1> А не на создание взамен них новых, как это имеет место в первом подходе.

3) сочетание вышеуказанных подходов, в котором электронные подписи признаются легитимными в принципе, но существует особый привилегированный вид электронных подписей, отвечающий определенным критериям. Данный подход отражен в [Директиве ЕС N 1999/93/ЕС "Об электронных подписях"](#) <1> и с недавнего времени - в России.

<1> Official Journal. 13/12. 19.01.2000.

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 <1>, Вашингтон <2>, Флорида <3>, а впоследствии и на уровне федерального закона США <4>) и в Европе (в Германии <5>, Италии <6>, Испании, Голландии, Финляндии, Франции, Швеции и во многих других странах). В 1999 г. Европейским союзом была принята [Директива](#) N 1999/93/ЕС "Об общих условиях использования электронных подписей в Сообществе" (**Directive on a Community framework for electronic signatures**) <7>, которая подобно **E-Sign Act** в США была направлена на обеспечение единообразия в понимании категории "электронная подпись" и обеспечение их взаимного признания европейскими странами.

<1> Utah Digital Signatures Act of 1996.

<2> Washington Electronic Authentication Act of 1996.

<3> Florida Electronic Signature Act of 1996.

<4> The Electronic Signatures in Global and National Commerce Act (E-Sign Act) of 2000.

<5> Gesetz zur Digitalen Signatur BT-Drs. 13/7934

vom 11.06.1997.

<6> Italian Electronic Document and Digital Signature Act 1997 (Legge Bassanini, 59/1997).

<7> Official Journal of the European Communities. L013. 19.01.00.

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. Подписи второго вида - продвинутые электронные подписи - должны соответствовать следующим требованиям:

- уникальным образом связаны с определенной стороной, подписавшей документ;

- имеют способность идентификации 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 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. <1>, который в отличие от своего предшественника построен по "гибридной" (третьей) модели регламентации использования 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).

<1> Типовой [закон](#) об электронных подписях, принятый Комиссией Организации Объединенных Наций по праву международной торговли, утвержден Резолюцией Генеральной Ассамблеи ООН от 24 января

2002 г. N A/56/588.

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 N 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.

<1> Ильиных Е.В., Козлова М.Н. [Комментарий](#) к Федеральному закону от 10 января 2002 г. N 1-ФЗ "Об электронной цифровой подписи" (постатейный). М., 2005.

Первым законом, посвященным регулированию электронных подписей, был Федеральный [закон](#) от 10 января 2002 г. N 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 целой плеядой 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).

<1> Леонтьев К.Б. Комментарий к Федеральному закону "Об электронной цифровой подписи" (постатейный). М., 2003. С. 6.

Учитывая технологическую жесткость [Закона](#) об ЭЦП 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. Не удивительно, что указанный [Закон](#) стал привлекательным объектом для критики. Так, в числе недостатков [Закона](#) об ЭЦП 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 регулирования <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, увольнения и т.д. <2>.

<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. N 3.

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 пять лет после принятия [Директивы](#) N 1999/93/ЕС) в Европе использовали усиленные

электронные подписи до 70% населения <1>.

<1> Данные взяты из [пояснительной записки](http://asozd2.duma.gov.ru/main.nsf/%28SpravkaNew%29?OpenAgent&RN=305592-5&02) к проекту Федерального закона N 305592-5 "Об электронной подписи" // <http://asozd2.duma.gov.ru/main.nsf/%28SpravkaNew%29?OpenAgent&RN=305592-5&02>.

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, а также на расширение сферы использования и допустимых видов электронных подписей <1>.

<1> [Пояснительная записка](#) к проекту Федерального закона N 305592-5 "Об электронной подписи".

Новый Федеральный [закон](#) от 6 апреля 2011 г. N 63-ФЗ "Об электронной подписи" (далее - Закон об ЭП) вступил в силу 8 апреля 2011 г. При этом старый [Закон](#) об ЭЦП не был отменен вплоть до 1 июля 2013 г., что породило достаточно парадоксальную ситуацию параллельного действия двух Законов, регулирующих однородные отношения.

Так или иначе, [Закон](#) об ЭП теперь является основным актом, регулирующим использование электронной подписи в России, в связи с чем необходимо рассмотреть подробнее его основные

положения.

В целом новый **Закон** в гораздо большей степени учитывает положения Типового **закона** ЮНСИТРАЛ об электронных подписях и **Директивы** ЕС N 1999/93/ЕС, во многом воспроизводя положения последней.

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, высланных на мобильный телефон при совершении конкретной транзакции <1>, использование в качестве идентификатора адреса электронной почты (для доступа к которой также необходимо знание пароля) <2> - все это подпадает под понятие простой

электронной подписи.

<1> См., например: [Определение](#) Приморского краевого суда от 7 апреля 2015 г. по делу N 33-2865, где говорится: "Согласно оферте смс-код используется в качестве электронной подписи клиента, для формирования им каждого электронного документа. В случае идентичности смс-кода, направленного банком, и смс-кода, введенного в форме электронного документа для подтверждения передачи клиентом соответствующего распоряжения/заявления через интернет-банк, такая электронная подпись считается подлинной и предоставленной клиентом".

<2> Как отмечено на официальном сайте Минкомсвязи России, выступающего в качестве уполномоченного федерального органа исполнительной власти в сфере использования электронной подписи, "если участники электронного взаимодействия достигли соглашения о том, что получение электронного сообщения с определенного адреса электронной почты будет считаться подписанием документа простой электронной подписью и при этом выполнено одно из вышеобозначенных условий, то такое электронное сообщение может считаться подписанным простой электронной подписью". См. в Интернете по адресу: <http://minsvyaz.ru/ru/appeals/faq/33/>.

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 имелось 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 Ф.И.О. 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 иногда высказываемому мнению о том, что простой электронной подписью в данном случае является связка "логин - пароль", 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, касающиеся гражданско-правовых отношений <1>, из которых следует признание равной юридической силы электронных документов, подписанных простой электронной 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 <2>. 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).

<1> Вместе с тем существуют нормативные правовые акты, которые приравнивают по юридической силе простую электронную подпись к собственноручной подписи при оказании государственных и муниципальных услуг. См.: [Постановление Правительства РФ от 25 января 2013 г. N 33 "Об использовании простой электронной подписи при оказании государственных и муниципальных услуг"](#), а

также [Правила](#) использования простой электронной подписи при оказании государственных и муниципальных услуг.

<2> См.: [п. 2](#) Рекомендаций по заключению договоров в электронной форме, утв. Ассоциацией российских банков 19 декабря 2012 г. // Вестник Ассоциации российских банков. 2013. N 1 - 2.

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 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 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.

КонсультантПлюс: примечание.

Комментарий к Гражданскому кодексу Российской Федерации, части первой (под ред. О.Н. Садикова) включен в информационный банк согласно публикации - КОНТРАКТ, ИНФРА-М, 2005 (3-е издание, исправленное, переработанное и дополненное).

<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. N Ф03-6794/2009 по делу N А24-5830/2008. В пересмотре дела в порядке надзора отказано [Определением](#) ВАС РФ от 14 апреля 2010 г. N ВАС-1375/10; см. также: [Постановление](#) ФАС Московского округа от 5 декабря 2003 г. N КГ-А40/9513-03 по делу N А40-47669/02-69-492.

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.

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 так же 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 малоприспособленным 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.

Оптимальной сферой применения усиленной неквалифицированной подписи представляется ее использование в закрытых информационных системах между контрагентами с уже сложившимися деловыми отношениями касательно договоров, содержание которых отличается информационной насыщенностью и длительными согласованиями. Особенно это справедливо в случаях, когда контрагенты находятся в разных странах, так как вопросы признания цифровой подписи, выданной иностранным удостоверяющим центром на территории России, и наоборот, признания на территории иностранного государства усиленной квалифицированной подписи, выданной российским центром, могут вызвать существенные затруднения. Кроме того, выдача усиленной квалифицированной подписи обычно требует личного присутствия подписанта, в то время как для усиленной неквалифицированной подписи такое присутствие необязательно.

Нередко усиленная неквалифицированная подпись используется в сфере дистанционного банковского обслуживания <1>. В таком случае удостоверяющим центром, выдающим сертификат ключа проверки электронной подписи, выступает сам банк, что позволяет локализовать процесс обработки

платежных транзакций, не вовлекая в него третьих лиц в виде аккредитованных удостоверяющих центров. Особую ценность применительно к усиленной неквалифицированной подписи имеет ее защитная функция, позволяющая "заморозить" документ по состоянию на определенный момент времени и отследить возможные несанкционированные изменения.

<1> См., например: Правила использования усиленной неквалифицированной электронной подписи ПАО "Промсвязьбанк" // <http://www.psbank.ru/Personal/Everyday/Remote/RulesEcp>.

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 выданного аккредитованным удостоверяющим центром <1>, а также использованием для ее создания средств, получивших специальное подтверждение соответствия их требованиям [Закона](#) об ЭП, т.е. сертифицированных ФСБ России.

<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. N 976 "О федеральном органе исполнительной власти, уполномоченном в сфере использования электронной подписи"). Перечень аккредитованных удостоверяющих центров размещен на сайте Минкомсвязи России: <http://minsvyaz.ru>.

В качестве примера усиленной квалифицированной электронной подписи можно привести электронную цифровую подпись, о которой шла речь в **Зако**не 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. Если провести аналогию с дверными ключами, то технология асимметричного шифрования может быть представлена в виде входной двери с двумя замочными скважинами. У пользователя - закрытый ключ, который закрывает дверь, а у контрагента - открытый, посредством которого дверь может быть открыта.

С принятием нового [Закона](#) данный вид электронной подписи стал не единственно возможным, а одним из возможных видов электронной подписи. С 1 января 2013 г. гражданам выдается универсальная электронная карта, в которую встроена усиленная квалифицированная электронная подпись <1>.

<1> Универсальная электронная карта (УЭК) - пластиковая карта, представляющая собой уникальное идентификационное средство гражданина. Основное предназначение УЭК - дистанционный заказ, оплата и получение государственных услуг. Предполагается, что карта заменит множество документов, в том числе медицинский полис и страховое пенсионное свидетельство, объединяя идентификационную карту, электронный кошелек с привязкой к банковскому счету, электронную подпись и даже проездной билет.

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 ([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 равнозначным его 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, 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 информации, 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 устанавливает 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 и ФСБ России <1> (ч. 3 ст. 16 Закона об ЭП).

<1> **Приказ** ФСБ России от 30 августа 2012 г. N 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. N 25563.

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 сертификата электронной подписи с выдачей его заявителю, который приобретает статус владельца такого сертификата. При этом важно подчеркнуть, что аккредитованный удостоверяющий центр должен обеспечить привязку выдаваемого сертификата к **реальной** личности, что обеспечивается возложенной на этот центр обязанностью установить личность заявителя - физического лица, обратившегося в него за получением квалифицированного сертификата, и корреспондирующей с ней обязанностью такого лица представить паспорт и иные документы, подтверждающие его статус (ст. 18 Закона об ЭП). 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, один 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. По сути, он является своего рода электронным паспортом участника электронного документооборота. 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 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>.

<1> См.: Приказ Минкомсвязи России от 5 октября 2011 г. N 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.

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 вариант, при котором подпись, проставленная иным сотрудником юридического лица, будет признана действительной, а сведения об уполномоченном

физическом лице носят информационный характер, 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 Интернете (неиспользование антивирусных программ, использование нелегального программного обеспечения, отсутствие ограничений по принятию документов только с определенного IP-адреса и пр.) <1>.

<1> Данный подход нашел свое отражение в отечественной судебной практике. См.: [Постановление](#) Семнадцатого арбитражного апелляционного суда от 12 декабря 2011 г. по делу N А60-15360/2011, оставленное в силе [Постановлением](#) ФАС Уральского округа от 30 марта 2012 г. N Ф09-1458/12.

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 ЭЦП (квалифицированных электронных подписей). Обычно клиенты банков оспаривают правомерность совершения банком операций по поручениям, сделанным неуполномоченными лицами с использованием ЭЦП клиента (квалифицированной электронной подписи). Стандартный ответ суда в таком случае заключается в том, что банк 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 неправомочность 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>.

<1> См., например: Постановления ФАС Московского округа от 13 ноября 2012 г. [N Ф05-12672/12](#) по делу N А40-18115/2012; ФАС Северо-Западного округа от 16 октября 2012 г. [N Ф07-5221/12](#) по делу N А66-9956/2011; ФАС Дальневосточного округа от 23 октября 2012 г. [N Ф03-4500/12](#) по делу N А73-7000/2011.

<2> [Постановление](#) Семнадцатого арбитражного апелляционного суда от 18 августа 2011 г. N 17АП-6233/2011-ГК по делу N А50-18570/2010.

<3> [Постановление](#) ФАС Северо-Кавказского округа от 27 апреля 2011 г. по делу N А63-6446/2010.

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 [Законом 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., подтверждаемого договором страхования ответственности, банковской

гарантией или договором поручительства ([п. п. 1, 2 ч. 3 ст. 16 Закона об ЭП](#)).

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, 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>.

<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 на деликтные отношения, в частности на нарушение исключительного права. См.: [Постановление](#)

Президиума ВАС РФ от 20 ноября 2012 г. N 8953/12; п. 23 Постановления Пленума ВС РФ N 5, Пленума ВАС РФ N 29 от 26 марта 2009 г. "О некоторых вопросах, возникших в связи с введением в действие части четвертой Гражданского кодекса Российской Федерации".

Поскольку электронная коммерция функционирует на базе Интернета 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 "иностраный 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) ^{<1>}, это препятствовало применению ЭЦП в трансграничных сделках, превратив ее, по существу, в инструмент электронного документооборота с госорганами Российской Федерации.

^{<1>} 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.

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, поскольку, 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>?

<1> Калятин В.О. Право в сфере Интернета. С. 130.

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 **законо** 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](#) N 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 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 решении 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.

<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](#) // Вестник гражданского права. 2006. N 2. Ч. 2. Т. 6.

Как известно, сообщения, посланные по электронной почте, могут затеряться и не дойти до адресата, отчасти в силу архитектуры сети Интернет, не гарантирующей 100-процентной 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 сходится во мнении, что данное правило не должно переноситься на электронную почту <3>.

<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.

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 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>.

<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.

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 отправленное 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 (е)). 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>.

<1> Reed C., Angel J. Op. cit. P. 202.

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 связывают 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, "здоровый 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" <1>. Данное соображение в полной мере применимо и к электронным сообщениям.

<1> Карапетов А.Г. [Расторжение нарушенного договора](#) в российском и зарубежном праве. М., 2007. С. 271.

В целях пресечения недобросовестных действий со стороны получателя закон вводит презумпцию наличия такой доставки в случае обстоятельств, находящихся в сфере контроля адресата, по причине 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. N 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. 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>.

КонсультантПлюс: примечание.

Монография В.С. Витко "Гражданско-правовая природа лицензионного договора" включена в информационный банк согласно публикации - Статут, 2011.

<1> Витко В.С. Гражданско-правовая природа лицензионного договора. М., 2012. С. 283.

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" 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.

<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.

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. <1>, 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 <2>.

<1> "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 Конвенции](#)).

<2> Weatherby v. Banham [1832] 5 C & P, 228; Treitel G. The Law of Contract. London, 2007. § 2-026, 2-046.

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 offerent 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 ИТ-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 средства могут располагаться за пределами правовой системы, где находятся отправитель и адресат сообщения; во-вторых, одна из сторон (а иногда и обе) может 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 обеспечивались 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. 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 находятся 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 разработчиками, "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>.

<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. Международно-правовое регулирование электронной коммерции: Автореф. дис. ... канд. юрид. наук. СПб., 2005. С. 10.

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 были фактически получены 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. Если информация, размещенная на сайте интернет-магазина, может быть квалифицирована как публичная оферта и покупатель совершил ее акцепт посредством размещения заказа, то договор будет считаться заключенным в месте нахождения продавца (владельца сайта интернет-магазина). Если же такая информация не выступала в качестве публичной оферты либо покупатель в процессе размещения заказа добавил какие-либо дополнительные условия, сделав тем самым встречную оферту, то последующий ее акцепт интернет-магазином будет означать, что договор был заключен в месте нахождения (месте жительства) покупателя.

§ 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 <1>.

<1> 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 Интернета, 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. ст. 172, 175 ГК РФ).

К слову сказать, подобные риски существуют и в зарубежных правовых системах, 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, дефиниция понятия "мелкая бытовая сделка" отсутствует в законодательстве, оно 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.

<1> См.: Тарасова А.Е. Указ. соч.

<2> Данный подход реализован, в частности, в российской версии **Apple Store**.

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 компании 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**-соглашения, 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 могут быть отнесены: 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 "компания 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 нелегально для современной компании" <3>.

<1> Савельев А.И. Лицензирование программного обеспечения в России: законодательство и практика. М., 2012. Гл. 2. § 2.

<2> Информационное [письмо](#) от 23 октября 2000 г. N 57 "О некоторых вопросах практики применения статьи 183 Гражданского кодекса Российской Федерации".

<3> Via Viente Taiwan, L.P. v. United Parcel Service, Inc. N 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 authority**), достаточную для того, чтобы связать компанию-работодателя соответствующими договорными обязательствами. Здесь представляет собой интерес доктрина доверия к внешним фактам, которая освещается далее применительно к электронным агентам.

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.

Наконец, немаловажное значение имеет позиция ВС РФ, согласно которой лицо, являющееся администратором домена, в котором расположен почтовый сервер компании, несет ответственность за сообщения, исходящие с такого почтового сервера. Как отметил Верховный Суд РФ, владелец (администратор) домена с соответствующим именем отвечает за любые действия, совершенные с использованием такого домена, в том числе за направление с его использованием электронных сообщений <1>. В связи с этим тот факт, что определенное электронное сообщение было отправлено лицом, которому компания предоставила почтовый адрес на сервере своей корпоративной почты, уже предполагает определенный уровень ответственности компании за действия работника, совершенные с использованием такого почтового ящика.

<1> [Постановление](#) Верховного Суда РФ от 24 апреля 2015 г. N 305-АД15-2693 по делу N А40-36625/2014.

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>.

<1> Tom Allen, Robin Widdison. Can Computers Make Contracts? // Harvard Journal of Law Technology. 1996. N 9.

Кроме того, получают распространение интернет-сервисы, которые предоставляют сторонам возможность заключения "умных" контрактов - соглашений, существующих в форме программного кода, имплементированного по технологии **Blockchain**, который обеспечивает автономность и самоисполнимость условий такого договора по наступлении заранее определенных в нем обстоятельств. В частности, оплата по таким соглашениям осуществляется в автоматическом режиме с использованием заранее зарезервированных средств на основании полученных сведений об исполнении договора другой стороной, которое также отслеживается данным сервисом в автоматическом режиме (например, посредством отслеживания данных RFID-меток на грузовых контейнерах, произошедших

изменений в электронных реестрах прав и др.). В настоящее время наиболее перспективной платформой для реализации "умных" контрактов считается платформа **Etherium** (от англ. **ether** - эфир, в связи с чем обычно произносится как "эфириум"). Данная платформа позволяет создавать собственные **токены** - цифровые активы, обладающие ценностью: единицы криптовалюты, доли в праве на актив и др. Распоряжение такими активами будет осуществляться посредством специального приложения - электронного кошелька. При этом создатель токенов может сам определять правила их распространения и ограничить возможность доступа к своей системе заранее определенным кругом лиц. При этом возникает возможность создания собственных частных экосистем, основанных на платформе **Blockchain**, в рамках которых будет осуществляться заключение и исполнение "умных" контрактов в отношении определенных токенов.

Кроме того, благодаря развитию технологии **Blockchain** активно ведутся дискуссии о возможности существования так называемых децентрализованных автономных организаций (**Decentralized Autonomous Organizations**), которые представляют собой программные комплексы, осуществляющие покупку и продажу активов, принятие организационных решений и иные действия на основе компьютерных алгоритмов без вмешательства человека. Такая организация не присутствует в физическом мире, у нее нет органов управления. В основе такой организации - совокупность "умных" контрактов. В качестве возможного примера сферы применения такой организации указывается управление венчурным проектом: спонсоры и участники проекта могут подавать свои предложения на рассмотрение остальных, осуществлять голосование и основанное на его результатах распределение ресурсов

<1>. В итоге возникает организация, основанная на прямом управлении "акционерами", но в которой функции исполнительных органов выполняет компьютерная программа. Такая программа может выплачивать дивиденды, платить по счетам контрагентов и выполнять иные функции. Отличительным преимуществом таких программных комплексов является стабильность отношений: невозможность произвольного прекращения или изменения условий проекта по инициативе руководящего органа, а равно невозможность такого органа сбежать с деньгами "акционеров". Прототипы программного кода для таких организаций уже разработаны и доступны на условиях **open source**-лицензий <2>.

<1> Tim Swanson. Op. cit. P. 53. См. также: Васькович А. Юридические электронные лица // Ведомости. 23.05.2016.

<2> Christoph Jentzsch. The Standard DAO Framework, inc. Whitepaper. URL: <https://github.com/slockit/DAO>.

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 контрагирования, 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 <1>:

<1> Данная классификация приводится в ст. 14 Единообразного закона США об электронных сделках.

1) "человек - электронный агент";

2) "электронный агент - электронный агент".

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-бота" <1>. Как отмечает В.О. Калятин, "программа же не принимает решение, а только перенаправляет клиенту заранее определенное на данный случай решение владельца сайта" <2>.

<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; Капев 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.

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 <1>, что можно рассматривать в качестве проявления общего принципа осуществления гражданских прав по усмотрению участников оборота (ст. 9 ГК РФ).

<1> Например, заранее выраженное согласие поручителя на последующее изменение основного обязательства (п. 16 Постановления Пленума ВАС РФ от 12 июля 2012 г. N 42 "О некоторых вопросах разрешения споров, связанных с поручительством"); заранее выраженное согласие на заключение сублицензионных договоров (п. 17 Постановления Пленума Верховного Суда РФ N 5, Пленума ВАС РФ N 29 от 26 марта 2009 г. "О некоторых вопросах, возникших в связи с введением в действие части четвертой Гражданского кодекса Российской Федерации").

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. В.О. Калятин приводит 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 <1>.

<1> Калятин В.О. Право в сфере Интернета. С. 337.

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, если продажная стоимость установлена в виде 40 долл. при обычной стоимости в 4000 долл., то акцептант не должен иметь возможность "ухватиться" (**snap**) за такое предложение) <1>. В приведенном выше примере нельзя говорить об очевидности ошибки - 100 фунтов не являются бросовой ценой, да и распродажи в канун Нового года являются обычным делом.

<1> 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. 2000. N 18. P. 427.

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 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. ст. 402, 403](#) ГК РФ). Из этого следует, что он должен тем более нести ответственность за действия подконтрольных ему электронных агентов, решение об использовании которых он принимал сам.

Примечательно, что отечественная судебная практика порой идет иным путем. Так, в одном из дел суд пришел к выводу, что договор купли-продажи не был заключен, поскольку "цена товара, указанная на сайте www.sapato.ru, была отображена некорректно в результате программного сбоя, произошедшего 22.04.2014, и была в несколько раз ниже рыночной цены" ^{<1>}. Представляется, что использование конструкции незаключенного договора хотя и возможно, но все же менее предпочтительно, поскольку является слишком прямолинейным, в отличие от специального механизма [ст. 178 ГК РФ](#), предусматривающего учет различных факторов (степень существенности заблуждения, возможность другой стороны распознать такое заблуждение с учетом содержания сделки и сопутствующих обстоятельств и др.). Признание договора незаключенным по причине технического сбоя электронного агента, действующего в интересах предпринимателей, в отсутствие учета подобных факторов может влечь освобождение предпринимателя от предпринимательского риска и фактически "исправление" судом его коммерческих просчетов за счет интересов потребителя.

^{<1>} См.: Апелляционное [определение](#) Хабаровского краевого суда от 22 апреля 2015 г. по делу N 33-2351/2015.

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 "воля" 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>.

<1> Дмитрик Н.А. [Осуществление субъективных гражданских прав](#) с использованием сети Интернет. С. 90.

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. Хакерские атаки в Интернете 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.

<1> См., например: Постановления Восьмого арбитражного апелляционного суда от 25 ноября 2011 г. [N A70-3415/2011](#) ("Согласно выводам эксперта исходящие международные соединения... инициировались посредством использования программы-бота. 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"); от 4 февраля 2013 г. [N 08АП-10404/12](#) (ответственность за ненадлежащую эксплуатацию абонентской линии или пользовательского (оконечного) оборудования несет сам абонент, что влечет возложение на него бремени негативных последствий несанкционированного доступа к сетям связи лиц, не имеющих на это права).

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 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 процесс 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>.

<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.

В качестве примера такой ситуации можно привести достаточно любопытное дело, рассмотренное судом штата Колорадо в 2007 г. <1>. Ответчиком по данному спору выступал известный интернет-архив **Wayback Machine**, который осуществляет копирование содержания веб-страниц различных сайтов Интернета с определенным ~~временным~~ 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.

<1> Internet Archive v. Shell. Civil Action N 06-cv-01726-LTB-CBS, 2007 U.S. Dist. LEXIS 10239 (D. Colo. Feb. 13, 2007).

В зарубежной доктрине предлагались различные подходы к решению подобных ситуаций.

1. Признание наличия отношений представительства (агентирования) между владельцем программы-бота (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 неправомерна. К функционированию таких систем не могут применяться общие принципы агентского права (например, принципы, предусматривающие ограничение ответственности при наличии вины агента) <2>.

<1> Fisher J. Computers as Agents: A Proposed Approach to Revised U.C.C. Article 2 // Indiana Law Journal. 1997. N 72. P. 545, 570.

<2> Пояснительная записка Секретариата ЮНСИТРАЛ к Конвенции ООН об использовании электронных сообщений в международных договорах. С. 69.

2. Признание электронного агента с элементами

искусственного интеллекта правосубъектным лицом <1>. 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 допустить возможность предъявления иска к такому "субъекту" <2>. В ответ на вполне резонный вопрос о том, каким имуществом будет отвечать такой "субъект", они предлагают использовать механизм страхования ответственности <3>. 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 <4>.

<1> Solum L. Legal Personhood for Artificial Intelligences // North Carolina Law Review. 1992. N 70. P. 1231.

<2> Wein L. The Responsibility of Intelligent Artifacts: Toward an Automated Jurisprudence // Harvard Journal of Law & Technology. 1992. N 6. P. 103 and ff.

<3> 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.

<4> Tom Allen, Robin Widdison. Op. cit. P. 42.

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 этих 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 <1>. А появление упоминавшихся в [гл. 1](#) настоящей книги децентрализованных автономных организаций, построенных на базе технологии **Блокчейн**, устраняет остатки сомнений в скором появлении новых видов "субъектов" права, основанных на самообучающихся автономных компьютерных алгоритмах.

<1> См., например: Pagallo U. The Laws of Robots: Crimes, Contracts and Torts. Springer-Verlag. Berlin, 2013.

3. Наибольший интерес представляет собой третий подход, заключающийся в применении к отношениям, связанным с использованием электронных агентов, теории доверия к внешним фактам <1>. 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, 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" <2>. 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" <3>.

<1> Yves Poullet. Conclude a Contract Through Electronic Agents? 1999.

<2> Demogue R. Notions fondamentales du droit prive. Paris, 1911. P. 67

<3> Покровский И.А. Основные проблемы гражданского права. М., 2003. С. 201.

Теория доверия к внешним фактам имеет много различных проявлений <1>. 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. Данный подход находит свое отражение, например, во французском <2>, голландском <3>, английском <4>, американском <5> договорном праве. 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 <6>.

<1> Одним из наиболее известных ее проявлений является объяснение концепции добросовестного приобретения права собственности от неуполномоченного лица. См. подробнее: Черепяхин Б.Б. Юридическая природа и обоснование приобретения права собственности от неуполномоченного отчуждателя. М., 2001.

<2> Nicholas B. The French Law of Contract, Clarendon Press Oxford. 2ed. 1992. P. 178.

<3> Harkamp A., Tillema M. Contract Law in the Netherlands. Kluwer Law International, 1995. P. 35, 61 and 76.

<4> McKendrick E. Op. cit. P. 23 - 50.

<5> Farnsworth on Contracts. 4th ed. Aspen Publishers. N.Y. P. 115.

<6> О регулировании стандартных условий договора и защите слабой стороны см. подробнее: Ключков 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. N 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.

В контексте электронных сделок она будет применяться приблизительно следующим образом. В случае если интернет-магазин использует электронных агентов, которые осуществляют оформление заказа, и такой заказ был принят, 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 контрактирования 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 перед 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) положило на действия такого лица. Примеров, в том числе и из сферы вещного права (например, правила 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, характера 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.

<1> Брагинский М.И., Витрянский В.В. Договорное

право. Общие положения. М., 2003. С. 172.

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 Интернете, обуславливает 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. ст. 450 - 453 ГК РФ). Другое дело, что данные положения не в полной мере 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.

<1> См.: [п. 1 ст. 420 ГК РФ](#), в котором сказано:

"Договором признается соглашение двух или нескольких лиц об установлении, изменении или прекращении гражданских прав и обязанностей".

Подобная практика одностороннего изменения условий договоров, заключенных в Интернете, 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. ст. 310 и 450.1](#) ГК РФ. В соответствии с новой редакцией [п. 2 ст. 310](#) ГК РФ "одностороннее изменение условий обязательства, связанного с осуществлением всеми его сторонами предпринимательской деятельности, или односторонний отказ от исполнения этого обязательства допускается в случаях, предусмотренных настоящим [Кодексом](#), другими законами, иными правовыми актами или договором.

В случае если исполнение обязательства связано с осуществлением предпринимательской деятельности не всеми его сторонами, право на одностороннее изменение его условий или отказ от исполнения обязательства может быть предоставлено договором лишь стороне, не осуществляющей предпринимательской деятельности, за исключением

случаев, когда законом или иным правовым актом предусмотрена возможность предоставления договором такого права другой стороне". Пункт 2 ст. 450.1 ГК РФ, как и ранее п. 3 ст. 450 ГК РФ, устанавливает, что "в случае одностороннего отказа от договора (исполнения договора) полностью или частично, если такой отказ допускается, договор считается 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. 2 ст. 450.1 ГК РФ (ранее - 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. 2 ст. 450.1 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. 450.1 ГК РФ входит в гл. 29 ГК РФ, поэтому п. 3 ст. 420 ГК РФ может быть использован в качестве обоснования приоритета положений ст. 450.1 ГК РФ перед ст. 310 ГК РФ <2>.

<1> В Постановлении ФАС Северо-Кавказского округа от 15 февраля 2000 г. по делу N Ф08-204/2000 указано: "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. N 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.

2. Признать п. 3 ст. 450 ГК РФ тем самым "законом", о котором говорится в ст. 310 ГК РФ, в качестве основания для легитимизации одностороннего

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>.

<1> Маковский А.Л. Общие правила об обязательствах в Гражданском кодексе // Вестник ВАС РФ. 1995. N 9. С. 96.

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 <1>. 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" <2> (далее - Закон о банках и банковской деятельности) **применяться не может** (выделено мной. - **А.И.**). Иное его истолкование правоприменителем не согласуется с **Конституцией РФ**".

<1> См.: **Постановление** Конституционного Суда РФ от 23 февраля 1999 г. N 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. N 3.

<2> 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 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](#) ГК РФ и [п. 3 ст. 450](#) ГК РФ.

Изложенная позиция может иметь непосредственное 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, а нормативно-интерпретационного акта" ^{<1>}.

^{<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. Ереван, 1999. Вып. 2 (4). С. 7.

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 <1>. 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 только в случае заключения между банком и гражданином, не являющимся предпринимателем, соответствующего дополнительного соглашения" <2>.

<1> Постановления ФАС Поволжского округа от 6 декабря 2010 г. по делу [N A12-10892/2010](#), Пятнадцатого арбитражного апелляционного суда от 22 июля 2013 г. [N 15АП-8131/2013](#) по делу [N A53-36813/2012](#), Первого арбитражного апелляционного суда от 22 июля 2013 г. по делу [N A43-5251/2013](#).

<2> [Постановление](#) Седьмого арбитражного апелляционного суда от 23 января 2013 г. по делу [N A27-13416/2012](#). См. также: [Постановление](#) Четырнадцатого арбитражного апелляционного суда от 14 мая 2013 г. по делу [N A13-12661/2012](#).

Таким образом, указание в договоре с потребителем права коммерческой организации об изменении в одностороннем порядке 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 <1>. Размещение информации в Интернете 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)" <2>. Молчание потребителя (отсутствие поступивших возражений или отказа от договора с его стороны в

течение определенного периода времени) не может приравниваться к согласию с выставленными изменениями, так как молчание не является конклюдентным действием <3>.

<1> [Постановление](#) ФАС Волго-Вятского округа от 8 февраля 2011 г. по делу N A28-14037/2009.

<2> Постановления ФАС Волго-Вятского округа от 8 февраля 2011 г. по делу [N A28-14037/2009](#), ФАС Дальневосточного округа от 7 февраля 2012 г. [N Ф03-6661/2011](#).

<3> [Постановление](#) ФАС Волго-Вятского округа от 8 февраля 2011 г. по делу N A28-14037/2009.

Применительно к договорам дистанционной купли-продажи товаров, заключаемым в сети Интернет, суды приходят к схожим выводам. Так, ссылка интернет-магазина на пользовательское соглашение, допускающее изменение цены договора в одностороннем порядке, не была принята судом, поскольку "в силу [ст. 310](#) ГК РФ односторонний отказ от исполнения обязательства и одностороннее изменение его условий не допускаются, за исключением случаев, предусмотренных законом. Таким образом, ответчик в одностороннем порядке отказался от исполнения договора купли-продажи, что противоречит положениям действующего законодательства". При этом, по мнению суда, факт отсутствия товара на складе у продавца не имеет правового значения для разрешения настоящего спора, поскольку из материалов дела следует, что указанный товар с производства не снят, его поставки не прекращены <1>. Включение в договор с

потребителем условия о допустимости одностороннего изменения договора может влечь установленную административную ответственность (ч. 2 ст. 14.8 КоАП РФ) <2>.

<1> Решение Промышленного районного суда г. Смоленска от 30 апреля 2015 г. по делу N 2-2013/2015.

<2> В **Постановлении** Девятнадцатого арбитражного апелляционного суда от 15 февраля 2013 г. по делу N А36-6311/2012 говорится: "Включение ООО "Компьютерные системы" в текст договора условий о возможности одностороннего изменения продавцом цены на заказанные позиции товара либо аннулирования заказа с учетом новой цены товара применительно к **пункту 1 статьи 16** Закона о защите прав потребителей ущемляет установленные законом права потребителей и образует состав административного правонарушения, предусмотренного **ч. 2 ст. 14.8 КоАП РФ**".

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, доступная 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 временными 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 тыс. до 20 тыс. рублей. 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. Например, такой практики нередко придерживаются сервисы социальных сетей, магазины цифрового контента (например, **iTunes**) и иные подобные сервисы.

В остальных случаях можно предусмотреть в договоре с потребителем условие примерно следующего содержания: "Изменение договора оформляется путем заключения дополнительного соглашения в письменной форме либо путем совершения абонентом конклюдентных действий в виде **(указание перечня 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.

^{<1>} [Постановление](#) Второго арбитражного апелляционного суда от 31 января 2012 г. по делу N А28-8512/2011.

Таким образом, существует два варианта легитимного изменения условий договора с

потребителем:

1) наличие основания для изменения такого условия в законодательстве -> уведомление потребителя о таком изменении в порядке, предусмотренном в соответствующем нормативном правовом акте и договоре;

2) 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.

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.

Рассматривая вопрос об одностороннем расторжении договора с участием потребителя в сфере электронной коммерции, необходимо остановиться и на

основаниях для такого расторжения договора, предоставленных потребителю. Одно из этих оснований предусмотрено в [ст. 26.1](#) Закона о защите прав потребителей применительно к договорам купли-продажи товаров дистанционным способом. В соответствии с [п. 4 данной статьи](#) потребитель вправе отказаться от товара в любое время до его передачи, а после передачи товара - в течение семи дней. При этом если информация о наличии у потребителя такого права не была предоставлена в момент доставки товара, то срок для возможного отказа от товара продлевается до трех месяцев с момента его передачи.

Можно обозначить следующие основные положения, касающиеся условий и порядка реализации права потребителя на отказ от товара.

Во-первых, данное право может быть реализовано лишь в рамках договора купли-продажи товара. Это правило неприменимо к договорам возмездного оказания услуг или подряда. В таких случаях должны применяться специальные положения ([ст. ст. 782 и 717](#) ГК РФ соответственно). Данное правило также не применяется к случаям приобретения цифрового контента, поскольку, как будет подробнее рассмотрено далее, возникающие отношения имеют природу лицензионного договора.

В этой части российское регулирование заметно отстает от европейского. Директива ЕС 2011/83/EU "О правах потребителей" предусматривает право потребителей на отказ от договоров, заключенных дистанционным способом, в том числе от договоров услуг и цифрового контента ([ст. ст. 9, 16 \(м\)](#)).

Во-вторых, право потребителя на отказ от товара

применимо к товару **надлежащего** качества. В этой связи указанное право является специальным по отношению к правилам, установленным в [ст. 25](#) Закона о защите прав потребителей, применительно к условиям и порядку обмена и возврата товара надлежащего качества. Об этом в том числе свидетельствует и факт повторения в [ст. 26.1](#) указанного Закона положения, схожего с содержащимся в его же [ст. 25](#), о том, что возврат товара надлежащего качества возможен в случае, если сохранены его товарный вид, потребительские свойства, а также документ, подтверждающий факт и условия покупки данного товара. Отсутствие у потребителя документа, подтверждающего факт и условия покупки товара, не лишает его возможности ссылаться на другие доказательства приобретения товара у данного продавца. В отличие от общих положений [ст. 25](#) Закона о защите прав потребителей, нормы [п. 4 ст. 26.1](#) этого Закона содержат более гибкие правила, обусловленные спецификой электронной коммерции: в качестве документа, подтверждающего факт и условия покупки товара, может выступать не только товарный или кассовый чек, но и иные документы, к числу которых вполне можно отнести распечатку сообщений электронной почты о принятии заказа и иные подобные документы ^{<1>}. Кроме того, при отсутствии указанного документа потребитель может ссылаться на любые другие доказательства приобретения товара у данного продавца, а не только на свидетельские показания.

^{<1>} Процессуальные аспекты предоставления подобного рода доказательств см. в [гл. 4](#) настоящей работы.

Если переданный во исполнение договора дистанционной купли-продажи товар является товаром ненадлежащего качества, то последствия продажи такого товара определяются общими положениями [ст. ст. 18 - 24](#) Закона о защите прав потребителей (в числе которых также есть право потребителя на отказ от исполнения договора и заявление требования о возврате уплаченной за него суммы).

В-третьих, реализация права на возврат товара, приобретенного дистанционным способом, ограничена лишь случаями, когда товар имеет индивидуально определенные свойства, в силу которых такой товар может быть реализован исключительно приобретающим его потребителем. Никаких специальных ограничений в отношении технически сложных товаров [ст. 26.1](#) Закона о защите прав потребителей не установлено, в связи с чем положения [Постановления](#) Правительства, предусматривающего ограничения возможности возврата технически сложных товаров надлежащего качества <1>, неприменимы к случаям реализации права на возврат товара на основании указанной [статьи](#). В противном случае утрачивалась бы основная цель их принятия - защита потребителя от судебных решений, принятых в отсутствие у него возможности непосредственного ознакомления с товаром в момент заключения договора. Правда, далеко не все суды придерживаются указанного подхода. В ряде случаев суды отказывали в удовлетворении требования потребителя о возврате уплаченной суммы за товар, приобретенный дистанционным способом, ссылаясь на его технически сложный характер <2>. Однако есть основания полагать, что подобная практика может измениться в связи с толкованием, данным Конституционным Судом РФ, поводом для обращения в который послужило решение суда, признавшего право потребителя на расторжение договора розничной

купли-продажи технически сложного товара надлежащего качества в одностороннем порядке и на возврат данного товара продавцу. Конституционный Суд указал на обоснованность применения соответствующих норм п. 4 ст. 26.1 Закона о защите прав потребителей, поскольку соответствующее регулирование установлено с учетом специфики способа продажи товара и направлено на предоставление гражданину - слабой стороне возможности компетентного выбора товара <3>.

<1> Постановления Правительства РФ от 19 января 1998 г. N 55 "Об утверждении Правил продажи отдельных видов товаров, перечня товаров длительного пользования, на которые не распространяется требование покупателя о безвозмездном предоставлении ему на период ремонта или замены аналогичного товара, и перечня непродовольственных товаров надлежащего качества, не подлежащих возврату или обмену на аналогичный товар других размера, формы, габарита, фасона, расцветки или комплектации", от 10 ноября 2011 г. N 924 "Об утверждении перечня технически сложных товаров".

<2> См., например: [Определение](#) Красноярского краевого суда от 29 октября 2015 г. N 4Г-2180/2015; Апелляционные определения Московского городского суда от 12 октября 2015 г. по делу N 33-37508/2015, Волгоградского областного суда от 4 февраля 2015 г. по делу N 33-1340/2015.

<3> [Определение](#) Конституционного Суда РФ от 19 ноября 2015 г. N 2724-О "Об отказе в принятии к рассмотрению жалобы гражданина Романова Романа

Андреевича на нарушение его конституционных прав пунктом 4 статьи 26.1 Закона Российской Федерации "О защите прав потребителей".

В-четвертых, при отказе потребителя от товара в порядке [ст. 26.1](#) Закона о защите прав потребителей продавец должен возратить уплаченную потребителем сумму (за вычетом расходов предпринимателя на доставку возвращенного товара) в течение 10 календарных дней со дня предъявления требования потребителем. Исходя из буквального толкования соответствующего положения указанного [Закона](#), можно прийти к выводу о том, что обязанность по возврату уплаченных сумм должна быть исполнена на основании одного лишь заявления потребителя безотносительно к тому, поступил ли товар обратно во владение предпринимателя. В этой части европейское законодательство также является более сбалансированным, закрепляя не только право потребителя на отказ от товара, но и связанные с ним обязанности, в частности обязанность по своевременному (в течение 14 дней) возврату товара, с которой корреспондирует право предпринимателя удерживать возмещение до получения товара или свидетельств о направлении такового в его адрес ([ст. 13 \(3\), 14 \(1\) Директивы ЕС "О правах потребителей"](#)). В отсутствие схожих положений в российском [Законо](#) о защите прав потребителей для обеспечения баланса интересов сторон можно сослаться на буквальный толкование положения [абз. 5 п. 4 ст. 26.1](#) данного Закона, согласно которому обязанность по возврату уплаченной суммы осуществляется "за исключением расходов продавца на доставку от потребителя возвращенного товара". Таким образом, пока соответствующая доставка не была осуществлена, обязанность по возврату уплаченной

суммы не возникает, в том числе и потому, что нельзя определить ее размер. Данное толкование, конечно, небесспорно, в связи с чем было бы целесообразно уточнить положения [ст. 26.1](#) Закона о защите прав потребителей более детальными положениями на сей счет.

В-пятых, в соответствии с [абз. 5 п. 4 ст. 26.1](#) Закона о защите прав потребителей потребитель, реализующий свое право на отказ от договора, несет бремя расходов на доставку возвращаемого товара в адрес предпринимателя. По смыслу соответствующего положения речь идет о стоимости той доставки, которая была инициирована потребителем уже после принятия им товара. В том случае, когда потребителю доставляется товар и он отказывается от него в момент его доставки, речь идет об услуге доставки заказанного товара, а не об услуге по доставке возвращенного товара. В случае отказа потребителя от товара в момент передачи товара расходы, связанные с доставкой товара, несет предприниматель.

Из положений [ст. 26.2](#) Закона о защите прав потребителей нельзя определить, применяются ли они ко всей совокупности товаров, заказанных потребителем у одного предпринимателя, либо же они могут быть реализованы в отношении каждого отдельного товара, входящего в "пакет". С одной стороны, данная [статья](#) использует формулировку "отказ от товара", а не "отказ от договора", что позволяет говорить о допустимости отказа от отдельных заказанных товаров. С другой стороны, не исключены возможные злоупотребления со стороны потребителей, которые могут разместить заказ на множество товаров, не имея изначально намерения все их приобрести, а с целью организовать возможность выбора подходящего товара из множества магазинов "с доставкой на дом".

Если подобного рода возможность не была оговорена заранее с продавцом и объем заказанных товаров является значительным, что обуславливает достаточно большие затраты предпринимателя на их отбор на складе и последующую доставку, то можно рассматривать такого рода действия покупателя как злоупотребление правом с его стороны. При таких обстоятельствах, в случае отказа предпринимателя от удовлетворения требования о частичном возврате и реализации принципа "все или ничего", данное положение может предоставить некоторую защиту от возможных последующих требований потребителя о неисполнении договора.

Второй вопрос, который возникает на почве реализации права на возврат товара в порядке [ст. 26.1](#) Закона о защите прав потребителей, касается судьбы договоров, которые были заключены в связи с приобретением такого товара, например договоров потребительского кредитования. В Директиве ЕС 2011/83/EU "О правах потребителей" содержится прямое указание на то, что в случае реализации права на отказ от договора утрачивают силу все иные сопутствующие ему договоры ([ст. 15](#)). Российское законодательство содержит схожие положения лишь применительно к способам обеспечения обязательства ^{<1>}. В [Законе](#) о защите прав потребителей нет подобного рода положений в отношении договоров, сопутствующих основному договору купли-продажи, в связи с чем последствия возврата товара на такие договоры необходимо определять отдельно, в соответствии с условиями таких договоров и применимыми к ним нормами законодательства. По общему правилу реализация права на возврат товара, приобретенного в кредит, не влечет автоматического прекращения кредитного договора, неисполнение

потребителем своих обязательств по нему может являться основанием для применения санкций. Кредитный договор может быть досрочно расторгнут, в частности, на условиях [ст. 11](#) Федерального закона "О потребительском кредите (займе)" ^{<2>}. Помимо прочего ими в ней предусматривается право заемщика в течение 14 календарных дней с даты получения потребительского кредита досрочно вернуть всю сумму такого кредита без предварительного уведомления кредитора с уплатой процентов за фактический срок кредитования, а если потребительский кредит был целевой, то соответствующий срок увеличивается до 30 календарных дней. При расторжении договора потребительского кредита в связи с возвратом товара в порядке [ст. 26.1](#) Закона о защите прав потребителей потребитель вправе требовать от предпринимателя вернуть ему сумму первоначального взноса, а от банка - всю остальную уплаченную им сумму за вычетом причитающихся банку процентов.

^{<1>} Прекращение основного обязательства влечет также прекращение обеспечивающего его обязательства, если иное не предусмотрено законом или договором.

^{<2>} Федеральный [закон](#) от 21 декабря 2013 г. N 353-ФЗ "О потребительском кредите (займе)".

Рассмотрев вопросы одностороннего изменения и расторжения договоров с участием потребителей, следует проанализировать, 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. 2 ст. 450.1](#) 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.

<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.

С недавних пор российское право пополнилось рядом положений, которые могут использоваться для противодействия возможным недобросовестным действиям со стороны предпринимательского договора, наделенной правом на одностороннее изменение его условий.

Во-первых, положения [ст. ст. 450](#) и [450.1](#) ГК РФ были дополнены указанием не то, что право на одностороннее изменение условий договора должно

осуществляться с соблюдением требований добросовестности и разумности. 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 с иском к конкретному пользователю 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 правом. 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 признания договора или его части недействительными как противоречащих закону (ст. ст. 10, 168 ГК РФ) <1>. Данное разъяснение предоставляет возможность для признания условия о неограниченном праве на одностороннее изменение договора недействительным, как и всех произведенных на его основе изменений. Также ст. 10 ГК РФ может являться основанием для взыскания убытков, понесенных клиентом в связи с односторонним изменением договора другой стороной, которое представляло собой злоупотребление правом.

<1> См.: п. 9 информационного письма Президиума ВАС РФ от 25 ноября 2008 г. N 127 "Обзор практики применения арбитражными судами статьи 10 Гражданского кодекса Российской Федерации".

Во-первых, поскольку большинство договоров, заключаемых в Интернете, могут быть квалифицированы в качестве договора присоединения (**click-wrap**- и **browse-wrap**-соглашения относятся к ним уже 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. Причем, если иное не установлено законом или не вытекает из существа обязательства, такое изменение или расторжение договора будет являться ретроактивным, т.е. иметь юридический эффект уже с момента заключения договора, тем самым достигая эффекта, схожего с признанием соответствующего условия недействительным. Относительно такого условия, как право на одностороннее изменение договора, применение ст. 428 ГК РФ для противодействия недобросовестному его использованию может быть затруднено тем фактом, что чрезмерно обременительным обычно 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 сначала было санкционировано ВАС РФ <1>, а впоследствии и самим законодателем, исключившим положения п. 3 ст. 428 ГК РФ, содержавшие ограничения использования ст. 428 ГК РФ в предпринимательских договорах.

<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. N 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.

Следует сделать еще одно важное замечание о соотношении вышеприведенных средств защиты. Представляется, что ввиду особого значения для обеспечения прав и охраняемых законом интересов участников гражданского оборота [ст. 10](#) ГК РФ может рассматриваться в качестве сверхимперативной нормы (нормы непосредственного применения, исходя из новой терминологии [ст. 1192](#) ГК РФ), 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. Поэтому [ст. 10](#) ГК РФ и связанные с ней положения [п. 4 ст. 450](#) и [п. 4 ст. 450.1](#) ГК РФ обладают гораздо большим защитным потенциалом в отношении клиентов - российских лиц, несмотря на возможное наличие оговорки об иностранном применимом праве.

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?

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>.

<1> См., например: *Margae, Inc. v. Clear Link Technologies, LLC*. N 2:07-CV-00916-TC, 2008 (D. Utah June 16, 2008); *Moringiello J., Reynolds W. Electronic contracting Cases 2008 - 2009 // The Business Lawyer*. 2009. N 65. 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)).

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, равно как и его обязанности периодически проверять сайт на предмет наличия изменений. Более

того, в соответствии с п. 1 ст. 450.1 ГК РФ право на односторонний отказ от договора полностью или частично может быть осуществлено управомоченной стороной путем уведомления другой стороны, при этом договор прекращается (изменяется) с момента получения такого уведомления, если иное не предусмотрено ГК РФ, другими законами, иными правовыми актами или договором. Таким образом, ГК РФ допускает установление иного, кроме уведомительного, порядка реализации права на одностороннее изменение договора и доведения до сведения другой стороны информации о новых условиях <1>. Таким образом, 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 их изменения в одностороннем порядке с размещением на том же веб-сайте обновленной версии <2>.

<1> Все, что было ранее сказано относительно одностороннего изменения условий договора **mutatis mutandis**, применимо и к определению оснований для одностороннего расторжения договора.

<2> **Постановление** ФАС Московского округа от 31 декабря 2009 г. N КГ-А40/13774-09.

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, однако есть все основания полагать, что в ближайшем будущем эмпирическая нагрузка на них существенно возрастет во многом благодаря электронной коммерции.

Глава 4. ПРОЦЕССУАЛЬНЫЕ АСПЕКТЫ ЭЛЕКТРОННОЙ КОММЕРЦИИ

§ 1. Общие замечания

Ранее уже отмечалось подозрительное отношение отечественных государственных органов к электронным документам, которое бросает самую 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 он был отправлен, 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 не удивительно, что бумага с подписью и печатью воспринимается как полноценное доказательство, а все остальное - с повышенным подозрением.

<1> Smith G. Internet Law & Regulation. Sweet & Maxwell. London. 4th ed. 2007. P. 872.

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 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 Интернета, ничего не стоит... Вместо того чтобы опираться на шаманскую информацию (в оригинале **"voodoo information"**. - **A.C.**) из Интернета, истец должен был охотиться на доказательства в бумажной форме, отвечающей требованиям допустимости" <1>.

<1> 76 F. Supp. 2d 773 (S.D. Tex. 1999).

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>.

<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 "неизвестно ни одного решения, ни одного авторитетного комментария, в которых бы звукозапись предполагаемого разговора была 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, указания первоначального источника компьютерной программы, с использованием которой они были получены, процедур, в соответствии с которыми информация вводилась, а также результатов тестов, подтверждающих точность и надежность электронных устройств. См.: Goode S. The Admissibility of Electronic Evidences // Review of Litigation. 2010. N 29. P. 5.

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" <1>, то подавляющее большинство участников оборота, находящихся под властью российского права и судебной юрисдикции, бродят 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 сфере отношений, возникающих в сети Интернет, имеет тенденцию к расширению. Существует еще и арбитраж, который весьма либерально подходит к вопросам допустимости доказательств.

<1> Иеринг Р. Цель в праве // Избранные труды. СПб., 2006. Т. I. С. 292.

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 процессуальной формы и оставляет перечень средств доказывания, которые можно использовать для установления фактических обстоятельств дела, открытым, 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>.

<1> См.: Арбитражный процесс: Учебник для студентов юридических вузов и факультетов / Под ред. М.К. Треушникова. 3-е изд., испр. и доп. М., 2007.

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 <1>.

<1> Исаенкова О.В. [Некоторые проблемы доказательств](#) и формы их представления в гражданском судопроизводстве // [Налоги](#). 2009. N 17.

Возникает вопрос: к какой категории доказательств относятся электронные сообщения, обмен которыми был осуществлен посредством Интернета, 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 <1>. Электронные документы и сведения с веб-сайтов вполне подпадают под понятие письменного

доказательства, поскольку их основная ценность заключается в их содержании. Правда, наличие у таких цифровых доказательств специфических черт приводит к выводам о том, что они являются письменными доказательствами особого рода <2>.

<1> См.: Боннер А.Т. Традиционные и нетрадиционные средства доказывания в гражданском и арбитражном процессе. М., 2013. С. 113.

<2> [Справочник по доказыванию](#) в гражданском судопроизводстве / Под ред. И.В. Решетниковой. 5-е изд., доп. и перераб. М., 2011. С. 45.

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 <1>.

<1> [Там же](#). С. 24.

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 <1>.

<1> [Практика применения Арбитражного процессуального кодекса](#) Российской Федерации / Отв. ред. И.В. Решетникова. 2-е изд., перераб. и доп. М., 2012.

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 <1>.

<1> Гражданский процесс / Под ред. В.В. Яркова. М., 2012. С. 223.

Рассмотрим, какие требования предъявляются к различным доказательствам в электронной форме,

которые могут иметь значение в контексте электронной коммерции.

§ 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 **ч. 3 ст. 75 АПК** РФ документы, полученные посредством факсимильной, электронной или иной связи, в том числе с использованием Интернета, 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 Верховным Судом 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, которые предусмотрены законом, иными правовыми актами или соглашением сторон".

В случаях, когда электронное сообщение, а точнее, документ, отправленный средствами электронной почты контрагенту, подписано 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.

<1> Под электронной цифровой подписью в данном случае имеются в виду электронная цифровая подпись по [Закону](#) об ЭЦП и усиленная квалифицированная подпись по [Закону](#) об ЭП.

Поскольку электронная цифровая подпись признается равнозначной собственноручной подписи лишь при определенных условиях <1>, помимо собственно электронного документа необходимо представить доказательства, подтверждающие соблюдение таких условий.

<1> См.: [ст. 11](#) Закона об ЭП, а также [ст. 4](#) Закона об ЭЦП.

Так, поскольку одним из таких условий является

действительность сертификата подписи на момент подписания документа, то должен быть представлен 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.

<1> См., например: [Постановление](#) ФАС Волго-Вятского округа от 11 августа 2010 г. по делу N А43-5226/2010.

Другим условием юридической силы электронной цифровой подписи является положительный результат проверки действительности электронной цифровой подписи. Для подтверждения подлинности ЭЦП необходимо обратиться в удостоверяющий центр выдавший соответствующий сертификат, с заявлением 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 представил 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, включаются: 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 утраты), бумажная копия такого договора должна содержать сведения о проверке и подтверждении подлинности такой подписи <1>.

<1> [Постановление](#) ФАС Московского округа от 10 апреля 2012 г. по делу N А40-74288/11-141-615.

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 содержал прямое указание на то, что он не распространяется на иные аналоги собственноручной подписи. В то же время специальных законов или иных правовых актов, регламентирующих 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 по определению 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 Интернета, 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 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 были высланы по электронной почте программа форума и пригласительные билеты. Факт участия представителей ответчика в форуме подтверждался регистрационным листом и фотоотчетом. Суд отказал в иске о взыскании стоимости оказанных услуг, сославшись на то, что представленных доказательств недостаточно 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 представлен оригинал, а копия не содержит "необходимых реквизитов документа (даты, номера), предусмотренных Государственным [стандартом](#) ГОСТ Р 51141-98" <1>.

<1> [Постановление](#) Девятого арбитражного апелляционного суда от 15 марта 2012 г. N 09АП-4617/2012-ГК по делу N А40-62542/11-87-479.

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 [Закон](#) об ЭП, который должен был способствовать развитию электронной коммерции и преодолению недостатков [Закона](#) об ЭЦП. И действительно, в отличие от [Закона](#) об ЭЦП [Закон](#) об ЭП предусматривает уже три типа электронной подписи: простая электронная подпись, усиленная неквалифицированная электронная подпись и усиленная квалифицированная электронная подпись (аналог электронной цифровой подписи, предусмотренной [Законом](#) об ЭЦП). 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. Примером служит следующая цитата из судебного решения: "Стороны ни в договоре, ни в приложении к нему не предусмотрели саму возможность обмена письмами посредством электронной почты (в том числе получение каких-либо документов посредством электронной почты), не 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> Постановления Девятого арбитражного апелляционного суда от 12 декабря 2014 г. [N 09АП-51179/2014-ГК](#) по делу N А40-183574/2013, от 18 апреля 2014 г. [N 09АП-10830/2014-ГК](#) по делу N А40-78449/2013, от 24 февраля 2012 г. по делу [N А40-93546/11-1-548](#). См. также: решение Арбитражного суда г. Москвы от 16 октября 2015 г. по делу N А40-148805/2015; Постановления Девятого арбитражного апелляционного суда от 20 июля 2015 г. [N 09АП-24987/2015](#) по делу N А40-202666/14, Третьего арбитражного апелляционного суда от 25 июля 2012 г.

по делу [N A33-543/2012](#), ФАС Уральского округа от 20 октября 2015 г. по делу [N A60-54628/2014](#), ФАС Центрального округа от 18 марта 2010 г. [N Ф10-561/10](#) по делу N A35-3401/2009.

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>.

<1> Ворожбит С.П. [Проблемы представления и исследования](#) электронных почтовых сообщений в арбитражном процессе // Арбитражный и гражданский процесс. 2010. N 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.

Не удивительно, 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" <1>. Иногда суды принимают электронную переписку в качестве доказательств и в отсутствие специальных положений в договоре, если другая сторона не сделала заявление о фальсификации доказательств <2> 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 <3>.

<1> [Постановление](#) ФАС Центрального округа от 21 января 2010 г. N Ф10-5994/09 по делу N А14-3050/2009/122/15. [Определением](#) ВАС РФ от 15 марта 2010 г. N ВАС-2621/10 отказано в передаче дела N А14-3050/2009/122/15 в Президиум ВАС РФ для пересмотра в порядке надзора данного [Постановления](#).

<2> [Постановление](#) ФАС Дальневосточного округа от 16 марта 2010 г. N Ф03-1209/2010 по делу N А59-3597/2009.

<3> [Определение](#) ВАС РФ от 15 марта 2010 г. N ВАС-2621/10 по делу N А14-3050/2009-122/15. См. также: Постановления ФАС Северо-Западного округа от 1 июня 2010 г. по делу [N А56-13328/2009](#), Девятого арбитражного апелляционного суда от 5 октября 2009 г. [N 09АП-15486/2009-ГК](#) по делу N А40-48586/09-48-349.

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 <1>.

<1> В [Постановлении](#) ФАС Северо-Кавказского округа от 8 августа 2012 г. по делу N А53-11601/2011 отмечено, что "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".

Значительный прогресс в использовании судами переписки по электронной почте в качестве доказательства стал наблюдаться после принятия [Постановления](#) Президиума ВАС РФ от 12 ноября 2013 г. N 18002/12, в котором была сформулирована поистине революционная правовая позиция, согласно

которой "отсутствие соглашения об обмене электронными документами между сторонами переписки, а равно отсутствие электронной цифровой подписи в отправляемых и получаемых документах (даже при наличии такого соглашения) не являются нарушением требований закона (в смысле [части 2 статьи 50 Конституции Российской Федерации](#) и [части 3 статьи 64 АПК РФ](#)) при доказывании неправомерных действий, в связи с чем не влекут безусловную невозможность использования соответствующих документов и материалов в качестве доказательств".

Несмотря на то что данное дело касалось нарушений в сфере антимонопольного законодательства (запрещенная законом координация деятельности хозяйствующих субъектов), т.е. публично-правовых отношений, суды распространяют эту позицию и на случаи нарушения договорных обязательств. Например, в одном из дел претензии к стороне по договору в отношении уведомления о готовности товара к отгрузке, высланные на электронный адрес этой стороны, но проигнорированные ею, были признаны надлежащим доказательством со ссылкой на позицию ВАС РФ о допустимости электронных документов в качестве доказательств неправомерных действий и в отсутствие заключенного соглашения об обмене такими документами <1>.

<1> [Постановление](#) Седьмого арбитражного апелляционного суда от 2 марта 2016 г. по делу N А45-13442/2015.

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, либо если такая сторона допустила нарушение законодательства, факт которого может подтвердить оспариваемый ею электронный документ.

Однако во избежание возможных споров 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 ^{<1>}, наличие таких положений в договоре, пусть и заключенном в электронной среде, более предпочтительно, нежели их полное отсутствие.

^{<1>} **Постановление** ФАС Московского округа от 28 декабря 2011 г. по делу N 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". См. также Апелляционное **определение** Нижегородского областного суда от 21 июля 2015 г. по делу N 33-7141/2015, в котором говорится, что "переписку посредством факсимильной связи и электронной почты суд правомерно признал обычаем делового оборота (**ст. 5** Гражданского кодекса РФ), так как стороны фактически признали приемлемым

обмен письменными документами и признание их содержания. Содержание деловой переписки сторонами не оспаривалось"; **Постановление** ФАС Восточно-Сибирского округа от 3 июня 2014 г. по делу N А33-15050/2013 констатировало: "Ни законодательно, ни соглашением сторон требования к документированию информации по спорным правоотношениям не установлены. При этом суды обоснованно учли сложившиеся взаимоотношения сторон по обмену электронными письмами без проставления электронной подписи".

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 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, действий (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. 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>.

<1> Малинина Е.С. [Электронное сообщение как доказательство](#) по делу в арбитражном судопроизводстве // Администратор суда. 2009. N 2.

<2> Боннер А.Т. Указ. соч. С. 512.

В [АПК РФ](#) отсутствуют требования относительно формы представления электронных документов в качестве доказательств. Однако на основании [ст. 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 <1>. 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 представить их в

нотариально заверенной форме (т.е. в виде протокола осмотра нотариусом информации на мониторе компьютера).

<1> См., например: [Определение ВАС РФ от 23 апреля 2010 г. N ВАС-4481/10](#); Постановления ФАС Московского округа от 20 мая 2010 г. [N КГ-А40/4455-10](#), ФАС Северо-Западного округа от 1 июня 2010 г. по делу [N А56-13328/2009](#), ФАС Центрального округа от 21 января 2010 г. [N Ф10-5994/09](#); Апелляционные определения Московского городского суда от 30 января 2013 г. по делу [N 11-3198/2013](#), Хабаровского краевого суда от 3 апреля 2015 г. по делу [N 33-1632/2015](#).

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 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>.

<1> См., например: [Постановление](#) ФАС Московского округа от 30 ноября 2009 г. N 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 N А-75-6285/2010.

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 <1>.

<1> 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.

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 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:

<1> Данный электронный адрес не принадлежит

автору и приведен лишь в качестве примера того факта, что под ним может скрываться кто угодно.

- 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 <1>;

<1> См. подробнее: Галяшина Е.И. [Речеведческие экспертизы в судопроизводстве](#) // Законы России: опыт, анализ, практика. 2011. N 12.

- 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 представленных 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 **mircrosoft.ru** с 5 декабря 2010 г. 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, переписке в электронном виде, находящейся в электронном почтовом ящике общества. Обществом были предоставлены суду логин и пароль для входа в электронный почтовый ящик. Суд изучил электронную переписку, осуществленную с почтового ящика **mailsvb@mail.ru** на принадлежащий ответчику почтовый ящик **liccilip@gmail.com**, и признал имеющиеся в материалах дела документы идентичными их электронным версиям.

В итоге суд пришел к выводу о том, что общество привело надлежащие доказательства, свидетельствующие о ведении между сторонами электронной переписки по вопросам согласования характеристик сайта, предоставления 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 представления 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 соответствующего содержания между сторонами, представленной ответчиком в вышеуказанные даты) <1>.

<1> [Постановление](#) Первого арбитражного апелляционного суда от 23 декабря 2011 г. по делу N А43-9577/2011, оставленное без изменения [Постановлением](#) ФАС Волго-Вятского округа от 18 апреля 2012 г.

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 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 звонка 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.

<1> Shao Dali v. Zhang Ershen Beijing First Intermediate People's Court, January 2001. См.: Wang M. Electronic Evidence in China // Digital Evidence and Electronic Signature Law Review. 2008. N 5. P. 48.

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 <1>. В связи с этим имеет смысл несколько уточнить высказывание А.Т. Боннера, который хотя и признает наличие в электронном адресе реквизитов, идентифицирующих электронный документ, но отмечает, что "такого рода реквизиты не позволяют с достоверностью установить отправителя электронного документа" <2>. 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).

<1> 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.

<2> Боннер А.Т. Указ. соч. С. 510.

Данный подход разделяется судебной практикой ВАС РФ и Верховного Суда РФ. В упоминавшемся ранее [Постановлении](#) Президиума ВАС РФ от 12 ноября 2013 г. N 18002/12 указано, что "получение или отправка сообщения с использованием адреса электронной почты, известного как почта самого лица или служебная почта его компетентного сотрудника, свидетельствует о совершении этих действий самим лицом, пока им не доказано обратное". Этот подход отражается и в практике Верховного Суда РФ, в одном из постановлений которого указано, что "общество как владелец (администратор) домена с соответствующим именем отвечает за любые действия, совершенные с использованием такого домена, в том числе за направление с его использованием электронных сообщений" <1>.

<1> [Постановление](#) Верховного Суда РФ от 24 апреля 2015 г. N 305-АД15-2693 по делу N А40-36625/2014.

Находит этот подход свое развитие и в арбитражной практике. Так, в одном из решений электронный адрес корпоративной почты был приравнен к электронной подписи и на этом основании был признан допустимым доказательством. Как отметил суд, "довод о том, что электронная переписка не имеет электронной подписи, в связи с чем не может быть принята как доказательство, отклоняется. В электронных адресах Цоя, Шубниковой и Орловой после символа "@" указано "isl.su". Подписи в электронных письмах содержат наименование компании ответчика, адрес и телефоны. Принадлежность данных электронных адресов ответчику подтверждается актом

осмотра сайта ЗАО "Региональный Сетевой Информационный Центр" (RU-CENTER). Данный домен зарегистрирован на имя Цоя Андрея Анатольевича, т.е. генерального директора общества. Таким образом, при переписке с названными лицами у компании не могло возникнуть сомнения в полномочиях лиц заключить сделку от имени ответчика. Тем более что в дальнейшем все договоренности сопровождались конклюдентными действиями сторон" <1>.

<1> [Постановление](#) ФАС Северо-Кавказского округа от 27 июля 2015 г. по делу N A32-19429/2014.

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, 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 <1>.

<1> [Постановление](#) ФАС Восточно-Сибирского округа от 18 февраля 2011 г. N A33-3344/2010. 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 явствовало из обстановки ([абз. 2 п. 1 ст.](#)

Установив факт принадлежности определенного электронного почтового ящика, на который 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 <1>. 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 Интернета, будет сказано далее.

<1> См. подробнее: Бегичев А.В. Обеспечение доказательств нотариусами: теория и практика. М., 2013. С. 197.

В рамках действующего процесса возможно заявление ходатайства об осмотре содержимого почтового ящика в порядке [ст. 78 АПК РФ](#), [ст. 58 ГПК РФ](#) <1>. К такому осмотру для оказания консультаций, непосредственной технической помощи при осмотре возможно привлечение специалиста, обладающего специальными знаниями в области информационных

технологий.

<1> См., например: Апелляционное [определение](#) Новосибирского областного суда от 30 июля 2015 г. по делу N 33-6464/2015, в котором сказано: "Более того, истец неоднократно настаивал на обзрении судом оригиналов переписки в персональном компьютере, от чего суд необоснованно отказался".

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 коти́ровочной заявкой, 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 коти́ровок. 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>.

<1> Решение арбитражного суда Хабаровского края от 2 апреля 2012 г. по делу N А73-1608/2012, оставленное без изменения [Постановлением](#) Шестого арбитражного апелляционного суда от 27 июня 2012 г. N 06АП-2252/2012.

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. Существуют прецеденты, в которых суды достаточно лояльно подходили к принятию распечаток лог-файлов провайдера <1>.

<1> В [Постановлении](#) ФАС Московского округа от 6 февраля 2013 г. по делу N А40-68757/11-42-562 установлено следующее: "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)".

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-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, которые лучше всего представлять в форме протокола осмотра нотариусом содержимого почтового ящика. В случае невозможности их 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](#)). Иногда суды толкуют положения [п. 6 ст. 71 АПК РФ](#) весьма формально и ограничительно ("до третьей запятой") и вовсе отказывают в приобщении к материалам дела копии документа по причине отсутствия его оригинала.

<1> Правовые аспекты использования интернет-технологий / Под ред. А.С. Кемрадж, Д.В. Головерова. С. 101.

Следует отметить, что предпочтение подлинных документов копиям свойственно не только российскому праву. Например, англо-американскому процессуальному 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 <1>. 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.

<1> Black's Law Dictionary, Thomson Reuters. 9th ed. 2011. P. 635.

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 намеревалось придать такую же юридическую силу. Если данные хранятся в компьютере или другом подобном устройстве, то подлинником письменного материала или записи будут являться любая распечатка или иной способ их представления в форме, доступной

для прочтения человеком, точно отражающей эти данные <1>.

<1> Federal Rules of Evidence, Rule 1003.

Аналогичных положений в российском законодательстве нет, как, впрочем, и законодательной дефиниции понятий "подлинник" и "копия". Исходя из положений [ГОСТа Р 51141-98](#) подлинником является первый или единичный экземпляр документа. Аналогичное положение закреплено в [п. 3.2](#) ГОСТа 6.10.4-84 относительно документа на машинном носителе <1>. 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 <2>.

<1> Карев Я.А. [Указ. соч.](#) С. 142.

<2> 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. N 6. С. 98.

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" <1>.

<1> Косовец А.А. Правовое регулирование электронного документооборота // Вестник Московского университета. Сер. 11: Право. 1997. N 4. См. также: Карев Я.А. [Указ. соч.](#) С. 144.

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 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 доказательства

в гражданском и арбитражном процессе

При рассмотрении споров, возникающих в сфере электронной коммерции, неизбежно встает вопрос о процессуальном статусе информации, содержащейся на веб-сайтах в сети Интернет. Необходимость ее представления в суд может обуславливаться, к примеру, необходимостью анализа договорных условий или их части, изложенных на веб-сайте, или размещенной информации о товаре (услуге) 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 Интернета, 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, расположенных 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 доказательств, тот факт, что информация, полученная из Интернета, имеет доказательственное значение как в судах общей юрисдикции, так и в арбитражных судах, не вызывает сомнений <4>. Ключевой вопрос заключается в том, в каком виде ее представить в суд.

<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]. 74.

<3> Боннер А.Т. Указ. соч. С. 527.

<4> Там же. С. 519 - 522, 532.

В американской судебной практике распечатки с официальных веб-сайтов принимаются в качестве доказательств при условии, что они содержат **URL** и дату распечатки <1>. 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 аффидевита от лица, которое обладает таким знанием (**someone with knowledge**). В некоторых случаях суды требуют, чтобы такое заявление исходило от владельца сайта <2>. Правда, как отмечается в американской литературе, в большинстве случаев суды относятся более либерально к условиям допустимости распечаток страниц веб-сайтов <3>. 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 <4>. 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 <5>. Распечатки с сайтов официальных органов принимаются в качестве доказательства без необходимости представления дополнительных доказательств их подлинности в порядке правила 902 (5) <6> Федеральных правил о доказательствах.

<1> U.S. Equal Emp't Opportunity Comm'n v. E.I. DuPont De Nemours & Co., N 031605, 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. N ВАС-16311/11 по делу N 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 распечатки - 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".

<2> Costa v. Keppel Singmarine Dockyard PTE, Ltd. (C.D. Cal. 2003); United States v. Jackson, 208 F.3d (7th Cir. 2000).

<3> Goode S. Op. cit. P. 14.

<4> Jarritos, Inc. v. Los Jarritos, N C-05-02380 (N.D. Cal, 2007) revised on other grounds (9th Cir. 2009). См. также: Kassouf v. White (Ohio App. 2000).

<5> Telewizja Polska USA, Inc. v. EchoStar Satellite Corp. N 02 C 3293 (N.D. Ill. 2004).

<6> Данный пункт содержит указание о том, что официальные публикации государственных органов "свидетельствуют сами о себе" (**self-authenticating**).

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 <1>. 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.

<1> Юзефович В.Б. [Доказательства и доказывание](#) в арбитражном процессе: анализ

правоприменительной практики. Выводы судебного юриста. М., 2012. С. 63.

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 Интернете). 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 [<1>](#). На доказательственный характер распечатки страницы с веб-сайта указано и в [Постановлении](#) Пленума ВАС РФ от 17 февраля 2011 г. N 12: 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 обновления этих сведений [<2>](#).

[<1> Постановление](#) ФАС Западно-Сибирского округа от 30 августа 2011 г. N А70-23/2011.

[<2> Постановление](#) Пленума ВАС РФ от 17 февраля 2011 г. N 12 "О некоторых вопросах применения Арбитражного процессуального кодекса Российской Федерации в редакции Федерального закона от 27 июля 2010 г. N 228-ФЗ "О внесении

изменений в Арбитражный процессуальный кодекс Российской Федерации".

Как отмечается, суды общей юрисдикции также все более активно принимают распечатки с сайтов в качестве доказательств доставки почтового отправления (сайт Почты России), в качестве доказательств места нахождения организации (сайт Федеральной налоговой службы) <1>.

<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. N 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 <1>, что обеспечивает достаточную гарантию аутентичности содержимого таких веб-сайтов.

<1> Требования о защите информации, содержащейся в информационных системах общего пользования, утв. Приказом ФСБ России и ФСТЭК от 31 августа 2010 г. N 416/489, п. 17.

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 <1>. В связи с этим имеет смысл позаботиться о придании такой распечатке дополнительной убедительности. Это может быть реализовано путем судебного или нотариального обеспечения доказательств.

<1> [Постановление](#) ФАС Московского округа от 5 февраля 2013 г. по делу N A40-135406/11-19-276: 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. N Ф09-9858/11 по делу N A76-2698/2011.

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 доказательств впоследствии будет невозможным и затруднительным. Поскольку информация в Интернете 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>.

<1> Это не означает, что суд готов удовлетворять все ходатайства об обеспечении доказательств, размещенных в Интернете. См., например: [Постановление](#) ФАС Московского округа от 29 июля 2009 г. N КГ-А40/6565-09 по делу N 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. N 78 "Обзор практики применения арбитражными судами предварительных обеспечительных мер". Пример удовлетворения подобного заявления см.: Определение арбитражного суда Свердловской области от 10 сентября 2015 г. по делу N А60-30404/2015.

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 Интернете 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 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 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>.

<1> [Письмо](#) ФНП от 13 января 2012 г. N 12/06-12 "Об обеспечении нотариусом доказательств" // Нотариальный вестник. 2012. N 4.

Действуя в соответствии с [п. 18 ст. 35, ст. ст. 102 - 103](#) Основ законодательства 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.

Какой-либо единообразной процедуры осмотра страницы веб-сайта в настоящее время не существует, поэтому она может варьироваться от нотариуса к нотариусу. Как правило, 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 <1>. 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.

<1> См. подробнее: Бегичев А.В. Указ. соч. С. 176 - 178.

Специалистами в области нотариата отмечается, что обширное применение технических мер при оценке достоверности расположения искомого веб-сайта по определенному адресу не в полной мере вписывается 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 лицо, обладающее специальными познаниями в области компьютерных технологий. Вместе с тем в судебной практике встречаются случаи, когда сторона пытается признать протокол нотариального осмотра сайта недопустимым доказательством по причине непроведения нотариусом вышеуказанных "подготовительных мероприятий" <2>.

<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> См., например: [Постановление](#) Суда по интеллектуальным правам от 28 января 2015 г. N C01-1286/2014 по делу N A40-169281/2013. В нем говорится: "...ответчик считает, что нотариальный протокол осмотра письменного доказательства от 02.07.2013 является неотнотимым, недопустимым и недостоверным доказательством по делу, поскольку нотариус не известил общество "ДревГрад" (ОГРН 1107746211000) о времени и месте обеспечения доказательств, отсутствует подтверждение действительности соединения нотариуса с сайтом www.derev-grad.ru, не указано, с помощью какого специального лицензионного программного обеспечения нотариус осуществлял выход на указанный

сайт для его осмотра, наименование интернет-провайдера, а также неясно, имелись ли у нотариуса специальные познания для осуществления указанного нотариального действия". Суд, правда, не высказал своей позиции по сути данного заявления, признав тем не менее протокол осмотра сайта допустимым доказательством.

В случае если содержание сайта изложено на иностранном языке, 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 <1>.

<1> Бегичев А.В. Указ. соч. С. 195.

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 становятся известны 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 <1>.

<1> Лещенко А.И., Лещенко А.И. [Актуальные вопросы обеспечения доказательств нотариусом](#) // Закон. 2008. N 9; Юзефович В.Б. [Указ. соч.](#) 2012. С. 65.

Пока соответствующие изменения не внесены, однако правоприменительная практика уже идет по пути следования этим рекомендациям. Так, в указанном ранее [письме](#) ФНП отмечается, что, "поскольку 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>.

<1> [Письмо](#) ФНП от 13 января 2012 г. N 12/06-12 "Об обеспечении нотариусом доказательств" // Нотариальный вестник. 2012. N 4.

<2> Постановления: ФАС Северо-Западного округа от 10 февраля 2011 г. по делу [N A56-14567/2010](#), ФАС Московского округа от 21 мая 2010 г. N [КГ-А40/4810-10](#) по делу N A40-10765/09-93-112; [Определение](#) Санкт-Петербургского городского суда от 20 июня 2011 г. N 33-9194/2011.

Ранее действовавшая редакция [ч. 2 ст. 102](#) Основ законодательства о нотариате не допускала возможности обеспечения нотариусом доказательств по делам, находящимся в производстве суда. Считалось, что данная норма является следствием соблюдения принципа непосредственности судебного разбирательства, закрепленного в [ч. 1 ст. 10](#) АПК РФ, согласно которому арбитражный суд при разбирательстве дела обязан непосредственно исследовать все доказательства по делу <1>, а также следствием наличия процедуры обеспечения доказательств непосредственно в [ГПК РФ](#) <2>.

<1> [Постановление](#) ФАС Московского округа от 11 сентября 2012 г. по делу N А40-111324/11-141-944.

<2> Как отмечено в [п. 7](#) Пленума Верховного Суда РФ от 15 июня 2010 г. N 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, не ограничен ([ст. ст. 64 - 66](#) ГПК РФ).

В этой связи арбитражные суды нередко признавали недопустимыми доказательства, обеспеченные нотариусом по заявлению заинтересованных лиц, в то время как дело, по которому обеспечено доказательство, находилось в производстве суда <1>.

<1> Постановления Девятого арбитражного апелляционного суда от 12 апреля 2010 г. [N 09АП-4914/2010-ГК](#) по делу N А40-72761/09-8-542, ФАС Московского округа от 15 августа 2012 г. по делу [N А40-118696/11-27-1014](#).

С 1 января 2015 г. [ч. 2 ст. 102](#) Основ законодательства о нотариате была исключена. Таким образом, в настоящее время нотариальный осмотр веб-сайта в Интернете возможен и в рамках уже рассматриваемого в суде спора. Кроме того, ГПК РФ пополнился еще одной важной нормой, которая гласит: "Обстоятельства, подтвержденные нотариусом при

совершении нотариального действия, не требуют доказывания, если подлинность нотариально оформленного документа не опровергнута в порядке, установленном [статьей 186](#) настоящего Кодекса, или не установлено существенное нарушение порядка совершения нотариального действия" ([ч. 5 ст. 61](#) ГПК РФ). Таким образом, если не доказана поддельность (подложность) нотариально оформленного документа или не доказано, что нотариусом допущены нарушения порядка совершения нотариального действия, причем только такие, которые имели существенное значение для соответствующего нотариального действия, никто не вправе произвольно требовать дополнительного подтверждения фактов, установленных и подтвержденных нотариусом. Данная норма закрепляет повышенную доказательную силу нотариально удостоверенных фактов.

В качестве альтернативы нотариальному осмотру возможна подача заявления об обеспечении доказательств 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 Интернете, может являться основанием для отмены вынесенного решения и направления дела на новое рассмотрение ^{<1>}. На возможность проведения судом осмотра размещенной в Интернете 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. ст. 58 и 184](#) ГПК РФ (с извещением

участвующих в деле лиц, с фиксированием результатов в протоколе, с привлечением при необходимости специалиста) <2>.

<1> **Постановление** ФАС Московского округа от 10 сентября 2012 г. по делу N А40-101177/11-34-904.

<2> **Пункт 7** Пленума Верховного Суда РФ от 15 июня 2010 г. N 16 "О практике применения судами Закона РФ "О средствах массовой информации".

Применительно к доказательствам, полученным из Интернета, 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"), посредством которого осуществляются 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>.

<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>.

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 <1>.

<1> С полным перечнем участников указанного консорциума можно ознакомиться на его официальном интернет-сайте:

<http://www.netpreserve.org/about-us/members>.

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 <1>, канадскими <2>, немецкими <3> 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**) <4>.

<1> 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.

<2> *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*, 2007 FC 411 (CanLII); *St. Joseph Media Inc. v. Starwood Hotels & Resorts Worldwide, Inc.*, 2010 TMOB 188 (CanLII).

<3> *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.

<4> 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_decision.s.jsp?q=-Wayback+Machine&start=20.

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 <1> или, напротив, в качестве доказательства отсутствия факта такого исполнения <2>, поскольку данные интернет-архива позволяют проследить динамику изменений, происходящих на веб-сайте применительно к определенным датам.

<1> **Постановление** Девятого арбитражного апелляционного суда от 7 августа 2008 г. по делу N А40-985/08-112-4.

<2> **Постановление** Одиннадцатого арбитражного апелляционного суда от 18 июля 2013 г. по делу N 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.

Данные из интернет-архива **Wayback Machine** позволяют отследить факт использования сайта в течение определенного периода времени <1>. В связи с этим достаточно часто данные из интернет-архива **Wayback Machine** использовались сторонами арбитражного процесса в спорах, связанных с нарушением товарных знаков. В частности, в качестве доказательства, подтверждающего факт использования товарного знака правообладателем (корпорацией **Mozilla**) <2>; факт использования доменного имени для осуществления деятельности, аналогичной той, в

отношении которой был зарегистрирован товарный знак <3>.

<1> Так, в **Постановлении** Двадцатого арбитражного апелляционного суда от 7 августа 2015 г. по делу N A68-8818/2014 говорится: "В спорный период (сентябрь 2013 года и декабрь 2013 года) компания с теми же телефонами, что сейчас использует истец, занималась реализацией торговых автоматов, что подтверждается распечаткой сайта <http://torgovie-avtomaty.ru> на сентябрь 2013 года и декабрь 2013 года, полученной из открытого архивного интернет-сервиса Internet Archive. Wayback Machine (<http://web.archive.org/>), содержащего выборочный архив версий сайтов в сети Интернет. Данные сведения находятся в открытом доступе. Кроме этого, данные распечатки сайта (в нижней части) содержат информацию о том, что создание сайта и его продвижение осуществляет ответчик".

<2> Решение Арбитражного суда г. Москвы от 14 сентября 2012 г. по делу N A40-8334/12.

<3> Решение Арбитражного суда г. Москвы от 11 июля 2013 г. по делу N A40-26695/13.

Приведенные судебные решения позволяют сделать вывод, что как зарубежные суды, так и отечественные арбитражные суды в общем 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 доказательств 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. Примечательно, что ФАС России прямо указывает в своих разъяснениях на возможность использования "результатов поиска в архиве Интернета (<https://archive.org/web/>) в качестве доказательств в делах, связанных с нарушением законодательства о рекламе" <1>.

<1> **Письмо** ФАС России от 28 августа 2015 г. N АК/45828/15 "О рекламе в сети Интернет".

Глава 5. ВЕБ-САЙТ КАК ОСНОВНОЙ ИНСТРУМЕНТ ЭЛЕКТРОННОЙ КОММЕРЦИИ

§ 1. Понятие веб-сайта. Его правовая природа и особенности регулирования

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>.

<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. N 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.

Под веб-сайтом обычно понимают совокупность электронных документов (файлов), объединенных под одним адресом (доменным именем и (или) **IP**-адресом). При этом веб-сайт является сложным объектом, состоящим из различных компонентов. К числу таких компонентов обычно принято относить: 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 специальных языков -

HTML (HyperText Markup Language), который отвечает за логическую структуру страницы, **CSS (Cascading Style Sheets)**, отвечающий за ее внешний вид, и др. В результате создается код, который впоследствии 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.

<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. Следует отметить, что в последнее время **HTML-язык** все меньше используется при создании страниц интернет-сайтов, по причине того что он ориентирован на статический контент. Получающие все большую популярность динамические страницы интернет-сайта, формирующиеся в процессе исполнения запроса пользователя и с учетом его индивидуальных характеристик, создаются движком веб-сайта или специальной компьютерной программой на сервере.

Интернет-магазины и сложные интерактивные сайты в сети Интернет нередко состоят из трех основных компонентов: 1) презентационного слоя (**presentation layer**); 2) слоя бизнес-логики (**logic layer**) и 3) слоя баз данных (**data layer**). Презентационный слой представляет собой клиентскую часть интернет-сервиса - веб-сайт, с которым

взаимодействует пользователь. Слой бизнес-логики представляет собой отдельный сервер, на котором содержатся приложения, обеспечивающие основной бизнес-функционал сервиса (функционал размещения заказа, оплаты и пр.). Слой баз данных доступен только с сервера приложения и содержит информацию о клиентах, совершенных транзакциях, товарах и т.д. После получения запроса с сервера приложения необходимая информация извлекается и передается для обработки на сервер приложения, а оттуда - пользователю. Подобная трехуровневая структура позволяет обеспечить повышенную безопасность интернет-сервиса (взлом клиентской части сервиса не влечет взлома сервера приложения и баз данных, которые представляют основную коммерческую ценность), а также масштабируемость сервиса за счет возможности более гибкого использования облачных сервисов. С юридической точки зрения данный подход означает, что, помимо четырех компонентов веб-сайта, рассмотренных ранее и относящихся к клиентской части веб-сайта (презентационному слою), сайт также будет включать в себя отдельный сервер приложений, в котором вопросы дизайна не так важны из-за того, что он не виден пользователю, но где сконцентрирован весь функционал интернет-сервиса, а также системы управления базами данных (СУБД) и сами данные. Все это накладывает отпечаток не только на договоры, связанные с разработкой таких сайтов, но и на количество объектов интеллектуальной собственности, входящих в их состав, на которые необходимо приобрести должный объем прав.

Для определения особенностей правового регулирования веб-сайта необходимо разграничивать частноправовые аспекты его регулирования, выражающиеся главным образом в определении его правового статуса как объекта гражданских прав, а

также публично-правовые аспекты, регламентирующие его место в системе законодательства об информации.

Гражданско-правовой статус веб-сайта

Долгое время в российском законодательстве отсутствовала легальная дефиниция понятия "веб-сайт", что спровоцировало шквал дискуссий на тему правовой природы веб-сайта <1>. Вся совокупность точек зрения по данному вопросу, существовавших до введения в действие части четвертой ГК РФ, можно свести к следующим трем <2>:

<1> Определение правовой природы того или иного технического или социального явления, нередко сопровождающееся выработкой его легальной дефиниции, представляет собой способ, посредством которого 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.

<2> Близнец И., Робинов А. Правовой статус гипертекстовых документов и целесообразность их регистрации в Роспатенте // Интеллектуальная

собственность. Авторское право и смежные права. 2002. N 7.

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) <1>. Поскольку совокупность 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 <2>. 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

его подвергаются не только материалы, размещенные непосредственно на нем, но и материалы, размещенные на других сайтах, что становится возможным за счет механизма гиперссылок <3>;

<1> Следует отметить отличительную особенность российского подхода к регулированию баз данных, ограничивающего данное понятие лишь электронными базами 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)).

<2> Петровский С. [Защита прав автора сайта](#) // Российская юстиция. 2001. N 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. N 1. См. также: Серго А. Интернет и право. М., 2003. С. 93. О целесообразности квалификации веб-сайта в качестве базы данных заявляет и В.О. Калятин (Калятин В.О. Право в сфере Интернета. С. 94 - 95).

<3> См.: Басманова Е.С. Интернет-сайт как объект имущественных прав: Дис. ... канд. юрид. наук. М., 2010. С. 110.

3) веб-сайт является объектом особого рода sui generis, состоящим из различных видов

информации <1>. Или в ином варианте: "особой формой организации электронной информации" <2>.

<1> 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.

<2> Гулак А.С. Место сайта сети Интернет в системе объектов гражданских правоотношений // Вестник Удмуртского университета. 2006. N 6.

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 <1>. 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 позволяют 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 <2>.

<1> Graham Smith. Op. cit. P. 760.

<2> См.: Басманова Е.С. Указ. соч. С. 61. Хотя, если веб-сайт будет состоять из динамических страниц, то оснований для возможной его квалификации в качестве программы для ЭВМ становится гораздо больше.

Что касается третьего варианта квалификации, то он является весьма привлекательным 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 <1>. 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 <2>.

<1> 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**.

<2> См.: Басманова Е.С. Указ. соч. С. 58.

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 <1>. В случае установления факта наличия существенных финансовых, материальных, организационных или иных затрат, понесенных при создании веб-сайта (презюмируемого при наличии не менее 10000 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. Уже сейчас можно найти отдельные решения, в которых обнаруживается сочувствие судов к данной позиции. Например, в качестве базы данных суд квалифицировал совокупность информации, размещаемой в социальной сети в течение продолжительного периода времени: **"По смыслу нормы абзаца 2 пункта 1 статьи 1334 ГК РФ несанкционированное администрирование**

лицом в своих интересах группы в социальной сети, содержащей базу данных, созданную другим лицом, является использованием базы данных и нарушением **исключительных прав правообладателя базы данных** (Выделено мной. - А.С.)" <2>. Поэтому когда бывший сотрудник истца, выступавший ранее администратором страницы компании в социальной сети, создал конкурирующую организацию и представил собранные на странице материалы наработками новой фирмы, это было квалифицировано в качестве не только недобросовестной конкуренции, но и использования материалов базы данных, смежное право на которую принадлежит истцу.

<1> Исчерпывающий характер перечня охраняемых объектов интеллектуальной собственности, содержащийся в [ст. 1225 ГК РФ](#), был подчеркнут в совместном Постановлении Пленумов ВАС и ВС РФ от 26 марта 2009 г. N 5/29 "О некоторых вопросах, возникших в связи с введением в действие части четвертой Гражданского кодекса Российской Федерации" ([п. 9.1](#)).

<2> [Постановление](#) СИП от 7 марта 2014 г. по делу N А56-58781/2012.

Однако в своей основной массе 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".

<1> Так, например, в решении Арбитражного суда Ростовской области от 12 февраля 2009 г. по делу N А53-21574/2008-С2-20 судом была изложена позиция относительно несоответствия веб-сайта легальной дефиниции базы данных.

Квалификация веб-сайта в качестве составного произведения, если сайт представляет собой результат творческого труда по подбору или расположению материалов, была первоначально предложена 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 <1>.

<1> [Постановление](#) ВАС РФ от 22 апреля 2008 г. N 255/08. См. также: [Постановление](#) ФАС Дальневосточного округа от 12 февраля 2013 г. N Ф03-1/2013.

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 <1>. Примечательно, что в данном деле суд провел аналогию между контентом веб-сайта и "витриной" интернет-магазина, включающей в себя созданные в результате творческого труда изображения и описания предлагаемого товара <2>. Квалификация интернет-сайта в качестве разновидности составного произведения нашла свое отражение в принятых изменениях в часть четвертую ГК РФ, новая редакция **п. 2 ст. 1260** которого прямо указала интернет-сайт в качестве разновидности составного произведения: "Составителю сборника и автору иного составного произведения (антологии, энциклопедии, базы данных, интернет-сайта, атласа или другого подобного произведения) принадлежат авторские права на осуществленные ими подбор или расположение материалов (составительство)". Также было 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". Однако эта поправка не была принята.

<1> **Постановление** ФАС Московского округа от 21 июня 2011 г. N КГ-А40/5623-11.

<2> Решение Арбитражного суда г. Москвы от 20 октября 2010 г. по делу N 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.

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 (б) то, что он 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 правопреемнику.

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 трудом (ст. ст. 1228, 1257 ГК РФ). При этом законодательство не содержит критериев такого творческого труда <1>. Представляется, что 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.

<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. N 9; Андреев Ю.Н. Судебная защита исключительных прав: цивилистические аспекты: [Монография](#). М., 2011.

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" <1>.

<1> См.: [Постановление](#) Девятого арбитражного апелляционного суда от 28 мая 2012 г. N 09АП-10525/2012-ГК по делу N А40-83853/11-51-730, оставленное в силе [Постановлением](#) ФАС Московского округа от 10 сентября 2012 г. по делу N А40-83853/11-51-730. См. также: [Постановление](#) ФАС Северо-Западного округа от 23 марта 2009 г. по делу N 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".

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 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, театральные 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>.

КонсультантПлюс: примечание.

Статья В.А. Дозорцева "Право на фильм как сложное многослойное произведение" включена в информационный банк согласно публикации - "Вестник ВАС РФ", 2000, N 3, 4.

<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 // Там же. 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. N 3. Т. 7. С. 124.

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" взаимосвязью: в отсутствие одного из них рабочего веб-сайта не получится. Поэтому веб-сайт вполне может быть отнесен 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.

<1> К данному выводу приходит, в частности, Е.С. Басманова. См.: Басманова Е.С. Указ. соч. С. 95.

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 <1>. Однако в

некоторых случаях вполне возможна квалификация веб-сайта в качестве мультимедийного продукта <2>. 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 <3>. Кроме того, новая редакция [ст. 1240](#) ГК РФ включила базу данных в качестве возможной разновидности сложного объекта, в связи с чем веб-сайт может быть квалифицирован как сложный объект в случае его предварительной квалификации в качестве базы данных.

<1> 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).

<2> См.: [Заключение](#) Исследовательского центра частного права по вопросам толкования и возможного применения отдельных положений части четвертой ГК РФ // Вестник гражданского права. 2007. N 3. Т. 7; Котенко Е.С. Мультимедийный продукт как объект авторских прав: Дис. ... канд. юрид. наук. М., 2012. С. 98.

<3> 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. N 2. 1997. P. 26; Sega

Квалификация веб-сайта одновременно в качестве составного и сложного произведения вызвала определенную критику в литературе как влекущая противоречивые результаты, поскольку составные и сложные объекты имеют разный правовой режим, и неэффективна ввиду того, что правовой статус объекта оказывается "висящим между двух стульев" <1>. Представляется, что квалификация объекта в качестве составного или квалификация его в качестве сложного не являются взаимоисключающими. [Статья 1240](#) ГК РФ не содержит перечня результатов интеллектуальной деятельности (произведений), 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 применения. 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.

<1> Котенко Е.С. Указ. соч. С. 95.

Так что одновременное придание веб-сайту статуса сложного объекта и составного произведения с самостоятельной дефиницией можно только всячески приветствовать как способствующее внесению большей 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.

Таким образом, с гражданско-правовой точки зрения веб-сайт можно рассматривать в качестве результата интеллектуальной деятельности - составного, сложного произведения. При определенных условиях также возможна квалификация веб-сайта в качестве объекта смежных прав - базы данных.

Публично-правовой статус веб-сайта

Публично-правовой статус веб-сайта в основном определяется [Законом](#) об информации. Данный [Закон](#) содержит легальную дефиницию интернет-сайта, согласно которой под сайтом в сети Интернет понимается совокупность программ для электронных вычислительных машин и иной информации, содержащейся в информационной системе, доступ к которой обеспечивается посредством Интернета по доменным именам и (или) по сетевым адресам, позволяющим идентифицировать сайты в Интернете.

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 указанного [Закона](#), одной из основных задач которого в сфере регулирования сети Интернет является регламентация порядка ограничения доступа к информационным ресурсам, 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.

<1> Федеральный [закон](#) от 28 июля 2012 г. N 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).

[Закон](#) об информации, помимо дефиниции веб-сайта, также содержит ряд положений, которые в ряде случаев могут возлагать дополнительные обязанности в связи с наличием на веб-сайте определенного коммуникационного функционала, позволяющего пользователям обмениваться сообщениями друг с другом.

В рамках так называемого антитеррористического пакета законов, принятых вследствие совершенных в декабре 2013 г. терактов в Волгограде, законодательство об информации пополнилось нормами о еще одном субъекте со специальным правовым режимом - об "организаторе распространения информации в сети Интернет" (далее - ОРИВСИ), правовой статус которого обозначен в [ст. 10.1](#) Закона об информации. На указанное лицо возлагаются три основные обязанности: 1) уведомление Роскомнадзора об осуществлении соответствующей деятельности, на основании которого лицо включается в специальный реестр; 2) обязанность по хранению данных в определенном объеме в течение шестимесячного срока; 3) обязанность по сотрудничеству с правоохранительными органами в определенном объеме. Основной целью принятия данных положений является обеспечение правоохранительных органов данными, которые могут представлять интерес для оперативно-разыскной деятельности, расследования и пресечения преступлений. С этой целью на лиц, осуществляющих соответствующую деятельность в Интернете, **de facto** были распространены обязанности, которые до этого уже выполняли операторы связи, что было весьма ожидаемо, учитывая слияние информационных и телекоммуникационных технологий, наблюдающееся с начала XXI в. Так или иначе, выполнение владельцем веб-сайта указанных обязанностей сопряжено со значительными затратами, в связи с чем имеет смысл остановиться на этих обязанностях подробнее <1>.

<1> См. подробный комментарий к [ст. 10.1](#) Закона об информации: Савельев А.И. [Комментарий](#) к

Федеральному закону от 27 июня 2006 г. N 149-ФЗ "Об информации, информационных технологиях и защите информации" (постатейный). М.: Статут, 2015. С. 123 - 141.

В соответствии с **ч. 1 ст. 10.1** Закона об информации организатором распространения информации в сети Интернет является лицо, осуществляющее деятельность по обеспечению функционирования информационных систем и (или) программ для электронных вычислительных машин, которые предназначены и (или) используются для приема, передачи, доставки и (или) обработки электронных сообщений пользователей Интернета. Данная дефиниция, будучи достаточно широкой по своей сути, существенным образом конкретизируется Постановлением Правительства РФ от 31 июля 2014 г. N 759, утвердившим **Правила** хранения данных <1>, которое использует уже несколько иной термин - "коммуникационный интернет-сервис". Под коммуникационным интернет-сервисом в соответствии с вышеуказанными правилами понимается "информационная система и (или) программа для ЭВМ, которая предназначена и (или) используется для приема, передачи и (или) обработки электронных сообщений пользователей Интернета в целях обмена электронными сообщениями между пользователями Интернета, в том числе для передачи электронных сообщений неопределенному кругу лиц". Как видно из указанного **Постановления**, ключевое значение имеет тот факт, что соответствующий коммуникационный функционал веб-сайта обеспечивает возможность обмена сообщениями **между пользователями**, а не просто между пользователем и владельцем веб-сайта.

<1> [Постановление](#) Правительства РФ от 31 июля 2014 г. N 759 "О Правилах хранения организаторами распространения информации в информационно-телекоммуникационной сети Интернет информации о фактах приема, передачи, доставки и (или) обработки голосовой информации, письменного текста, изображений, звуков или иных электронных сообщений пользователей информационно-телекоммуникационной сети Интернет и информации об этих пользователях, предоставления ее уполномоченным государственным органам, осуществляющим оперативно-разыскную деятельность или обеспечение безопасности Российской Федерации" // СПС "КонсультантПлюс".

Таким образом, если веб-сайт предусматривает различного рода чаты, форумы либо возможность оставления пользователями отзывов и комментирования таких отзывов другими пользователями, то он может быть квалифицирован в качестве "организатора распространения информации в сети Интернет. Если же веб-сайт содержит просто форму обратной связи или иные средства коммуникации, которые обеспечивают возможность контакта с администрацией веб-сайта, то владелец такого ресурса не должен признаваться организатором распространения информации в Интернете.

Как отмечалось ранее, одной из обязанностей ОРИвСИ является подача уведомления в Роскомнадзор, на основании которого такое лицо включается в специальный реестр. Порядок подачи уведомления регламентирован в [Постановлении](#) Правительства РФ от 31 июля 2014 г. N 746 <1>, которое предусматривает возможность подачи такого уведомления как по инициативе, исходящей от самого

организатора распространения информации в Интернете, так и от Роскомнадзора.

<1> [Постановление](#) Правительства РФ от 31 июля 2014 г. N 746 "Об утверждении Правил уведомления организаторами распространения информации в информационно-телекоммуникационной сети Интернет Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций о начале осуществления деятельности по обеспечению функционирования информационных систем и (или) программ для электронных вычислительных машин, предназначенных и (или) используемых для приема, передачи, доставки и (или) обработки электронных сообщений пользователей информационно-телекоммуникационной сети Интернет, а также ведения реестра указанных организаторов" // СПС "КонсультантПлюс".

Пока в качестве ОРИВСИ регистрируются организации, предоставляющие сервисы электронной почты, социальных сетей, удаленного хранения данных, размещения блогов и крупных новостных порталов с возможностями ведения дискуссий между пользователями (вне зависимости от наличия или отсутствия регистрации такого портала в качестве сетевого СМИ) <1>. Опасения, что в такой реестр попадут интернет-магазины с формой для обратной связи или официальные веб-сайты организаций, пока не подтвердились, по-видимому, вследствие того что такие веб-сайты не охватываются понятием коммуникационного интернет-сервиса. Также в числе зарегистрированных лиц пока числятся только российские юридические лица, хотя никаких

ограничений по применению положений об ОРИВСИ к иностранным интернет-ресурсам [ст. 10.1](#) Закона об информации не содержит.

<1> В числе первых в реестр организаторов распространения информации в Интернете Роскомнадзор внес: ООО "Яндекс" (сервис электронной почты "Яндекс Почта"; облачный сервис хранения данных "ЯндексДиск"; сервис социальной сети "Мой круг"); ООО "Рамблер Интернет Холдинг" (сервис "Рамблер Почта"); ООО "Мэйл.Ру" (коммуникационный сервис "Mail.ru Агент"; сервис "почта Mail.ru"; сервис социальной сети "Мой мир"); ООО "В контакте" (сервис социальной сети vk.com); ООО "Одноклассники" (сервис социальной сети odnoklassniki.ru); ООО "Юкоз Медиа" - сервис создания веб-сайтов и бесплатного хостинга uCoz.ru; ОАО "Си-Медиа" (ряд сервисов тематических и новостных порталов: film.ru, cars.ru, newsland.ru и др.). Полная версия реестра доступна в формате "открытых данных" по ссылке: <http://rkn.gov.ru/opendata/7705846236-InformationDistribution/>.

Основной обязанностью ОРИВСИ является хранение информации о фактах приема, передачи, доставки и (или) обработки голосовой информации, письменного текста, изображений, звуков или иных электронных сообщений пользователей Интернета и информации об этих пользователях в течение шести месяцев с момента окончания осуществления таких действий ([ч. 3 ст. 10.1](#) Закона об информации). Состав подлежащей хранению информации конкретизирован в [Правилах](#) хранения данных. В основном данная информация может охватываться понятиями "данные о трафике", "метаданные" или "информация об

информации" (например, сведения об IP-адресе, с которого произведена регистрация или авторизация, и о ее времени; сведения о точном времени приема, передачи, доставки и (или) обработки электронных сообщений с указанием информации об адресатах этих сообщений). Содержимое самих коммуникаций не подлежит хранению.

Для того чтобы вышеуказанные данные попадали под обязанности хранения, они должны иметь определенную привязку к российской территории. В соответствии со [ст. 12](#) Правил хранения данных такая привязка может выражаться в форме использования при регистрации или авторизации сетевых адресов, идентифицируемых как российские (главным образом речь идет об IP-адресах, выделяемых российскими операторами связи); получения интернет-сервисом географических данных, указывающих на нахождение пользователя на территории РФ (например, данные GPS-устройства); предоставления при регистрации реквизитов документов, выданных в России; указания контактных телефонов российских операторов связи или информации о местонахождении лица, полученной от уполномоченных органов.

Несмотря на то что данное положение привязывает возникновение обязанности по хранению информации к условию, связанному с территорией РФ, вряд ли данное положение можно рассматривать в качестве содержащего некие юрисдикционные критерии, подобные "тесту минимальных контактов" или "направленной деятельности". Положения [п. 12](#) Правил хранения данных достаточно прямолинейны и никак не учитывают обстоятельств, из которых усматривалась бы воля владельца коммуникационного интернет-сервиса на включение России в сферу своей бизнес-стратегии, а наличие таких обстоятельств является необходимым

условием применения вышеуказанных юрисдикционных критериев <1>. Скорее, указанные положения должны толковаться исключительно в техническом ключе: как конкретизация характеристик подлежащих хранению сообщений.

<1> См. подробнее: [гл. 2](#) настоящей книги.

Сведения, подлежащие хранению в соответствии с [ч. 3 ст. 10.1](#) Закона об информации и [Правилами](#) хранения данных, должны храниться на территории Российской Федерации. По-видимому, это означает, что ОРИВСИ должен иметь на праве собственности или ином праве оборудование, расположенное на территории РФ, на котором будут содержаться базы данных с соответствующими сведениями. При этом запрета на параллельное хранение и обработку таких данных на оборудовании, расположенном за рубежом, ни [ст. 10.1](#) указанного Закона, ни подзаконные акты к ней не содержат.

Требование о хранении данных на территории РФ, очевидно, обусловлено главным образом юрисдикционными соображениями: наличие информации на территории РФ дает отечественным правоохранительным органам дополнительные основания для ее истребования (принцип распространения юрисдикции государственных органов на все, что расположено на территории государства). Подобный подход может, однако, вступать в определенный конфликт с существующими международными соглашениями РФ с иностранными государствами по вопросам о взаимной правовой помощи (**Mutual Legal Assistance Treaties**) <1>.

которые, по идее, должны применяться при взаимодействии с иностранными организаторами распространения информации. Ведь, как отмечалось ранее, положения [ст. 10.1](#) Закона об информации также могут быть распространены в том числе за счет наличия возможности блокировки иностранного веб-сайта, не соблюдающего соответствующие положения.

<1> Например, такое соглашение существует между Россией и США. См.: [Договор](#) о взаимной правовой помощи по уголовным делам между США и Россией от 1999 г. В данном [Договоре](#) содержится процедура и основания для отказа в предоставлении информации (запрос не соответствует требованиям соглашения, или предоставление такой информации осуществляется в связи с расследованием военных преступлений, или предоставление информации противоречит государственным интересам стороны и т.д.).

Помимо хранения, ОРИВСИ обязан в соответствии с [ч. 3 ст. 10.1](#) Закона об информации выполнять установленные требования к оборудованию и программно-техническим средствам, используемым им для распространения информации в Интернете в эксплуатируемых им информационных системах. Такие требования устанавливаются Минкомсвязи России по согласованию с органами, осуществляющими оперативно-разыскную деятельность <1>. По всей видимости, в данном случае речь идет о необходимости установления систем, аналогичных СОПМ (Система оперативно-разыскных мероприятий), внедрение которых является одним из условий получения лицензии оператором связи и требования к которым

также устанавливаются Минкомсвязи России.

<1> [Постановление](#) Правительства РФ от 31 июля 2014 г. N 741 "Об определении федерального органа исполнительной власти, уполномоченного на установление требований к оборудованию и программно-техническим средствам, используемым организатором распространения информации в информационно-телекоммуникационной сети Интернет в эксплуатируемых им информационных системах".

Исполнение обязанностей по хранению данных о трафике и установке специализированного программно-аппаратного обеспечения призвано создать надлежащие технические и правовые условия для обеспечения главной обязанности ОРИВСИ - сотрудничать с российскими уполномоченными правоохранительными органами.

Так, ОРИВСИ обязан предоставлять уполномоченным государственным органам, осуществляющим оперативно-разыскную деятельность или обеспечение безопасности РФ, информацию о фактах приема, передачи, доставки и (или) обработки голосовой информации, письменного текста, изображений, звуков или иных электронных сообщений пользователей Интернета и информацию о таких пользователях ([ч. 3 ст. 10.1](#) Закона об информации). Предоставление такой информации осуществляется в порядке "запрос - ответ". В [Правилах](#) хранения данных конкретизированы виды запросов (стандартные, срочные и т.д.) и сроки ответов на них.

Перечень органов, осуществляющих оперативно-разыскную деятельность, содержится в [ст.](#)

13 Федерального закона от 12 августа 1995 г. N 144-ФЗ "Об оперативно-розыскной деятельности". К ним относятся органы МВД, ФСБ, ФСО, СВР, ФСИН, ФСКН, а также таможенные органы. При этом ОРИВСИ не требуется взаимодействовать со всеми ими напрямую. Согласно [Постановлению](#) Правительства РФ от 31 июля 2014 г. N 743 <1> органы федеральной службы безопасности, являясь уполномоченными органами, осуществляют взаимодействие с организаторами распространения информации при проведении в рамках оперативно-розыскной деятельности оперативно-розыскных мероприятий, в том числе в интересах других уполномоченных органов.

<1> [Постановление](#) Правительства РФ от 31 июля 2014 г. N 743 "Об утверждении Правил взаимодействия организаторов распространения информации в информационно-телекоммуникационной сети Интернет с уполномоченными государственными органами, осуществляющими оперативно-розыскную деятельность или обеспечение безопасности Российской Федерации" // СПС "КонсультантПлюс".

Неисполнение владельцем веб-сайта обязанностей, вытекающих из наличия у него статуса ОРИВСИ, может влечь административную ответственность (ст. [13.31](#) КоАП РФ), а при неустранении соответствующих нарушений в установленный срок - ограничение доступа к такому веб-сайту на территории РФ в порядке, предусмотренном в ст. [15.4](#) Закона об информации.

В завершение рассмотрения вопроса о публично-правовом статусе 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 <1>, учитывая, что она во многом устарела с принятием в 2011 г. поправок в [Закон](#) РФ "О средствах массовой информации" (далее - Закон о СМИ) <2>. 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 <3>. Таким образом, вопрос о целесообразности регистрации веб-сайта в качестве СМИ должен решаться путем тщательного взвешивания всех плюсов и минусов такого шага.

<1> Подробнее см., например: Петровский С.В. [Сайт - иное СМИ: коллизии права](#) // Журнал российского права. 2001. N 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. N 1.

<2> См.: Федеральный [закон](#) от 14 июня 2011 г. N 142-ФЗ "О внесении изменений в отдельные законодательные акты Российской Федерации в связи с совершенствованием правового регулирования в сфере средств массовой информации".

<3> [Пункт 23](#) Постановления Пленума ВС РФ от 15 июня 2010 г. N 16 "О практике применения судами Закона Российской Федерации "О средствах массовой информации".

информации".

Для того чтобы веб-сайт стал частью сети Интернет и был доступен ее пользователям, обычно необходимо пройти три основных этапа: 1) разработать веб-сайт; 2) заключить договор с провайдером хостинга; 3) выбрать и зарегистрировать доменное имя <1>. Рассмотрим данные этапы подробнее.

<1> Klosek J. The Legal Guide to E-Business. Westport, Connecticut, London, 2003. P. 10.

§ 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 <1>; 2) как договоры возмездного оказания услуг <2>; 3) как договоры авторского заказа <3>. Встречается также и квалификация данного договора в качестве смешанного, с элементами договора подряда и договора возмездного оказания услуг <4>.

<1> См., например: Постановления Тринадцатого арбитражного апелляционного суда от 3 декабря 2009 г. по делу [N A56-13527/2009](#), ФАС Северо-Западного

округа от 7 июня 2011 г. по делу [N A56-4382/2010](#), Девятого арбитражного апелляционного суда от 29 апреля 2013 г. [N 09АП-12471/2013-ГК](#) по делу N A40-148075/12-12-684, ФАС Волго-Вятского округа от 9 марта 2010 г. [N A17-2284/2009](#).

<2> Постановления Одиннадцатого арбитражного апелляционного суда от 6 октября 2011 г. по делу [N A55-2984/2011](#), Седьмого арбитражного апелляционного суда от 16 июня 2010 г. [N 07АП-2156/10](#) по делу N A03-11831/2009.

<3> [Постановление](#) Шестого арбитражного апелляционного суда от 20 ноября 2012 г. N 06АП-5030/2012 по делу N A73-4956/2012.

<4> [Постановление](#) ФАС Уральского округа от 22 апреля 2010 г. N Ф09-3004/10-С2 по делу N A76-20390/2009-2-856.

Наиболее распространенной в судебной практике является квалификация договора на разработку веб-сайта в качестве договора подрядного типа. Поддерживается она и в отечественной доктрине <1>. 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 делимый от личности исполнителя результат, подлежащий сдаче заказчику. Во-вторых, положения [гл. 37](#) ГК РФ о договоре подряда содержат наиболее детальное

регулирование вопросов, связанных с процессом создания определенного результата по заданию заказчика, его сдачи-приемки, распределения рисков необходимости проведения дополнительных работ, ответственности за недостатки и пр.

<1> Калятин В.О. Право в сфере Интернета. С. 96; Барабыкин П.В. Указ. соч. С. 72.

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 создает формальные препятствия для использования норм о договоре возмездного оказания услуг для регулирования отношений, возникающих в связи с созданием веб-сайта.

КонсультантПлюс: примечание.

[Монография](#) Ю.В. Романца "Система договоров в гражданском праве России" включена в информационный банк согласно публикации - Норма, Инфра-М, 2013 (2-е издание, переработанное и дополненное).

<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. N 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. N 1. Можно не соглашаться с выводами и аргументацией данного **Постановления**, но отрицать его наличие и возможное юридическое значение при анализе рассматриваемого вопроса было бы некорректно.

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, как отмечалось ранее, 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) <1>; возможно применение специальной договорной конструкции - договора авторского заказа. В том случае, если исполнителем выступает юридическое лицо, конструкция договора авторского заказа неприменима.

<1> В соответствии со [ст. 1257](#) ГК РФ автором произведения науки, литературы или искусства признается **гражданин**, творческим трудом которого оно создано.

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. 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 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, который 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.

<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.

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. Как показывают исследования, средний пользователь оценивает веб-сайт за 50 миллисекунд: за этот промежуток времени он четко понимает, нравится ли ему данный веб-сайт, и решает, стоит ли задержаться здесь или лучше идти дальше <1>. 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 в формате программы, в которой создавался макет. Как правило, в качестве такой программы выступает **Adobe Photoshop CS2**, соответственно, результаты формируются в формате файла PSD.

<1> Lindgaard G. et. al. Attention Web Designers: You Have 50 MiHiseconds to Make a Good First Impression! // Behaviour & Information Technology. 2006. Vol. 25. Iss. 2.

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. Кроме того, на данном этапе может осуществляться интеграция веб-сайта с бизнес-приложениями заказчика и различными базами данных, например базой данных клиентов заказчика.

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 внести прозрачность в процесс регламентации распределения исключительных прав на такие объекты между заказчиком и разработчиком, а также обеспечить единство веб-сайта как передаваемого объекта.

<1> Graham Smith. Op. cit. P. 758.

Следует отметить, что приведенная выше

этапность разработки веб-сайта является, скорее, идеальной моделью и нередко на практике "обрастает" дополнительными этапами, например разработкой сценариев поведения пользователя на веб-сайте. Для того чтобы пользование интернет-сервисом или интернет-магазином не превращалось в пытку для пользователя, элементы интерфейса должны быть интуитивно понятными. Для разработки такого интерфейса нередко привлекаются UX-инженеры (аббревиатура от англ. **user experience**), которые детально изучают целевую аудиторию и оптимизируют типовые сценарии взаимодействия пользователя с веб-сайтом.

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 приобретает статус задания заказчика в контексте [ст. 702 ГК РФ](#) и становится 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>.

<1> См.: п. 6 информационного письма Президиума ВАС РФ от 25 ноября 2008 г. N 127 "Обзор практики применения арбитражными судами статьи 10 Гражданского кодекса Российской Федерации". См. также: Определения ВАС РФ от 30 мая 2012 г. N [ВАС-6830/12](#) по делу N A04-1367/2011, от 25 июня 2010 г. N [ВАС-7668/10](#) по делу N A27-9091/2009.

Не менее важной является регламентация в договоре на разработку веб-сайта порядка распределения исключительных прав на объекты, выступающие его составными частями <1>. Здесь существуют различные варианты, наиболее предпочтительным из которых для заказчика является переход исключительных прав на такие объекты к нему. Это не только 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 <2>. 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 и бизнес-процессами заказчика. Поскольку совершаемые обновления могут подпадать под понятие производного произведения <3>, совершение подобных действий требует согласия правообладателя. Очевидно, что если правообладателем выступает то лицо, которое заказывает модификации, никаких проблем с получением отдельного согласия (лицензии) на совершение таких действий нет. Если по условиям договора на разработку веб-сайта заказчик не приобретает статуса правообладателя в отношении созданных компонентов, ему необходимо позаботиться о том, чтобы предоставленная от исполнителя лицензия, помимо всего прочего, включала право на последующую переработку таких компонентов.

<1> Kunze C. Web Site Legal Issues // Santa Clara Computer & High Technology Law Journal. 1998. Vol. 14. P. 479 - 482; Graham Smith. Op. cit. P. 757.

<2> Как известно, чем прочнее права на объект, тем выше его цена.

<3> В соответствии с [п. 2 ст. 1259 ГК РФ](#) под производными произведениями понимаются произведения, представляющие собой переработку других произведений.

Разумеется, разработчик веб-сайта заинтересован в том, чтобы иметь возможность использования тех наработок, которые он сделал для

заказчика, в своих будущих проектах <1>. Такие наработки могут иметь немалую ценность, составляя конкурентное преимущество разработчика и позволяя минимизировать затраты времени и средств путем использования проверенных решений. Указанные факторы обуславливают 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 объектам авторского права, 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 <2>. Кроме того, после внесенных поправок в часть четвертую [ГК РФ](#) положения [ст. 1296 ГК РФ](#) могут применяться не только к договорам на создание на заказ компьютерных программ и баз данных, но и к договорам на создание иных видов произведений, что снимает возможные вопросы о ее применимости к договорам на разработку веб-сайтов.

<1> Klosek J. Op. cit. P. 12.

<2> Здесь, правда, могут возникнуть вопросы относительно толкования понятия "собственные нужды". Но, как представляется, оно является достаточно широким, чтобы охватить ситуации использования результата интеллектуальной деятельности компанией в целях осуществления своего основного вида деятельности.

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. Целесообразно 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>.

<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 именуется **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. С недавних пор данная концепция была введена в ГК РФ, в соответствии со ст. 406.1 которого стороны обязательства при осуществлении ими предпринимательской деятельности могут своим соглашением предусмотреть обязанность одной

стороны возместить имущественные потери другой стороны, возникшие в случае наступления определенных в таком соглашении обстоятельств и не связанные с нарушением обязательства одной из его сторон (потери, вызванные невозможностью исполнения обязательства, предъявлением требований третьими лицами или органами государственной власти к стороне или к третьему лицу, указанному в соглашении, и т.п.). Соглашением сторон должен быть определен размер возмещения таких потерь или порядок его установления.

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 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 рассмотрении 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 Интернету. При наличии необходимого оборудования и собственного канала доступа в 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 Интернете.

В доктрине под хостингом обычно понимают услуги по предоставлению провайдером дискового пространства для размещения веб-сайта пользователя на сервере, подключенном к Интернету под постоянным IP-адресом, с его последующим техническим обслуживанием <1>.

<1> См., подробнее: Басманова Е.С. Указ. соч. М., 2010. С. 71; Камфер Ю., Бойкова М. Интернет: от сложного к простому // Бухгалтерское приложение к газете "Экономика и жизнь". 2000. N 52; Савельев А.И. Гражданско-правовое регулирование договоров между клиентом и интернет-провайдером в сети Интернет: Дис. ... канд. юрид. наук. М., 2008. С. 18.

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, выделенным такому сайту, такой хостинг именуют физическим.

Услуга размещения на одном IP-адресе нескольких веб-сайтов с различными доменными именами получила название "виртуальный хостинг" <1>.

<1> См., например: Барабыкин П.В. Указ. соч. С. 55, 56.

Наконец, существуют ситуации, когда владелец

веб-сайта обладает собственным сервером, который размещается в дата-центре провайдера, обеспечивающего его постоянное подключение к Интернету 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. <1>.

<1> Подробнее о видах и особенностях договора хостинга см.: Савельев А.И. Гражданско-правовое регулирование договоров между клиентом и интернет-провайдером в сети Интернет.

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 <1>. Так, провайдером хостинга является лицо, оказывающее услуги по предоставлению вычислительной мощности для размещения информации в информационной системе, постоянно подключенной к Интернету. Отсюда следует, что под хостингом понимаются услуги по предоставлению вычислительной мощности для размещения информации в информационной системе, постоянно подключенной к Интернету <2>.

<1> См.: [Закон](#) "О внесении изменений в Федеральный закон "О защите детей от информации, причиняющей вред их здоровью и развитию" и отдельные законодательные акты Российской Федерации".

<2> Данное определение вряд ли можно признать удачным, поскольку ключевой термин "вычислительные мощности", на котором оно зиждется, является весьма неопределенным.

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 лицензии на деятельность в качестве оператора связи.

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" <1>, 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).

"Телематические службы", утв. Приказом Министерства РФ по связи и информатизации от 23 июля 2001 г. N 175.

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. N 87 <1> 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 <2>, 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.) <3> (например, в ходе организации "обратной связи" с пользователем веб-сайта, при функционировании различного рода форумов), то получается, что услуги хостинга подпадают под понятие телематических услуг связи и получение лицензии на их оказание становится весьма целесообразным.

<1> [Постановление](#) Правительства РФ от 18 февраля 2005 г. N 87 "Об утверждении перечня наименований услуг связи, вносимых в лицензии, и перечней лицензионных условий".

<2> [Постановление](#) Правительства РФ от 10

сентября 2007 г. N 575 "Об утверждении Правил оказания телематических услуг связи".

<3> 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 обмена, поддерживаемым взаимодействующими информационной системой и абонентским терминалом (п. 2).

Услуги хостинга вполне могут подпасть также и под определение услуги связи, содержащееся в ст. 2 Федерального закона от 7 июля 2003 г. N 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. Кроме того, дефиниция хостинга, выводимая из Закона об информации, включает в себя упоминание о необходимости обеспечения постоянного подключения к Интернету. 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.

<1> См. подробнее: Савельев А.И. [Применение судами норм Гражданского кодекса Российской Федерации о публичных договорах](#) // Вестник гражданского права. 2009. N 4.

Однозначного ответа на вопрос, необходимо ли провайдеру хостинга иметь лицензию оператора связи, на данный момент нет. Минкомсвязи России так и не дало вразумительных разъяснений по данному вопросу, хотя в ответ на индивидуальные запросы, а также в неофициальных беседах представители этого ведомства говорят об отсутствии необходимости получения лицензий на хостинг.

Многие провайдеры подстраховываются и получают лицензию на телематические услуги связи и услуги связи по передаче данных. Хотя при этом они, избавляясь от рисков, связанных с вероятностью квалификации их деятельности в качестве осуществляемой без специального разрешения ([ч. 2 ст. 14.1 КоАП РФ](#)), принимают на себя все возможные риски, связанные с возможным привлечением их к ответственности за несоблюдение лицензионных положений и правил оказания соответствующих услуг связи. Одно можно сказать со значительной долей определенности: если услуги хостинга предоставляются на безвозмездных началах, то получения лицензии оператора связи не требуется, поскольку лицензированию подлежат только возмездные услуги связи <1>.

<1> См.: [п. 1 ст. 29](#) Федерального закона от 7

июля 2003 г. N 126-ФЗ "О связи".

Теперь целесообразно обратиться к рассмотрению условий договора хостинга.

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" <1>; предоставляемые дополнительные сервисы (например, ведение статистики посещаемости сайта, поддержка защищенных соединений и пр.).

<1> См.: Гуров В.В. Корпоративный веб-хостинг // Сети и системы связи. 2008. N 3 (165). С. 28.

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**) <1>.

<1> Klosek J. Op. cit. P. 17.

Одним из существенных показателей, характеризующих качество услуги хостинга, является пропускная способность линии связи, используемой

провайдером хостинга, характеризующая объем данных, 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.

<1> Graham Smith. Op. cit. P. 765.

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 <1>. Как отмечается, средним показателем времени реакции сервера является 85 миллисекунд <2>.

<1> Калятин В.О. Право в сфере Интернета. С. 98. См. также: Online Contract Formation / Ed. by Stephan Kinsella and Andrew Simpson. Oceana Publications: N.Y., 2004. P. 355.

<2> Roditti E. Computer Contracts. Vol. I. Mathew Bender. 2006. P. 1951.

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% <1>. 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.

<1> Ibid. P. 1828.

Наконец, целесообразно отразить в договоре хостинга положения, касающиеся судьбы веб-сайта в случае расторжения договора. Применительно 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 о разграничении ответственности за контент, размещенный на данном сайте иными лицами (владельцем веб-сайта или его посетителями), между владельцем веб-сайта и провайдером хостинга, который в основном заключается в определении пределов ответственности провайдера хостинга.

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 их, а не неких трудноидентифицируемых пользователей или владельцев сайта, которых надо сначала отыскать, а потом умудриться с них что-либо успешно взыскать.

<1> Reed C., Angel J. Op. cit. P. 240.

<2> Как известно из курса логики, причина причины есть причина следствия.

Очевидно, что возложение на интернет-провайдеров полной ответственности за действия третьих лиц пагубно скажется на развитии электронной коммерции и всей сети Интернет в целом: повлечет 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 на размещаемый контент <1>. С другой стороны, технические реалии функционирования сети Интернет не позволяют игнорировать интернет-провайдеров в качестве "хранителей" его врат (**gatekeepers**) и обусловленный ими 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 эту

проблематику в компаративном аспекте <2>, однако все же необходимо в общем виде остановиться на наиболее важных моментах, учитывая, что в условиях трансграничной природы Интернета провайдерам хостинга приходится иметь дело с зарубежным законодательством.

<1> Savin A. Op. cit. P. 104.

<2> Одним из наиболее полных компаративных исследований по данной тематике является работа: 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_responsMityof_the_intemetinterme-diaries_final.pdf. На русском языке достаточно подробно данные вопросы освещаются в работе: Войниканис Е. **Право интеллектуальной собственности** в цифровую эпоху. Парадигма баланса и гибкости. М., 2013. С. 288 - 352.

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. (Communications Decency Act, CDA), в котором есть ст. 230 (с), включающая положения 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. Иными словами, пользователи Интернета защищены от возможной ответственности за хостинг (размещение) или репостинг информации, ранее опубликованной иными лицами. При этом факт принятия провайдером мер по фильтрации, модерированию или ограничению доступа к контенту, который провайдер или пользователь считает противоправным, не дает дополнительных оснований для возникновения ответственности за размещение такого контента. Как отмечается, данное законодательное положение во многом предопределило появление и расцвет различных интерактивных интернет-сервисов вроде Youtube, Amazon, Facebook и пр., поскольку при наличии рисков привлечения к ответственности самой онлайн-платформы за комментарии и контент пользователей вряд ли они бы существовали в том виде, в каком они известны сейчас. В отсутствие аналогичных законодательных положений в иных странах подобное регулирование превратило США в "безопасную гавань" для онлайн-сервисов, связанных с распространением информации, имеющей политическую, религиозную или прочую "чувствительную" окраску с точки зрения требований национальных законодательств иных стран <1>.

<1> CDA 230: The Most Important Law Protecting Internet Speech. URL: <https://www.eff.org/issues/cda230>.

Неудивительно, что 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 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>.

<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.

Однако ст. 230 CDA не применяется к случаям нарушения исключительных прав в сети Интернет.

Основным законом, регламентирующим ответственность интернет-провайдеров 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** (в пер. с англ. - тихая гавань). 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 <1>: 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 <2>; 3) оперативное удаление такого контента по получении уведомления от правообладателя или его агента (так называемая процедура **notice-and-take-down**) <3>. В числе дополнительных условий Закон указывает: 1) наличие политики защиты авторских прав, предусматривающей расторжение договора (удаление аккаунта) пользователей, неоднократно нарушающих авторские права; 2) назначение специального контактного лица, специализирующегося на взаимодействии с правообладателями; 3) непротивление и содействие в применении правообладателями технических средств защиты произведений.

<1> § 512 (c).

<2> 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).

<3> Bellia, Schiff and Post's Cyberlaw: Problems of Policy and Jurisprudence in the Information Age. West Group Publishing. 2004. P. 523.

В общем виде действие процедуры

notice-and-take-down на практике можно проиллюстрировать в виде следующего алгоритма:

- **A** размещает песню, правообладателем которой является **B**, на сайте, хостируемом провайдером **C**;

- **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; прилагает заявление о том, что **B** добросовестно считает, что **A** не имеет разрешения от него или его агентов на размещение данной песни, заявление о достоверности приведенной в уведомлении информации;

- **C** на основании полученного заявления удаляет песню с сайта и направляет об этом уведомление **A**;

- **A** имеет право направить контр уведомление, 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;

- **C**, получив контр уведомление, уведомляет **B** и ждет 10 - 14 рабочих дней;

- если **B** не подает иск в течение вышеуказанного срока, то **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, размещенную при предоставлении услуг хостинга, если он не был осведомлен о ее противоправном характере, а также о фактах или обстоятельствах, из которых такой противоправный характер очевиден <2>, и после получения соответствующих сведений оперативно удалил противоправную информацию или прекратил доступ к ней (ст. 14).

<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 экономике 2004 г. (**Loipour la confiance dans l'économie numérique**); в Англии - в Закон об электронной коммерции 2002 г. (**Electronic Commerce Regulations**).

<2> Данная оговорка может быть актуальной, в частности, применительно к популярным пиратским файлообменным сайтам. См.: Savin A. Op. cit. P. 116.

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 предreshает **автоматически** вопрос о его виновности. Это просто означает, что ответственность 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 Бельгийского суда об обязанности 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>.

<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.

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 <1>, Сингапур) <2> содержатся схожие нормы. Даже в Китае, вопреки распространенному в российской доктрине ошибочному мнению о полной ответственности провайдеров за действия пользователей <3>, реализован принцип возложения на провайдера 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 <4>.

<1> Закон Японии 2001 г. N 137 об ограничениях ответственности провайдеров телекоммуникационных услуг за убытки и о праве требовать раскрытия информации об отправителе. Неофициальный английский перевод: www.isc.meiji.ac.jp/~sumwel_h/doc/codeJ/provider-e.htm.

<2> Graham Smith. Op. cit. P. 639 - 641.

<3> См., например: Рассолов И.М. [Указ. соч.](#) § 3 гл. 3; Примакова О.М. [Нарушение авторского права в сети Интернет](#) // Правовые вопросы связи. 2011. N 1; Наумов В.Б. Право и Интернет: очерки теории и практики. С. 19.

<4> См.: разъяснения Верховного суда КНР от 22 ноября 2000 г. по вопросам применения закона в спорах, связанных с нарушением авторских прав в сети Интернет; Регуляции о защите права на коммуникации посредством информационных сетей 2006 г. Цит по: Graham Smith. Op. cit. P. 556 - 557.

В России вопрос о пределах ответственности интернет-провайдеров является не менее актуальным <1>. Подобно тому как это имеет место в США, в России к разным типам информации применяются нормы разных законов.

<1> См.: [п. 2.5 разд. VII Концепции развития гражданского законодательства Российской Федерации](#) // Вестник ВАС РФ. 2009. N 11.

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 (ч. 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 <1>; 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 (ч. 2 ст. 1).

<1> См., например: [Постановление Четвертого арбитражного апелляционного суда от 27 февраля 2012 г. по делу N 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).

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 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 иницирует 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 хостинг-провайдер "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. N 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. N 09АП-26277/2009-ГК по делу N А40-89751/09-51-773, оставленное в силе [Постановлением](#) ФАС Московского округа от 11 мая 2010 г. N 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 иным лицом, к которому должны быть предъявлены требования из нарушения авторских прав, ответственность может понести провайдер хостинга.

Критерии освобождения провайдеров хостинга, изложенные в [Постановлении](#) ВАС РФ 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.

<1> [Постановление](#) Президиума ВАС РФ от 1 ноября 2011 г. N 6672/11 по делу N А40-75669/08-110-609.

Как справедливо отмечается в литературе, из [Постановления](#) ВАС РФ по делу "Агава-софт" неясно, какие конкретно действия должен совершить провайдер хостинга, для того чтобы считать себя в безопасности <1>. 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 данном [Постановлении](#) ВАС РФ ориентирует суды на то, чтобы наличие специальных программ по предупреждению и отслеживанию контрафактных произведений и их эффективность анализировалось в **любом** случае. Правда, непонятно, 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 судебского усмотрения.

<1> Войниканис Е. [Указ. соч.](#) С. 340.

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 словосочетания "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>.

<1> Федеральный [закон](#) от 2 июля 2013 г. N 187-ФЗ "О внесении изменений в отдельные законодательные акты Российской Федерации по вопросам защиты интеллектуальных прав в информационно-телекоммуникационных сетях".

Ответственность провайдеров хостинга (в терминологии части четвертой [ГК РФ](#) - информационных посредников, предоставляющих возможность размещения материалов в Интернете) урегулирована в [п. 3 ст. 1253.1 ГК РФ](#).

Данное лицо не несет ответственности за нарушения интеллектуальных прав, произошедшие в результате размещения в Интернете 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 необходимых и достаточных мер и порядок их осуществления могут быть установлены законом" <1>.

<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. N 7. С. 34.

Как отмечалось ранее, 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, первоначально направленного на борьбу с нелегальным распространением фильмов в Интернете, а впоследствии распространенном и на другие объекты авторских прав (кроме фотографий). 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.

Представляется, что, исходя из положений [п. 3 ст. 1253.1](#) ГК РФ, провайдер хостинга приобретает знание о том, что использование на его интернет-ресурсе какого-либо из объектов исключительных прав, загруженного пользователем, является неправомерным, в момент получения от правообладателя или иного уполномоченного им лица уведомления, содержащего сведения о конкретном объекте, исключительное право на который нарушено, и конкретном материале, размещенном на интернет-ресурсе, где такой объект содержится. Общее уведомление о массовых нарушениях исключительных прав на интернет-сайте информационного посредника, не содержащее обоснованных фактов нарушений прав на конкретные объекты, не позволяет говорить о том, что информационный посредник знал о соответствующем нарушении ^{<1>}. В равной степени не позволяют говорить об этом уведомления, которые хотя и содержат соответствующую информацию, но не исходят от правообладателя или уполномоченного им лица.

<1> Данный подход уже начинает находить свое отражение в отечественной судебной практике. Так, суд не принял аргумент истца о том, что информационный посредник "должен был знать" о нарушении его исключительного права, поскольку сведения о том, что на площадке такого посредника неоднократно осуществляются нарушения исключительных прав, содержались в известном докладе **Special 301** Администрации представителя США в сфере внешней торговли (**Office of the US Trade Representative**). См.: решение Арбитражного суда г. Санкт-Петербурга и Ленинградской области от 23 октября 2013 г. по делу N А56-34224/2013.

Вменение провайдеру хостинга знания о конкретных нарушениях не должно осуществляться на основании имевших место в СМИ или иных информационных площадках обсуждений, в которых не участвовал уполномоченный представитель информационного посредника, поскольку это означало бы возложение на него обязанности по мониторингу информационного пространства, что не соответствует природе предоставляемых сервисов, а также означало бы переложение бремени по защите исключительного права с самих правообладателей на информационных посредников, что вступало бы в противоречие с целями введения [ст. 1253.1](#) ГК РФ и норм об особенностях ответственности информационных посредников <1> в зарубежных странах: развитие Интернета при обеспечении баланса интересов заинтересованных лиц (пользователей, информационных посредников и правообладателей). Приведенное толкование основано на практике разрешения подобного рода вопросов, выработанной в Европе и США <2>.

<1> См.: [Постановление](#) Суда по интеллектуальным правам от 22 июня 2015 г. N C01-524/2015 по делу N A40-66554/2014, в котором говорится: "Учитывая, что компания YouTube не может нести ответственность за наполнение иными лицами видеохостинга, находящегося в открытом доступе, а также принимая во внимание, что ответчик уже отреагировал на уведомления истца о нарушении исключительных прав и заблокировал спорный контент, суды отметили, что требование истца к компании **YouTube** является фактически попыткой переложить на информационного посредника обязанность по мониторингу деятельности третьих лиц, идентификации контента и выявлению нарушений".

<2> См. подробнее: Савельев А.И. [Критерии наличия действительного](#) и предполагаемого знания как условия привлечения к ответственности информационного посредника // Закон. 2015. N 11. С. 48 - 60.

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"? Однозначного ответа на данный вопрос пока нет, хотя в ряде решений СИП рекомендации ВАС РФ находят свое отражение даже после вступления в силу положений [ст. 1253.1 ГК РФ](#) <1>. Представляется, что постановления ВАС РФ, если и могут применяться, то только в части, не противоречащей [ГК РФ](#), в том числе касательно объема тех условий, которые необходимы и достаточны для освобождения информационного посредника от ответственности.

<1> См., например: [Постановление](#) Суда по интеллектуальным правам от 24 апреля 2015 г. N C01-251/2015 по делу N A40-150342/2013.

§ 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 Интернета.

Суть доменного имени можно вкратце обозначить следующим образом. Каждый компьютер, подключенный к Интернету, 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 символическое имя конкретному IP-адресу в Сети <1>. В доктрине под доменным именем понимается **зарегистрированное в установленном порядке символическое обозначение, заменяющее цифровой IP-адрес компьютера, подключенного к Интернету, 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>.

<1> Серго А.Г. Интернет и право. С. 29.

<2> Калятин В.О. Доменные имена. С. 14.

<3> [Статья 2](#) Закона об информации.

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" <1>.

<1>

<http://www.wipo.int/amc/en/center/flag/domains.html>

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 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>.

<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. N 2011-18/81 (в ред. от 20 сентября 2012 г.) (далее - Правила регистрации доменных имен) <http://www.cctld.ru/ru/docs/rules.php>. 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 стоп-лист доменных имен, который содержит в себе примеры подобного рода словоупотребления. Нахождение доменного имени в стоп-листе является безусловным основанием для отказа в его регистрации.

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**) <1>. О том, как рассматриваются подобного рода конфликты, будет подробнее сказано далее. Сейчас хотелось бы остановиться на вопросах регистрации доменного имени.

<1> См.: пункты 3.1.3, 3.1.4 Правил регистрации доменных имен, где закреплено: "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".

Регистрация и поддержка доменных имен осуществляются на началах саморегулирования специальными организациями, каждая из которых отвечает за свою часть доменных имен сети Интернет. Координирующую 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).

<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.

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 <1>. Регистрация доменных имен носит явочный (заявительный) характер и осуществляется на основании публичного договора об оказании услуг регистрации (ст. 426 ГК РФ) <2>.

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 Интернете.

<1> Список таких регистраторов доступен на сайте Координационного центра национального домена сети Интернет // <http://cctld.ru/ru/registrators/>.

<2> 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 доменного имени представляет собой внесение регистратором в специальный реестр сведений о доменном имени, его администраторе и иных сведений, установленных правилами. Такая регистрация носит срочный характер - один 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 Интернета 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>?

<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. 2009. N 42. P. 289.

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 <1>. 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 <2>.

<1> Pitman Training Limited & Another v. Nominet UK & Another (1997) FSR 797; Murray A. Internet Domain Names: The Trade Mark Challenge 11 International Journal of Law and Information Technology. 2001. N 6. P. 294 - 295.

<2> Graham Smith. Op. cit. P. 171.

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 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 киберсквоттинга" <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>.

<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 киберсквоттингом (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).

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 <1>.

<1> Graham Smith. Op. cit. P. 265 - 266.

Вопрос правовой природы доменного имени был недавно предметом рассмотрения Европейского суда по правам человека (далее - ЕСПЧ). 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 за их аннулированием) были обусловлены легитимным общественным интересом в обеспечение защиты прав на товарные знаки и не являлись чрезмерными <1>. Таким образом, ЕСПЧ 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 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>.

<1> Paeffgen GmbH v. Germany. 18.09.2007. [N 25379/04](#), 21688/05, 21722/05 и 21770/05.

<2> Европейская конвенция о защите прав человека и основных свобод. Право на собственность. М., 2002. С. 4.

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 <1> и доменное имя как средство адресации в Интернете <2>.

<1> 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. N 5.

<2> См., например: Бабкин С.А.

Интеллектуальная собственность в сети Интернет. С. 422; Милютин З.Ю. Правовой статус доменного имени // Патенты и лицензии. 2005. N 6; Невзоров И. О соотношении доменного имени с объектами интеллектуальной собственности // Хозяйство и право. 2006. N 1.

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 доменного имени оказываются шире, чем функции только товарных знаков (знаков обслуживания) или фирменных наименований" <1>. В практике ВАС РФ можно найти некоторую поддержку указанной позиции. Так, в одном деле было указано, что "доменные имена фактически трансформировались в средство, выполняющее функцию товарного знака, который дает возможность отличать соответственно товары и услуги одних юридических или физических лиц от однородных товаров и услуг других юридических или физических лиц" <2>.

<1> Калятин В.О. Доменные имена. С. 19.

<2> [Постановление](#) Президиума ВАС РФ от 16 января 2001 г. N 1192/00.

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 в купе с отсутствием опыта их законодательного регулирования за рубежом <1>. 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 <2>. Правда, долго эта норма не прожила: в октябре 2010 г. упоминание о доменных именах из данной нормы было исключено <3>. Единственными положениями ГК РФ,

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.

<1> 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. N 3.

<2> Еременко В.И. [О совершенствовании правового регулирования](#) доменных имен в Российской Федерации // Законодательство и экономика. 2012. N 10.

<3> Федеральный [закон](#) от 4 октября 2010 г. N 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 группы по присоединению Российской Федерации к Всемирной торговой организации от 17 ноября 2011 г. // СПС "КонсультантПлюс").

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 Интернета идентифицировать конкретную информацию, зафиксированную на компьютере (сервере) третьего лица, и в первую очередь служит именно цели идентификации документа с информацией в Интернете <1>.

<1> Невзоров И.В. [Правовая природа доменного имени](#) и его соотношение с объектами интеллектуальной собственности // Предпринимательское право. 2005. N 4.

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" <1>. Схожую позицию поддерживает и С. Бабкин, который считает, что "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" <2>. 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.

<1> Милютин З.Ю. Соотношение доменных имен со средствами индивидуализации: Дис. ... канд. юрид. наук. М., 2005. С. 78 - 81.

<2> Бабкин С.А. Интеллектуальная собственность в сети Интернет. С. 422.

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 первоначальный 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 Интернете 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 несвойственна 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".

<1> Юрасов А.В. Указ. соч. С. 284.

Возможно, со временем ситуация изменится и законодатель встанет перед необходимостью придания доменному имени особого правового 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. В лучшем случае его можно рассматривать в качестве отдельного способа использования товарного знака. Следовательно, на доменное имя как таковое 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. Такое относительное имущественное право вполне может быть объектом распоряжения и даже предметом наследования ^{<2>}.

^{<1>} См.: ст. 6 Правил регистрации доменных имен.

^{<2>} Новоселова Л.А. Можно ли передать по

наследству доменное имя? // Патенты и лицензии. Интеллектуальные права. 2014. N 9. С. 19.

§ 6. Споры в сфере доменных имен

Учитывая неизбежные конфликты между владельцами доменных имен и обладателями прав на фирменные наименования 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 ^{<1>}, но хотелось бы отметить следующее.

^{<1>} 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.**

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, которые должен понести правообладатель, могут выступить 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>.

<1> <http://www.icann.org/ru/dndr/udrplPolicy-ru.htm>

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.) <1>. В соответствии с действующими правилами регистрации доменов в зоне **.ru** и **.рф**, а также домена **.su** процедура **UDRP** для доменных споров национальной зоны доменов первого уровня **.ru, .рф** и **.su** не применяется. Кроме того необходимо отметить, что сфера применения **UDRP** ограничена лишь защитой товарных знаков (знаков обслуживания), поскольку в этой сфере законодательство различных стран является наиболее гармонизированным по сравнению с нормами о фирменных наименованиях, коммерческих обозначениях, защите имени гражданина.

<1> Полный список см.:
<http://www.wipo.int/amc/en/domains/cctld/>. Следует
отметить, что .RU и .РФ в их число не входят, равно как
и .US.

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)
Арбитражный и медиационный центр ВОИС (**WIPO
Arbitration and Mediation Center**); 5) Арабский центр по
рассмотрению споров в сфере доменных имен (**Arab
Center for Domain Name Dispute Resolution**) <1>.
Споры, связанные с географическими доменами
верхнего уровня, рассматривают организации,
определенные администратором такого домена.

<1> <http://www.icann.org/en/help/dndr/udrpProviders>

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**. В основе данных критериев лежат соображения недобросовестной конкуренции:

1) доменное имя идентично или сходно до степени смешения с товарным знаком или знаком обслуживания, правообладателем которых он является;

2) у владельца доменного имени нет прав или законных интересов в отношении его;

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** не доступны 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 внесударственный характер <1>.

<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.

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 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>.

<1> См., например: [ст. 5](#) Федерального закона от 24 июля 2002 г. N 102-ФЗ "О третейских судах в Российской Федерации" (далее - Закон о третейских судах), в которой сказано, что спор может быть передан на разрешение третейского суда при наличии заключенного между сторонами третейского соглашения; в [ст. 7](#) Закона РФ от 7 июля 1993 г. N 5338-1 "О международном коммерческом арбитраже" говорится, что 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. 2009. N 19. P. 1186.

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" <1>. Правда, данный "продукт", по мнению ряда специалистов, не очень сочетается с российской правовой системой.

<1> 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>.

<1> Серго А.Г., Сокерин К.В. [Особенности защиты права на доменное имя](#) // Юрист. 2007. N 6.

<2> Незнамов А.В. [Подведомственность доменных споров](#) специализированным центрам в системе критериев национальной подведомственности // Арбитражный и гражданский процесс. 2010. N 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 <1>. 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 случае будет идти, скорее, не о создании параллельного механизма, а об адаптации **UDRP** к российским реалиям, что не одно и то же.

<1> Подобно тому, как не имеет практической ценности создание специальной "адаптированной для России" свободной лицензии.

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 недобросовестным 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>.

<1> **Постановление** Тринадцатого арбитражного апелляционного суда от 5 октября 2007 г. по делу N А56-46111/2003.

<2> **Постановление** ФАС Северо-Западного округа от 11 января 2008 г. по делу N А56-46111/2003.

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 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" <1>.

<1> [Постановление](#) Президиума ВАС РФ от 11 ноября 2008 г. N 5560/08.

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, хотя и сделал это под видом конкретизации критериев нарушения содержащегося в [ст. 10.bis](#) Парижской конвенции общего запрета недобросовестной конкуренции, под которой понимается всякий акт

конкуренции, противоречащий честным обычаям в промышленных и торговых делах.

Впоследствии в [Постановлении](#) от 18 мая 2011 г. N 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**.

В Постановлении Президиума Суда по интеллектуальным правам от 28 марта 2014 г. N СП-21/4 "Об утверждении справки по вопросам, возникающим при рассмотрении доменных споров" указано, что "по спорам о доменных именах, тождественных или сходных до степени смешения с товарными знаками, при рассмотрении вопросов о недобросовестности лица, участвующего в деле, суд в соответствии с [п. 1 ст. 5](#), [п. п. 1 и 2 ст. 10](#) ГК РФ, [параграфами 2 и 3 ст. 10.bis](#) Парижской конвенции для установления содержания честных обычаев при регистрации и использовании (администрировании, делегировании и других действиях) доменных имен может использовать положения, сформулированные в Единообразной политике по разрешению споров в связи с доменными именами" ([п. 3](#)).

Так что в настоящее время положения **UDRP** вполне можно считать плотно интегрированными в российскую арбитражную практику в качестве конкретизации существующих в сети Интернет обычаев для целей непосредственного применения норм международного права (Парижской [конвенции](#)).

Следует отметить, что **UDRP** является далеко не единственной процедурой рассмотрения споров в сфере доменных имен, альтернативной судебному судопроизводству. Существует ряд других, более новых

процедур, разработанных **ICANN** и ориентированных на применение в отношении новых доменных зон верхнего уровня.

К их числу следует отнести Единообразную процедуру оперативного приостановления делегирования доменного имени **URS (Uniform Rapid Suspension System)**, которая является упрощенным, более дешевым и оперативным вариантом **UDRP** <1>. Основные отличия **URS** от **UDRP** таковы:

<1> <http://newgtlds.icann.org/en/applicants/urs>

1) **в сфере применения** - URS применяется только к новым функциональным доменам верхнего уровня **gTLD**, принятым **ICANN**, например, .aero, .attorneys, .website и др.), и не применяется к традиционным функциональным доменам вроде .com, .net, .org. UDRP же применяется и к тем и к другим;

2) **в средствах защиты** - в то время как UDRP позволяет требовать передачи спорного доменного имени правообладателю, URS дает возможность лишь приостановить функционирование спорного доменного имени на период его регистрации. При этом с такого домена будет осуществляться переадресация на информационную систему со сведениями о наличии спора по процедуре **URS**. Таким образом, URS не решает вопросы принадлежности доменного имени, она фактически лишь устраняет онлайн-присутствие нарушителя на период действия регистрации доменного имени;

3) **в сроках и стоимости рассмотрения** -

рассмотрение спора по **UDRP** занимает в среднем 60 дней, по **URS** - 16 дней; стоимость рассмотрения жалобы по **UDRP** (в арбитражном центре **WIPO**) составляет в среднем 1500 долларов США, по **URS** - 375 долларов США.

Существуют и иные, менее значительные отличия.

Примером спора по процедуре **URS** является дело **IBM Corporation v. Denis Antipov**, связанное с регистрацией последним доменных имен **ibm.guru** и **ibm.ventures**. Арбитр, вынося решение в пользу **IBM**, отметил, что спорные доменные имена в основной части идентичны товарному знаку заявителя. При этом аргумент ответчика, что данные доменные имена он предполагал использовать для новостного сайта или сайта сообщества, не был признан свидетельствующим о добросовестном характере приобретения соответствующих доменных имен ответчиком <1>.

<1> International Business Machines Corporation v. Denis Antipov. National Arbitration Forum. 12 February. 2014. N FA1402001542313.

В целом процедура **URS** представляет собой значительный интерес как пример дальнейшего развития альтернативных форм рассмотрения споров в сети Интернет. Однако пока она не достигла уровня популярности, сопоставимого с популярностью **UDRP**, главным образом, по причине достаточно слабого средства защиты, предоставляемого ею, - временной приостановки делегирования доменного имени. После окончания срока действия регистрации такого имени

оно снова становится доступным для продажи, и если заявитель упустит этот момент, он может столкнуться с необходимостью заявления еще одного требования.

Другой альтернативной процедурой рассмотрения доменных споров является **PDDRP (Post-Delegation Dispute Resolution Procedure)**, предоставляющая обладателю прав на товарный знак возможность предъявить требования, связанные с нарушением использования его доменного имени, непосредственно в региональную регистратуру (для стран европейского региона - **RIPE NCC**), минуя как администратора, так и непосредственного регистратора доменного имени <1>. Данная процедура, в частности, предназначена для пресечения недобросовестного поведения регистраторов доменных имен, получающих какую-либо выгоду от киберсквоттинга, совершаемого посредством их сервисов. Поскольку администратор доменного имени не является стороной данного разбирательства, решение, выносимое по его итогам, не затрагивает вопросов принадлежности спорного доменного имени, но может содержать санкции в отношении регистратора доменного имени: приостановление права регистрировать новые доменные имена до устранения нарушения, прекращение статуса регистратора <2>.

<1>

<http://newgtlds.icann.org/en/Program-status/Pddrp>

<2> См. подробнее: Arnot J. Navigating Cybersquatting Enforcement in the Expanding Internet // The John Marshall Review of Intellectual Property Law. 2014. Vol. 13. URL: <http://goo.gl/rWdcd4>.

Существуют и иные альтернативные (внесудебные) формы рассмотрения доменных споров, действующие применительно к определенной доменной зоне. Например, **Intellectual Property Defensive Registration Challenge Policy** (Политика рассмотрения претензий, основанных на зарегистрированных правах интеллектуальной собственности) <1>, применяемые к доменной зоне ".pro"; **Charter Eligibility Dispute Resolution Policy** (Правила рассмотрения споров о соответствии регламенту доменной зоны) <2>, применяемые к доменным зонам ".aero", ".coop", ".museum", ".travel"; **Restrictions Dispute Resolution Policy** (Политика рассмотрения споров об ограничениях), применяемые к доменной зоне ".biz" <3> и ряд других <4>.

<1>

<https://www.icann.org/resources/IPages/ipdrpc-2012-02-25-en>

<2>

<https://www.icann.org/resources/IPages/cedrp-2012-02-25-en>

<3>

<https://www.icann.org/resources/IPages/rdrp-2012-02-25-en>

<4> Обзор данных форм рассмотрения доменных споров см.: Гладкая Е.И., Серго А.Г. Доменные споры. Международные системы их рассмотрения. М., 2015.

Применение альтернативных форм рассмотрения доменных споров является эффективным средством избежания сложностей, связанных с рассмотрением споров в государственных судах и сопряженных с этим

юрисдикционных проблем, в частности, исполнения решения суда в отношении иностранного ответчика и (или) регистратора доменного имени.

Однако данные формы рассмотрения споров недоступны в случае возникновения спора по поводу доменного имени, зарегистрированного в зоне .ru (.рф). АПК РФ предусматривает юрисдикцию российских арбитражных судов по рассмотрению подобного рода споров (п. 9 ч. 1 ст. 247). При этом российский регистратор доменного имени обязан исполнять соответствующее решение <1>.

<1> См.: Положение о процедурах, подлежащих применению при возникновении споров о доменных именах, утв. решением Координационного центра национального домена сети Интернет от 20 сентября 2012 г. N 2012-07/47. URL: <http://cctld.ru/files/pdf/docs/litigations.pdf>.

В связи с этим регистрация доменного имени веб-сайта в зоне .ru (.рф) сопряжена с рядом юрисдикционных рисков. Во-первых, споры, связанные с таким доменным именем или коммерческой деятельностью, осуществляемой посредством веб-сайта с этим доменным именем, подчинены юрисдикции российских арбитражных судов и к соответствующим спорным отношениям применяется российское право. Применительно к спорам в сфере доменных имен это может означать, в частности, возможность "обратного захвата" доменного имени владельцем товарного знака, который его зарегистрировал позже регистрации доменного имени. Такая возможность существует в силу нередко отдаваемого российскими арбитражными судами

приоритета праву на товарный знак <1>. И хотя практика в данной сфере является неоднородной <2>, риски в этой сфере все равно остаются. Как отмечается, практика "обратного захвата" "получила в нашей стране широкое распространение при легальной поддержке в законодательстве, что дискредитирует Россию в глазах мирового сообщества" <3>.

<1> Обзор практики см.: Баханец Р. Битва за доменные имена: если понравился чужой домен, смело забирайте его. 19 января 2016 г. URL: <https://vc.rUIP/cliff-2>.

<2> См., например: [Постановление](#) СИП от 4 февраля 2015 г. по делу N A40-58425/2014. В данном случае суды всех инстанций отказали в требовании о запрете использования в доменном имени ответчика обозначения, схожего с зарегистрированным товарным знаком и фирменным наименованием истца, указав на приоритет права на доменное имя, поскольку оно было зарегистрировано ранее дат регистрации истца в качестве юридического лица и приоритета товарного знака. Противоположный подход см.: [Постановление](#) СИП РФ от 15 июля 2014 г. по делу N A41-20527/2013.

<3> Гладкая Е.И., Серго А.Г. Указ. соч. С. 20.

Кроме того, с наличием доменного имени в зоне .ru (.рф) российские регуляторы связывают распространение на владельца такого сайта требований законодательства о рекламе <1>, законодательства о персональных данных <2> (указанные вопросы будут подробно рассмотрены далее).

<1> **Письмо** ФАС РФ от 3 августа 2012 г. N АК/24981 "О рекламе алкогольной продукции в Интернете и печатных СМИ".

<2> <http://www.minsvyaz.ru/ru/Personaldata/>

В связи с этим владелец веб-сайта должен тщательно проанализировать вопрос о целесообразности использования доменного имени, зарегистрированного в зоне .ru (.рф): принимая во внимание, с одной стороны, возможные юрисдикционные риски, а с другой - риски киберсквоттинга (риски захвата ставшего известным доменного имени, изначально зарегистрированного в иной доменной зоне киберсквоттером из зоны .ru или .рф).

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 Интернете, но исполняются в реальном мире, и 2) договоры, которые заключаются и **исполняются** в Интернете.

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 (потокное 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 телекоммуникационных 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>.

<1> Войниканис Е. [Указ. соч.](#) С. 35.

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 <1>. 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 <2>.

<1> Материалы регионального исследования "В стремлении к успеху" ("**The Sky is Rising**"). Floor 64, 2013. <http://www.techdirt.com/skyisrising2/>.

<2> Там же.

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 Интернету: 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.

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), о свободном использовании произведения (ст. ст. 1273 - 1275 ГК РФ) или компьютерных программ (ст. 1280 ГК РФ).

При приобретении цифрового контента его правовой режим устанавливается преимущественно лицензионным договором либо посредством договора оказания услуг. Тем самым регулирование отношений по использованию такого контента осуществляется в договорном порядке, а учитывая повсеместное использование в Интернете конструкций договора присоединения в виде **click-wrap**- и **browsewrap**-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?

<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.

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 лицензируемых объектов авторского права. Существует достаточно большой блок объектов, которые в литературе и на практике обозначаются как объекты виртуальной собственности (**virtualproperty**). 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 обуславливает целесообразность рассмотрения возможных способов ее регулирования и существующей зарубежной практики в данной области.

<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. 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" <1>. 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 обуславливает сложности в ее копировании и передаче. Легкость распространения цифрового контента создает не только дополнительные возможности для правообладателей, но в то же время и дополнительные стимулы для противоправных действий за счет снижения технических барьеров, свойственных традиционным носителям (необходимость специального оборудования, временные затраты и пр.) <2>. Эта особенность цифровой информации особенно усиливается спецификой сети Интернет, обеспечивающей легкость и дешевизну распространения информации безотносительно к ее характеру. То, что ранее было доступно лишь при наличии дорогостоящего оборудования и при прочих условиях, стало доступно для любого заинтересованного индивида. Вследствие этого правообладатели начали больше внимания уделять контролю над частным использованием произведения.

<1> Graham Smith. Op. cit. P. 16.

<2> The Digital Dilemma. Intellectual Property in the

Information Age. Washington: National Academy Press, 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.

2. Неразрывна взаимосвязь цифрового контента и процесса его копирования: для того чтобы получить к нему доступ, произведение 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, являющегося основным устройством, посредством которого контент "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 ним означает **контроль над доступом к такой информации**. 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>.

<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. 1 п. 2 ст. 1270 ГК РФ). Схожие положения содержатся и в американском Законе об авторском праве (§ 117).

<2> Войниканис Е. [Указ. соч.](#) С. 114.

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.

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, то изменение информации, размещенной на веб-сайте, может быть осуществлено без особых проблем. Подобная пластичность в совокупности с легкостью поиска оцифрованного контента за счет возможности его индексирования создает беспрецедентные условия для создания производных произведений на его основе. Как справедливо отмечается, для человека цифровой эпохи свобода означает не только свободу выражать свое мнение или 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.

<1> Войниканис Е. [Указ. соч.](#) С. 204.

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 Интернету, 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 дезинтермедияция). С другой стороны, как еще более чем 40 лет назад отмечал Герберт Саймон (**Gerbert Simon**), "в условиях богатства информации возникает бедность внимания" <1>. 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 обусловлена 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.

<1> Simon H. Designing Organizations for an Information-Rich World: Computers, Communications and Public Interest / Ed. M. Greenberger. Baltimore, 1971.

Рассмотренные отличительные черты, свойственные цифровому контенту, демонстрируют необходимость использования специальных правовых норм, в том числе в сфере договорного права, с целью учета особенностей данной категории объектов. Традиционные договорно-правовые модели вроде договора купли-продажи, история существования которых берет свое начало еще со времен римского права и которые "заточены" под физические объекты, не могут в полной мере учесть особенностей цифрового контента. Как следствие, предоставление схожей по содержанию информации регламентируется различными договорными типами в зависимости от формы и способа предоставления такой информации пользователю.

Как отмечалось ранее, доминирующей договорной моделью для дистрибуции цифрового контента стал 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 произведения <3>. 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.

<1> Схожие положения содержатся в ст. 202 Закона об авторских правах США, где сказано, что "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. 2010. N 62. P. 195.

<3> Подробнее вопрос о возможности и целесообразности распространения положений об исчерпании права на "электронные" экземпляры будет рассмотрен далее.

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 <1>. Лицензионные соглашения либо лицензионные условия в составе комплексных соглашений стали своего рода обычаем (стандартом) в сферах, связанных с использованием высоких технологий, в том числе в сфере распространения цифрового контента <2>.

<1> Winston E. Why Sell What You Can License - Contracting around Statutory Protection of Intellectual Property // George Mason Law Review. 2006. N 14. P. 100.

<2> 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>.

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", снижения цен для некоммерческого использования произведения и т.п. В целом считается, что лицензирование предоставляет более широкий выбор возможностей по обеспечению доступа к информации

<1> The Digital Dilemma. Intellectual Property in the Information Age. Washington: National Academy Press, 2001. P. 101.

Наконец, использование лицензионных договоров достаточно удобно для правообладателей и уполномоченных ими лиц, поскольку позволяет обеспечить гармонию с техническими средствами защиты авторских прав, которые становятся все более популярными в сфере распространения цифрового контента. Такие технические средства 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 обеспечивает тем самым правообладателю больше возможностей для контроля над использованием цифрового контента, предоставляя их ему или иному уполномоченному им лицу. И правообладатели активно пользуются указанной возможностью, противопоставляя 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.

<1> Hugenholtz B. Code as Code, or the End of Intellectual Property as We Know It // Maastricht Journal of European and Comparative Law. 1999. N 6. P. 318.

§ 3. Особенности дистрибуции программного обеспечения в электронной форме по российскому праву

Перипетии применения положений договорного права к отношениям, связанным с дистрибуцией объектов авторского права, в том числе посредством сети Интернет, лучше всего проиллюстрировать на вопросах, связанных с распространением программного обеспечения. Данные отношения успели "обрасти" значительным объемом судебной практики и являются актуальными практически для любой современной организации.

В качестве основных договорных моделей распространения программного обеспечения в указанной сфере можно выделить следующие:

- 1) **договор купли-продажи экземпляров;**
- 2) **лицензионный (сублицензионный) договор.**

При распространении экземпляров компьютерной

программы на основании договоров купли-продажи (поставки) соответствующий экземпляр рассматривается в качестве товара. Его покупатель становится лицом, правомерно владеющим экземпляром программы для ЭВМ, и приобретает права, предусмотренные [ст. 1280](#) ГК РФ. Эти права конкретизируются условиями лицензионного соглашения (при его наличии) с правообладателем, заключаемого в порядке [п. 3 ст. 1286](#) ГК РФ. В случае если экземпляр программы приобретается не напрямую у правообладателя, а у посредника (дистрибьютора, реселлера и т.п.), то такой экземпляр компьютерной программы должен быть лицензионным (неконтрафактным), для чего дистрибьютору необходимо иметь разрешение ("авторизацию") правообладателя на такое распространение, за исключением случаев, когда право на распространение было исчерпано на основании [ст. 1272](#) ГК РФ.

В случае заключения лицензионного договора предполагается предоставление конечному пользователю права использования компьютерной программы на основании лицензионного или сублицензионного договора. В таком случае лицензионный договор обычно заключается конечным пользователем с самим правообладателем напрямую либо с иной компанией, входящей в его группу, которая заключила с правообладателем лицензионный договор.

Предоставление экземпляра программы или возможности получить его путем загрузки в сети Интернет является в таком случае лишь способом исполнения такого лицензионного (сублицензионного) договора, поскольку в отсутствие доступа к экземпляру компьютерной программы невозможно реализовать право на ее использование <1>. Как отметил СИП в

одном из решений, "вопреки выводам судов первой и апелляционной инстанций, передача материального носителя (дистрибутива), являющегося формой распространения программного обеспечения, в рамках лицензионного договора наряду с передачей во временное пользование исключительных прав на результат интеллектуальной деятельности, не свидетельствует о смешанном характере такого договора, поскольку передача дистрибутива, содержащего программу для начальной инициализации системы, сама по себе не может быть предметом договора без предоставления прав использования программы" <2>.

<1> См.: Савельев А.И. [Актуальные вопросы судебной практики](#) в сфере оборота программного обеспечения в России // Вестник Высшего Арбитражного Суда РФ. 2013. N 4. Примечательно, что данный "пассаж" неоднократно воспроизводился в судебных решениях. См., например: Постановления Пятнадцатого апелляционного суда от 18 июля 2014 г. по делу [N A53-25097/2013](#), от 14 февраля 2015 г. по делу [N A53-25093/2013](#).

<2> [Постановление](#) СИП от 5 июня 2014 г. по делу N A40-88983/2013.

В целом указанное разграничение является вполне понятным и долгое время не вызывало особых споров на практике. Однако в последние годы ситуация в значительной степени изменилась.

Во-первых, традиционные способы распространения компьютерных программ в виде

"коробочных" версий (**retail version**) все более и более вытесняются способами распространения их в электронной форме: посредством предоставления ссылок для скачивания и в некоторых случаях также ключей, необходимых для активации установленной программы. Это обусловлено 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 обязательных таможенных процедур в случае импорта материальных носителей программы <1>.

<1> В соответствии с [письмом](#) Федеральной таможенной службы России от 17 марта 2006 г. N 15-14/8524 "О таможенном оформлении информации, передаваемой по сети Интернет таможенному оформлению подлежит не информация (компьютерная программа, мобильный контент), перемещаемая в Сети 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.).

Во-вторых, существенные корректировки внесли и изменения в налоговом законодательстве. С 2008 г. в соответствии с Налоговым кодексом РФ не подлежит

обложению НДС реализация прав использования компьютерных программ на основании лицензионных договоров (подп. 26 п. 2 ст. 149 НК РФ). Данное положение было разъяснено Минфином России, которое распространило действие данной льготы и на сублицензионные договоры со ссылкой на п. 5 ст. 1238 ГК РФ, согласно которому к таким договорам применяются нормы о лицензионном договоре <1>.

<1> **Письмо** Минфина России от 1 апреля 2008 г. N 03-07-15/44 "О взимании НДС с операций по передаче прав на использование результатов интеллектуальной деятельности". Следует отметить, что данная позиция является небезупречной с гражданско-правовой точки зрения. Согласно п. 3 ст. 2 ГК РФ гражданское законодательство по общему правилу не применяется к налоговым отношениям, за исключением случаев, прямо предусмотренных законодательством. Ни НК РФ, ни ГК РФ не содержат специальных правовых норм о применимости положений НК РФ о лицензионном договоре также и к сублицензионным соглашениям.

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. Особенно этот подход стал актуальным для тех пользователей программного обеспечения, которые реализуют свои товары или услуги без НДС (главным образом для банков и страховых организаций), поскольку они не могут принять к вычету "входной" НДС.

На юридическую сомнительность данной

практики уже неоднократно указывалось в литературе <1>. Основной проблемой является тот факт, что зарубежные правообладатели обычно не предоставляют дистрибьюторам прав на установку и непосредственное использование программы, а дают лишь право на распространение <2>, 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, заключаемого в упрощенном порядке, предусмотренном в п. 5 ст. 1286 ГК РФ (так называемые оборотные лицензии, или **click-wrap-лицензии**). Данное соглашение заключается при загрузке или установке программного продукта. Ценность такого **click-wrap-соглашения** для правообладателя состоит не столько в дани традиции, сколько в возможностях, которые предоставляет наличие прямых отношений с конечным пользователем. В частности, возможность в одностороннем порядке изменять лицензионные метрики при развитии технологий, регламентировать порядок проведения аудита развернутого программного обеспечения и т.д. Вместе с тем конечный пользователь также приобретает определенные преимущества от наличия такого соглашения: он перестает быть зависимым от состояния договорных отношений в цепочке правообладатель - лицензиат - сублицензиат. В приведенной классической sublicензионной схеме, если по каким-либо причинам правообладатель разрывает договор с лицензиаром (деавторизует дистрибьютора), то согласно ст. 1238 ГК РФ прекращают свое действие и sublicензионный договор, и основанное на нем право использования программы конечным пользователем. Или другой пример. Срок

действия сублицензионного договора не может выходить за пределы срока действия лицензионного договора, лежащего в его основе, что создает риски для приобретения программных продуктов на условиях "вечной лицензии" (т.е. действительной в течение всего срока действия исключительного права). Наличие же прямого лицензионного соглашения с правообладателем по модели **click-wrap** позволяет урегулировать вопрос о сроке действия лицензии непосредственно в нем, освобождаясь тем самым от рисков, связанных со статусом партнерских соглашений, заключенных между правообладателями и посредниками.

<1> 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. N 3; Домрачева Е. [Неоднозначная льгота](#) // ЭЖ-Юрист. 2008. N 36; Вычугжанин Р.А. [Лицензия на софт](#) // ЭЖ-Юрист. 2009. N 3.

<2> См., например: пояснения компании по вопросам лицензионной политики в решении Арбитражного суда г. Москвы от 6 сентября 2010 г. по делу N А40-80627/10-118-416; [Постановление](#) ФАС Московского округа от 1 сентября 2011 г. N КА-А40/9419-11 по делу N А40-140882/10-129-522.

Правда, структура договорных отношений, при которой конечный пользователь заключает сублицензионный договор с посредником, впоследствии заключая еще и лицензионное соглашение с

правообладателем, страдает одним существенным недостатком. Если право воспроизведения и использования программы, понимаемое в данном случае как возможность осуществления действий, необходимых для функционирования программы в соответствии с ее назначением (формулировка взята из [п. 1 ч. 1 ст. 1280 ГК РФ](#)), предоставляется на основании **click-wrap-соглашения** с правообладателем, легитимность которого не оспаривается ни в законодательстве, ни в судебной практике <1>, то оно не может одновременно предоставляться другим лицом на основании иного соглашения: одно и то же право не может возникать на основании двух разных соглашений с разными лицами. Как следствие, соглашения, заключаемые между посредниками и конечными пользователями, в большинстве случаев не обладают признаками лицензионных или сублицензионных соглашений, так как по ним конечному пользователю не предоставляется ни одного правомочия, входящего в состав исключительных прав в соответствии со [ст. 1270 ГК РФ](#).

<1> Так, особенности правового режима таких соглашений были разъяснены в Постановлении Пленума ВС РФ N 5 и Пленума ВАС РФ N 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](#)).

Возникает вопрос, как тогда следует квалифицировать такие соглашения? Если в их рамках осуществляется предоставление материального носителя, то подобные "сублицензионные" договоры должны рассматриваться как договоры купли-продажи материальных носителей, при условии что

предполагается последующее заключение лицензионного договора в порядке п. 5 ст. 1286 ГК РФ <1>. Однако вопрос в том, как квалифицировать аналогичные договоры, которые заключаются между посредниками и конечными пользователями и в рамках которых предоставляется не материальный носитель, а лишь ссылка на ресурс, где можно скачать дистрибутив программы и (или) регистрационный код (ключ активации)?

<1> Письмо Минфина России от 1 апреля 2008 г. N 03-07-15/44 "О взимании НДС с операций по передаче прав на использование результатов интеллектуальной деятельности".

По причинам, указанным ранее, сублицензионным договором такие соглашения считать в ряде случаев нельзя по причине отсутствия предоставления права использования (осуществления действий, необходимых для функционирования программы в соответствии с ее назначением) программного обеспечения по цепочке правообладатель - дистрибьютор - (реселлер) - конечный пользователь. Такое право возникает у пользователя на основании лицензионного соглашения с правообладателем, заключаемым напрямую в порядке п. 5 ст. 1286 ГК РФ. Однако, если такого соглашения не будет и соответствующее право будет "транслировано" через посредников по цепочке соглашений от правообладателя к конечному пользователю, то квалификация соглашения между конечным пользователем и посредником, предоставляющим ему соответствующий регистрационный код (ключ), в качестве сублицензионного вполне возможна.

Иногда на практике встречается и иной вариант структурирования таких отношений - договор купли-продажи с оформлением товарно-транспортной накладной. Однако такая квалификация не укладывается в классические каноны положений о купле-продаже, объектом которой является товар, а в качестве такового 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 по договору в том смысле, о котором здесь идет речь, - договору цессии имущественного права, в основании которого лежит договор купли-продажи <1>. 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 сделку по их отчуждению (продаже) - договором купли-продажи <2>. 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 материального объекта, сколько в качестве посредника, обеспечивающего возможность приобретения лицензионного (неконтрафактного) экземпляра программного продукта, а в ряде случаев также "пропускающего через себя" лицензионный платеж.

<1> См.: например: Новоселова Л.А. [Сделки уступки права \(требования\)](#) в коммерческой практике. Факторинг. М., 2003.

КонсультантПлюс: примечание.

[Монография](#) М.И. Брагинского, В.В. Витрянского "Договорное право. Договоры о передаче имущества" (книга 2) включена в информационный банк согласно публикации - Статут, 2002 (4-е издание, стереотипное).

<2> См.: Брагинский М.И., Витрянский В.В. Договорное право. Книга вторая: Договоры о передаче имущества. М., 2003. С. 265 - 266.

Таким образом, мы приходим к следующим выводам относительно правовой природы соглашений, заключаемых при приобретении компьютерной программы конечным пользователем у посредника:

1) при наличии материального носителя - это купля-продажа (поставка);

2) при электронной форме распространения компьютерной программы и отсутствии заключаемого впоследствии прямого лицензионного соглашения между конечным пользователем и правообладателем ([п. 5 ст. 1286](#) ГК РФ) - это сублицензионный договор;

3) при электронной форме распространения компьютерной программы и наличии заключаемого впоследствии прямого лицензионного соглашения между конечным пользователем и правообладателем ([п. 5 ст. 1286](#) ГК РФ) - это посреднические услуги (как представляется, преимущественно агентского характера). Именно квалификация указанных отношений в качестве посреднических услуг представляется наиболее адекватной, поскольку она корректно "улавливает" суть отношений и позволяет учитывать нематериальный характер предоставляемого "блага".

Но поскольку квалификация по п. 3 данного перечня не позволяет воспользоваться налоговой льготой по [подп. 26 п. 2 ст. 149](#) НК РФ, налоговые соображения нередко приводят к деформации гражданско-правовой природы договора.

Интересно, что в спорах с налоговой службой суды нередко встают на сторону налогоплательщика.

Так, в поле зрения налогового органа попала схема, при которой программное обеспечение, принадлежащее **Microsoft** и **Лаборатории Касперского**, было приобретено конечным пользователем у реселлера (ООО "Открытые Технологии") на основании сублицензионного договора, который, в свою очередь, приобрел его на основании сублицензионного договора у ООО "Монт Волгоград".

Возник спор, в процессе рассмотрения которого налоговый орган заявил о неправомерности применения реселлером льготы, предусмотренной [подп. 26 п. 2 ст. 149 НК РФ](#) в отношении операций по реализации (передаче) прав на использование программ для ЭВМ по сублицензионным договорам конечным пользователям. По мнению инспекции, представленные налогоплательщиком (реселлером) сублицензионные договоры не соответствуют требованиям части четвертой [ГК РФ](#) и являются договорами купли-продажи товаров, реализация которых облагается НДС. Кроме того, налоговый орган полагал, что положения [подп. 26 п. 2 ст. 149 НК РФ](#) не подлежат применению ввиду отсутствия у реселлера права на заключение сублицензионных договоров.

Исследуя вопрос о соотношении договора купли-продажи и лицензионного договора, судебные инстанции пришли к выводу, что предметом договора с конечным пользователем являлось именно неисключительное право на воспроизведение программного обеспечения и его использование в объеме, определенном договором. Суды сочли названные договоры соответствующими требованиям, предъявляемым к лицензионным договорам, поскольку они содержат указание на результат интеллектуальной деятельности (право на использование программ для ЭВМ) и способ его использования. Кроме того, суд подчеркнул, что [НК РФ](#) не устанавливает для налогоплательщика обязанности подтверждать наличие у него полномочий на передачу сублицензиатам прав на использование программ для ЭВМ. В данном случае действует принцип добросовестности налогоплательщика, установленный [п. 7 ст. 3 НК РФ](#). При этом бремя доказывания направленности действий налогоплательщика на получение необоснованной

налоговой выгоды, в частности налоговой льготы, возложено на налоговую инспекцию <1>.

<1> [Постановление](#) ФАС Северо-Кавказского округа от 14 ноября 2014 г. по делу N А53-25097/2013.

В целом вопрос о правовой природе соглашений, заключаемых в сфере цифровой дистрибуции программного обеспечения, пока еще далек от своего окончательного разрешения. Многое будет зависеть от политики налоговых органов по отношению к существующим схемам распространения программных продуктов в России, ведь такие схемы во многом являются следствием особенностей отечественного налогового регулирования. Уже сейчас можно найти зачатки ограничительного подхода налоговых органов и судов к применению налоговой льготы в соответствии с [подп. 26 п. 2 ст. 149](#) НК РФ, продемонстрированного применительно к отношениям, связанным с налогообложением доходов от продажи цифрового контента в рамках онлайн-игр <1>. Не исключено, что в условиях кризиса и при необходимости увеличения поступлений в бюджет налоговые органы будут более пристально анализировать заключаемые при дистрибуции программного обеспечения соглашения на предмет обоснованности применения налоговых льгот, а суды будут более лояльными к их выводам. Либо, что более вероятно, спорная налоговая льгота, предусмотренная [подп. 26 п. 2 ст. 149](#) НК РФ, не имеющая аналогов в зарубежном налоговом законодательстве, будет отменена. Соответствующие инициативы уже появились на момент подготовки данного издания <2>.

<1> Речь идет о нашумевшем судебном споре налогового органа с компанией ООО "Мэйл.ру Геймз". См.: [Постановление](#) ФАС Московского округа от 18 июня 2015 г. по делу А40-91072/2014 и акты нижестоящих судов. Подробно указанное дело будет рассмотрено далее.

<2> [Проект](#) Федерального закона N 962487-6 "О внесении изменений в части первую и вторую Налогового кодекса Российской Федерации". Данный [законопроект](#) представляет собой масштабные изменения в налоговое законодательство с целью адаптации его к реалиям электронной коммерции. Применительно к [подп. 26 п. 2 ст. 149](#) НК РФ им предлагается исключить из перечня освобожденных от НДС операций права на использование программ для ЭВМ, предоставляемые на основании лицензионного договора. Ожидается, что данная льгота будет отменена с 1 января 2017 г.

§ 4. Предоставление удаленного доступа как особая модель распространения цифрового контента

В последнее время все большую популярность приобретают онлайн-сервисы, предоставляющие возможность удаленного доступа к цифровому контенту: потоковому видео и аудио, новостям, программному обеспечению и т.п. Причем наибольшее внимание в отечественной юридической литературе и практике уделяется рассмотрению вопросов квалификации договоров на предоставление удаленного доступа к компьютерным программам, в связи с чем анализ договорно-правовых аспектов рассматриваемой

бизнес-модели лучше всего проводить именно на примере данного вида объектов.

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** <1>. Далее в настоящей работе в отношении договоров на предоставление удаленного доступа к функционалу программного обеспечения будет использоваться термин **SaaS**.

<1> Абстрагируясь от отдельных технических аспектов функционирования облачных сервисов, в целом данное определение облачного сервиса можно представить в упрощенном виде как автоматизированный способ предоставления вычислительных мощностей, в том числе программного обеспечения, в режиме удаленного доступа через сеть Интернет по запросу клиента. Или еще проще: под облачными сервисами можно понимать технологическую модель, при которой вместо какого-либо физического ресурса предоставляется его виртуальная модель.

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 ИТ-сфере нередко носят маркетинговый характер и в связи с этим не обязаны точно передавать правовую суть явления. В юридической литературе до сих пор не утихают споры относительно того, к какому типу договора следует отнести **SaaS**.

Из всего многообразия договорных конструкций можно выделить два основных типа договоров, которые могут быть использованы для оформления **SaaS**-отношений: лицензионный договор и договор возмездного оказания услуг <1>. Рассмотрим подробнее аргументы за и против соответствующей квалификации.

<1> Кроме того, в качестве кандидатов "второй очереди" можно упомянуть договор аренды, смешанный и непоименованный договоры. См. подробнее: Савельев А.И. [Правовая природа "облачных" сервисов: свобода договора, авторское право и высокие технологии](#) // Вестник гражданского права. 2015. N 5.

При обосновании применения лицензионного договора используются 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 <1>. Например, использование 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 правомочие можно было бы условно обозначить как "предоставление доступа к программе посредством сети Интернет или "использование **SaaS**-версии программы". В таком случае не следует путать данный способ с правомочием доведения до всеобщего сведения ([подп. 11 п. 2 ст. 1270 ГК РФ](#)), которое тоже относится к использованию произведения в Интернете. 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.

<1> См.: [Комментарий](#) к части четвертой Гражданского кодекса Российской Федерации / Под ред. А.Л. Маковского. М., 2008. С. 403.

2. Минимизация регуляторных рисков.

Предоставление **SaaS** по модели лицензионного договора позволяет минимизировать риски, связанные с признанием предложений данного типа услугами связи, требующими получения лицензии. Такие риски обусловлены широким определением в законодательстве понятия "услуги связи", с одной стороны, и отсутствием дефиниции понятия "телематическая услуга связи" - с другой. В соответствии с [п. 32 ст. 2 Закона о связи](#) услуга связи -

это деятельность по приему, обработке, хранению, передаче, доставке сообщений электросвязи или почтовых отправлений. С формально-технической точки зрения функционирование облачного сервиса предполагает обмен сообщениями между сервером провайдера и устройством пользователя, т.е. их прием, обработку и передачу, а иногда и хранение. В соответствии с [Постановлением](#) Правительства РФ от 18 февраля 2005 г. N 87 <1> предоставление пользователю возможности приема и передачи телематических электронных сообщений охватывается понятием "телематическая услуга связи". При этом само определение телематической услуги связи отсутствует как в данном [Постановлении](#), так и в [Правилах](#) оказания телематических услуг связи <2>. Схожая неопределенность имеет место и в отношении услуг хостинга, с которыми отдельные виды облачных сервисов могут иметь некое родство. Использование иных договорных моделей позволяет лишний раз не привлекать внимание правоприменительных органов, осуществляющих контроль за соблюдением законодательства о лицензировании и связи.

<1> [Постановление](#) Правительства РФ от 18 февраля 2005 г. N 87 "Об утверждении перечня наименований услуг связи, вносимых в лицензии, и перечней лицензионных условий" (в ред. от 24 января 2008 г.).

<2> [Постановление](#) Правительства РФ от 10 сентября 2007 г. N 575 "Об утверждении Правил оказания телематических услуг связи". При этом дефиниция телематического электронного сообщения, содержащаяся в данных [Правилах](#), также не добавляет какой-либо юридической определенности:

"телематическое электронное сообщение" - это одно или несколько сообщений электронной связи, содержащих информацию, структурированную в соответствии с протоколом обмена, поддерживаемым взаимодействующими информационной системой и абонентским терминалом.

3. Организационные соображения.

Структурирование **SaaS** по модели лицензионного договора может быть более удобным при продвижении решения **SaaS** к конечному пользователю через цепочку посредников. Предоставление услуг облачного сервиса по цепочке гораздо проще структурировать как передачу лицензии по аналогии с широко используемыми вендорами классическими моделями дистрибуции программного обеспечения, чем как "передачу услуг" с последующим заключением ряда субподрядных договоров. Если соответствующий облачный сервис принадлежит провайдеру, который одновременно выступает производителем программного обеспечения, и доступ к такому сервису предоставляется через сеть дистрибьюторов, то использование конструкции лицензионного договора позволяет вендору и дистрибьюторам использовать те же контрактные документы и процедуры, что и для распространения лицензий на программное обеспечение, значительно облегчая процесс вывода на рынок соответствующего сервиса.

4. **Налоговые соображения.** Отношения по предоставлению удаленного доступа к программе посредством Интернета также нередко становятся предметом налоговой оптимизации и оформляются лицензионным договором с целью применения льготы по НДС, о которой уже говорилось ранее <1>.

<1> В скором времени, уже с 1 января 2017 г., данный аспект может утратить свою актуальность в связи с отменой соответствующей льготы. См.: [Проект федерального закона N 962487-6 "О внесении изменений в части первую и вторую Налогового кодекса Российской Федерации"](#).

В пользу применения к **SaaS** конструкции договора возмездного оказания услуг можно привести следующие аргументы.

1. **Соответствие технической стороне возникающих отношений.** Основные действия по исполнению договора совершаются на стороне провайдера **SaaS**: "информация хранится и обрабатывается на оборудовании исполнителя. Логические операции также производятся на оборудовании исполнителя" <1>. 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?" <2>. Действительно, пользователь **SaaS** не имеет **технической** возможности использования программы без непосредственного и **постоянного** участия провайдера. Данный факт позволяет говорить о том, что связь между сторонами **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.

<1> Серов А. [SaaS: программное обеспечение или услуга?](#) // ЭЖ-Юрист. 2011. N 17.

<2> [Там же.](#)

2. Соответствие коммерческим аспектам возникающих отношений. Договор возмездного оказания услуг учитывает специфику регулирования вопросов оплаты. В соответствии со [ст. 781](#) ГК РФ заказчик обязан оплатить оказанные ему услуги в сроки и в порядке, которые указаны в договоре возмездного оказания услуг. Данный порядок оплаты полностью соответствует основному преимуществу облачных сервисов, выражающегося в возможности платить исключительно за фактически потребленные вычислительные мощности (**pay as you go**). Напротив, лицензионный договор предполагает возникновение обязанности по уплате вознаграждения за сам факт предоставления права, а не за его фактическое использование <1>.

<1> См.: Постановление Пленума ВС РФ и Пленума ВАС РФ от 26 марта 2009 г. N 5/29, [п. 13.7](#).

Кроме того, появляется возможность регулирования отношений, связанных с качеством предоставляемых облачных сервисов, в том числе путем заключения соглашений об уровне сервиса (**Service level agreements, SLA**). Дело в том что вопросы качества предоставляемого в рамках

лицензионного договора программного обеспечения никоим образом не регулируются в части четвертой ГК РФ и существующая судебная практика исходит из того, что предмет лицензионного договора - "неисключительное право, которое, не являясь вещью, не может быть некачественным" <1>. В то же время правовое регулирование договора возмездного оказания услуг предполагает возможность субсидиарного применения норм о договоре подряда (ст. 783 ГК РФ), а общие положения договора подряда (ст. ст. 724, 725 ГК РФ) содержат детальную регламентацию вопросов качества работы, в частности, возможность сторон своим соглашением установить соответствующие параметры качества и ответственность за их несоблюдение.

<1> Постановления ФАС Московского округа от 2 июля 2013 г. по делу N A40-111104/12-26-947, от 30 сентября 2009 г. N КГ-A40/9849-09.

Наконец, нормы о договоре возмездного оказания услуг содержат положения о возможности одностороннего отказа от договора каждой из сторон (ст. 782 ГК РФ). При этом в соответствии с разъяснениями Пленума ВАС РФ стороны коммерческого договора могут самостоятельно определять порядок и последствия реализации данного права <1>. Иными словами, стороны могут в любой момент отказаться от договора, который стал им в тягость, и при этом адаптировать режим расторжения к своим потребностям. Нормы о лицензионном договоре таких положений "по умолчанию" не содержат, связывая стороны всерьез и надолго.

<1> **Пункт 4** Постановления Пленума ВАС РФ от 14 марта 2014 г. N 16 "О свободе договора и ее пределах".

3. Квалификация SaaS по модели договора возмездного оказания услуг позволяет подчеркнуть наличие у провайдера таких сервисов статуса информационного посредника. Это позволяет им воспользоваться специальными положениями об освобождении от ответственности при распространении запрещенных видов информации с использованием их сервисов. Так, в соответствии с **п. 3 ст. 17** Федерального закона от 27 июля 2006 г. N 149-ФЗ "Об информации, информационных технологиях и защите информации" (далее - Закон об информации) "в случае, если распространение определенной информации ограничивается или запрещается федеральными законами, гражданско-правовую ответственность за распространение такой информации не несет лицо, оказывающее услуги:

1) либо по передаче информации, предоставленной другим лицом, при условии ее передачи без изменений и исправлений;

2) либо по хранению информации и обеспечению доступа к ней при условии, что это лицо не могло знать о незаконности распространения информации".

Из указанной нормы следует, что лицо, претендующее на применение специальных оснований освобождения от ответственности, должно предоставлять свои решения именно по модели договора об оказании услуг, а не какого-либо иного договора, в том числе лицензионного. Данное положение **Закона** об информации может иметь

значение для решения вопроса об освобождении провайдера облачного сервиса от ответственности за распространение информации, порочащей честь, достоинство или деловую репутацию какого-либо лица, либо от ответственности перед субъектом персональных данных за обработку таких данных, осуществляемую в облаке <1>.

<1> См. подробнее: [Комментарий](#) к Федеральному закону от 27 июля 2006 г. N 149-ФЗ "Об информации, информационных технологиях и защите информации" (постатейный). М.: Статут, 2015. С. 308 - 311.

Следует сразу оговориться, что квалификация **SaaS** в качестве договора оказания услуг 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 функционала программы, предоставляемой 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.

Проанализировав возможные преимущества и аргументы в пользу обеих договорных конструкций, следует ответить на вопрос о том, какой тип договора является наиболее адекватным применительно к **SaaS с точки зрения существа возникающих отношений**.

Одним из основных критериев "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 описанным и достаточно очевидным критерием, то квалификация **SaaS** в качестве лицензионного договора с применением норм авторского права 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 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 полномочия, которые предоставляются на основании лицензионного договора. Но пользователь не осуществляет использование экземпляра программы каким бы то ни было способом, требующим вмешательства авторского права. Он получает 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.

<1> См.: Серов А. [Указ. соч.](#)

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.

<1> Разуваев В.Э. [Софт как услуга](#) // ЭЖ-Юрист. 2010. N 5.

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.

Тем не менее в отечественной доктрине продолжают высказываться мнения в пользу лицензионной природы договора **SaaS** <1>. Наиболее иллюстративной является позиция ректора РГАИС профессора И.А. Близнеца, который, отвечая на вопрос о правовой природе **SaaS**, утверждает, что "здесь можно дать однозначный ответ. Поскольку программные продукты охраняются нормами авторского права, то использование договора услуг в данном случае неприемлемо. Должно заключаться стандартное лицензионное соглашение независимо от того, как этот программный продукт распространяется - посредством установки на компьютер покупателя или через облако. И такой точки зрения придерживается большинство стран мира" <2>. Хотя профессор говорит лишь о **SaaS**, в принципе данные соображения применимы к любым случаям использования объектов авторского права посредством получения к ним доступа по Интернету.

<1> Разуваев В.Э. [Софт как услуга](#) // ЭЖ-Юрист. 2010. N 5.

<2> Интернет-интервью с И.А. Близнецом, ректором Российской государственной академии интеллектуальной собственности: "[Реализация государственной политики](#) в области интеллектуальной собственности" от 20 мая 2015 г. // СПС "КонсультантПлюс";

<http://www.consultant.ru/law/interview/bliznets2/>.

При всей внешней логичности данного мнения, оно, на наш взгляд, является неверным во всех своих основных тезисах, коих, по сути, три:

1) использование программ для ЭВМ возможно лишь на основании лицензионного договора, использование иных договоров неприемлемо;

2) способ использования программного обеспечения не имеет значения для целей указанной квалификации, равно как и факт наличия или отсутствия экземпляра программы у пользователя при таком использовании;

3) во всех остальных высокоразвитых странах применяется аналогичный подход.

В отношении первого тезиса можно привести как минимум **два возможных возражения**.

Во-первых, принцип свободы договора ([ст. 421](#) ГК РФ) никто не отменял, и никаких ограничений применительно к сфере использования программного обеспечения он не содержит. ГК РФ допускает возможность заключения иных договоров по поводу программного обеспечения, например договора доверительного управления (исключительные права прямо указаны в числе объектов доверительного управления в [ст. 1013](#) ГК РФ). Другой вопрос: имеет ли это смысл? Кроме того, вполне возможны ситуации, когда пользователь программы является "лицом, правомерно владеющим экземпляром программы для ЭВМ". В таком случае в соответствии со [ст. 1280](#) ГК РФ он может использовать такую программу в указанных

законом пределах без какого-либо лицензионного договора.

Во-вторых, если применить высказанные И.А. Близнецом идеи к повседневной практике, то получится, что при **любом** (!) посещении и использовании веб-сайтов в сети Интернет будет требоваться наличие лицензионного договора, так как в составе веб-сайта всегда есть компьютерная программа, удаленный доступ к которой осуществляется посредством браузера, как и в случае с **SaaS**. Ведь в соответствии с **п. 13 ст. 2** Закона об информации сайт в сети Интернет представляет собой "**совокупность программ для ЭВМ** и иной информации, содержащейся в информационной системе, доступ к которой обеспечивается посредством сети Интернет по доменным именам и (или) по сетевым адресам (Выделено мной. - **А.С.**)". Очевидно, что такой подход имеет определенные проблемы со здравым смыслом и сложившейся практикой, что, по-видимому, может быть объяснено ложностью заложенных в него предпосылок.

В отношении второго тезиса необходимо отметить следующее. Как отмечалось ранее, в случае с **SaaS** и иными облачными сервисами программное обеспечение установлено на оборудовании провайдера и находится под его полным контролем, пользователь получает лишь возможность удаленного доступа к его отдельным функциям ("полезным свойствам"). Использование программы в классическом "авторско-правовом" смысле со стороны пользователя при этом не осуществляется: он потребляет результаты использования программы другим лицом, в данном случае - провайдером облачного сервиса. К схожему выводу приходят и германские юристы, утверждающие, что "поскольку в случае с **SaaS** выполнение программы

с технической точки зрения осуществляется за пределами компьютера пользователя, со стороны пользователя не совершается ее использования с точки зрения авторского права, и, как следствие, какого-либо специального разрешения от правообладателя на него не требуется" <1>.

<1> Spindler G. Rechtliche Rahmenbedingungen des "Software as a Service" Konzepts // Software-as-a-Service: Anbieterstrategien, Kundenbedürfniss und Wertschöpfungsstrukturen / Benlian A., Hess Th., Buxmann P. (Hgs.). S. 37.

Отдельные фрагменты программы, используемой в удаленном режиме, конечно, воспроизводятся в оперативной памяти на устройстве пользователя. Однако в соответствии с [подп. 1 п. 2 ст. 1270 ГК РФ](#) такое воспроизведение не имеет последствий с точки зрения авторского права: "Не считается воспроизведением краткосрочная запись произведения, которая носит временный или случайный характер и составляет неотъемлемую и существенную часть технологического процесса, имеющего единственной целью правомерное использование произведения либо осуществляемую информационным посредником между третьими лицами передачу произведения в информационно-телекоммуникационной сети, при условии что такая запись не имеет самостоятельного экономического значения". В случае с использованием функционала программного обеспечения, предоставляемого в рамках облачных сервисов, данные условия выполняются в полной мере.

Так что наличие или отсутствие у пользователя

экземпляра программного обеспечения имеет важное значение для целей квалификации отношений, возникающих в связи с его использованием.

Третий же тезис сторонников применения конструкции лицензионного договора, согласно которому данный подход принят в большинстве стран мира, также опровергается даже поверхностным анализом практики некоторых зарубежных стран.

Так, в Германии Верховный суд рассматривал спор, возникший из договора на использование бухгалтерского программного обеспечения в удаленном режиме, через призму договора аренды, а не лицензионного договора <1>. По мнению суда, тот факт, что компьютерная программа защищена авторским правом, никоим образом не влияет на правовую природу основной обязанности провайдера по предоставлению доступа к ней, которая в равной степени может возникать в отношении как защищенных, так и не защищенных авторским правом программ, а лишь предполагает необходимость наличия дополнительных договорных условий, которые нужны для совершения действий, указанных в ст. 69 (с) немецкого Закона об авторских и смежных правах 1965 г. и требующих разрешения правообладателя (воспроизведение, переработка, распространение и т.д.).

<1> См: BGH, 15.11.2006 - XII ZR 120/04 (http://medien-internet-und-recht.delPdf/vt_MIR_Dok._009-2006.pdf).

Во Франции суд квалифицировал договор по

предоставлению программного обеспечения по управлению базой данных в удаленном режиме, заключенный между компаниями **Oracle** и **UMP**, именно в качестве договора оказания услуг (**le contrat de prestation de service**) <1>.

<1> Tribunal de grande instance de Nanterre
Ordonnance de référé 30 novembre 2012. URL:
[http://www.legalis.net/spip.php?page=jurisprudence-detision
&id_article=3794](http://www.legalis.net/spip.php?page=jurisprudence-detision&id_article=3794).

В США также существуют различные точки зрения по поводу квалификации облачных сервисов <1>.

<1> См. описание зарубежных подходов в кн.: Савельев А.И. **Правовая природа облачных сервисов: свобода договора, авторское право и высокие технологии** // Вестник гражданского права. 2015. N 5.

Таким образом, бесспорных оснований для безусловного отнесения договоров **SaaS** к разряду лицензионных договоров нет. Наиболее адекватной существу возникающих из договора **SaaS** отношений договорной конструкцией является договор возмездного оказания услуг. При этом по российскому праву можно квалифицировать такого рода соглашения и как лицензионные договоры, и как договоры возмездного оказания услуг, в зависимости от налоговых, организационных и маркетинговых соображений <1>. Анализ судебной практики показывает, что в большинстве своем суды придерживаются той квалификации, которую выбрали сами стороны.

Наиболее распространенной в судебной практике является квалификация подобного рода договоров как договоров возмездного оказания услуг <2>.

<1> Договоры **SaaS** могут быть и 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. Но 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. 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. N 4.

<2> **Постановление** Четвертого арбитражного апелляционного суда от 19 декабря 2014 г. N 04АП-4738/2014 по делу N А78-5032/2014; решений Арбитражного суда Забайкальского края от 26 января 2015 г. по делу N А78-14182/2014, Арбитражного суда Новосибирской области от 4 июня 2014 г. по делу N А45-402/2014.

При применении лицензионного договора рекомендуется последовательно использовать в нем терминологию, свойственную именно лицензионным договорам ("лицензиар", "лицензиат", "использование ПО"), избегая терминов, свойственных другим договорам ("услуга", "исполнитель", "заказчик" и т.п.), и обозначений вроде "облачный сервис", а также четко специфицировать программное обеспечение, которое используется при предоставлении облачного сервиса. Договор будет выглядеть вполне "по-лицензионному", и суд или иной правоприменительный орган вряд ли будет оспаривать такую его квалификацию. Так, например, в одном из споров стороны заключили договор о предоставлении доступа к **SaaS**-версии программного комплекса **CRM** "Клиенты и продажи" на период пользования им сроком один месяц. Данный договор был структурирован по модели лицензионного договора. Суд поддержал указанную квалификацию, взыскав с лицензиара уплаченную лицензиатом сумму аванса в связи с неисполнением лицензиаром обязанности по предоставлению доступа к программе <1>.

<1> Решение Арбитражного суда г. Москвы от 24

июля 2015 г. по делу N A40-85252/15.

Представляется, что вышеприведенные соображения в значительной степени применимы и к иным видам контента (получению доступа к потоковому видео или аудио). Поскольку соответствующие виды объектов, так же как и компьютерные программы, относятся к объектам авторского права, в условиях существования открытого перечня правомочий на их использование в [ст. 1270 ГК РФ](#) вполне возможно заключение лицензионного договора. Однако в силу тех же самых соображений, что и с программным обеспечением, наиболее адекватной договорной конструкцией для отношений по предоставлению удаленного доступа к цифровому контенту является договор возмездного оказания услуг.

В завершение необходимо сделать еще один важный вывод, который следует из приведенного анализа. Поскольку вся система правомочий, входящих в состав авторского права субъекта, рассчитана на распространение копий (экземпляров) произведений и воспринимается как основной способ реализации авторского права, современные бизнес-модели распространения цифрового контента, при которых экземпляры не распространяются, а предоставляется лишь некое право доступа к объектам авторского права, не "улавливаются" авторским правом. По мере роста популярности таких моделей может получиться так, что авторское право окажется "за бортом" и регламентация доступа к объектам авторского права будет осуществляться средствами 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 с регламентации 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 обширное исследование.

§ 5. Исчерпание прав и цифровой контент

Нормы об исчерпании прав являются неотъемлемой частью любого современного законодательства в области интеллектуальной собственности <1>. Они выступают одним из важнейших ограничений исключительного права, установленных законом, и имеют своей целью способствование свободному обращению товаров. В частности, это достигается путем создания условий для возникновения так называемого вторичного рынка, объектами которого являются поддержанные товары, в том числе книги и аудиозаписи. Нормы об исчерпании прав 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 <2>.

<1> В Европе соответствующие положения содержатся в национальном законодательстве государств - членов ЕС, нашли свое отражение они и в [ст. 4 Директивы ЕС от 22 мая 2001 г. N 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.

<2> Reese A. The First Sale Doctrine in the Era of Digital Networks // Boston College Law Review. 2003. N 44. P. 585.

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.

<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. Mannheim, 1978. S. 100).

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 <1>. 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 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 <2>. контексте распространения цифрового контента в сети Интернет нас будет интересовать вопрос о применимости положений об исчерпании прав на объекты авторского права к случаям распространения экземпляров произведений в электронной форме.

<1> Bobbs-Merill Co. v. Straus. 210 U.S. 339, 350 - 351 (1908).

<2> 17 U.S.C. § 109(a).

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 <1>.

<1> См. подробнее: Eurie Hayes Smith IV. Digital First Sale: Friend of Foe? // Cardozo Arts & Entertainment Law Journal. 2005. N 22. P. 369 - 370.

Американские 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 (в сервисе **iTunes** или **ReDigi**) музыкальные произведения в виде электронных файлов <1>.

<1> Capitol Records, LLC v. ReDigi, Inc., USDC S.D. N.Y., March 30, 2013.

В Европе вопрос о допустимости применения положений об исчерпании прав к произведениям, распространяемым в электронной форме, решается в зависимости от вида объекта авторского права.

Компьютерные программы подпадают под особый режим, предусмотренный Директивой N 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 ЕС. При этом в п. 7 преамбулы Директивы N 2009/24/ЕС указывается на ее применимость к любым компьютерным программам независимо от их формы.

Одним из наиболее известных споров в указанной области является дело **UsedSoft GmbH v. Oracle International Corporation**, рассмотренное Европейским

судом справедливости. 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. Суд указал четыре условия, при которых перепродажа электронных экземпляров программного продукта является допустимой: 1) такой продукт был введен в оборот на территории Европейского экономического сообщества с согласия правообладателя; 2) правообладатель предоставил "вечную" лицензию, не ограниченную сроком действия; 3) правообладатель получил разумное вознаграждение; 4) первоначальный приобретатель программы удалит все копии программы. Важно подчеркнуть, что Европейский суд четко 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>.

<1> UsedSoft GmbH v. Oracle International Corp.
ECJ. Case C-128/11. 3 July 2012.

Дальнейшее развитие событий достаточно любопытно. После принятия указанного решения Европейским судом справедливости дело было направлено в немецкий суд для рассмотрения по существу с учетом обозначенных критериев. Однако компания **UsedSoft** внезапно отказалась от дальнейших судебных процессов и согласилась с требованиями **Oracle** о прекращении противоправной деятельности (**Cease and desist**). Как отмечается, основной причиной для данного решения стали проблемы, связанные с доказыванием наличия критериев, обозначенных в решении Европейского суда. В частности, нотариально заверенное заявление продавца о том, что он является правомерным владельцем программного продукта, уплатил лицензионное вознаграждение и удалил свой экземпляр программы, было сочтено немецким судом недостаточным. Также у компании могли возникнуть проблемы с предоставлением документов, демонстрирующих порядок предоставления права на использование программного продукта <1>.

<1> Schneider A. The End of the UsedSoft Case and its Implications for "used" Software Licences. 30 April 2015.
URL:
<http://onlinegameslaw.com/the-end-of-the-usedsoft-case-and-its-implications-for-used-software-licences/>.

Как видно, применение доктрины исчерпания прав в отношении программного обеспечения в Европе сопряжено с выполнением ряда условий, которые позволяют в некоторой степени минимизировать риски

злоупотреблений в указанной сфере и пресечь развитие недобросовестных бизнес-моделей. Так, например, немецкий суд в одном из дел признал не соответствующей требованиям положений об исчерпании прав практику перепродажи лицензионных ключей к компьютерным играм, которые были изначально приобретены в "коробочном" варианте. По мнению суда, положения об исчерпании прав не позволяют дробить первоначально приобретенный продукт на составные части и реализовывать их самостоятельно <1>.

<1> Urteil, LG Berlin, 11 März 2014. N 16 O 73/13.
URL: <http://goo.gl/ZwzgMQ>.

Таким образом, европейское законодательство допускает применение положений об исчерпании прав в отношении компьютерных программ, распространяемых в электронной форме, что не означает, однако, отсутствия сложностей, связанных с подтверждением факта наличия соответствующих условий на практике.

Что же касается вопроса о допустимости применения положений об исчерпании прав к иным объектам авторского права (книгам, фильмам и т.п.), то здесь однозначного решения пока нет. Во многом это обусловлено существованием различных директив ЕС в отношении программного обеспечения и иных объектов авторских прав, различающихся по содержанию в части положений об исчерпании прав. Указанные различия хорошо иллюстрируются следующими судебными решениями.

По мнению немецкого суда, положения об

исчерпанию прав не применяются к электронным книгам, поскольку в соответствии с Директивой N 2001/29/ЕС "О гармонизации некоторых аспектов авторских и смежных прав в информационном обществе" принцип исчерпания прав действует только в случае продажи материальных носителей и из-под его действия исключаются случаи предоставления доступа к ним в процессе оказания услуг, особенно онлайн-услуг (п. п. 28, 29 преамбулы). При этом подходы, изложенные в деле **UsedSoft**, в таком случае неприменимы, поскольку в отношении программного обеспечения действует своя директива и, как следствие, решение вопроса о допустимости исчерпания прав в отношении его не охватывается ограничениями, применимыми ко всем иным объектам авторских прав и содержащимися в [Директиве N 2001/29/ЕС <1>](#).

<1> Urteil LG Bielefeld, 5 März 2013. N 4 O 191/11.
URL: <https://openjur.de/u/621610.html>.

Несколько иной подход использовали голландские суды. Так, в январе 2015 г. Апелляционный суд г. Амстердама вынес предварительное решение по делу компании **Tom Kabinet**, организовавшей онлайн-сервис по реализации ранее приобретенных электронных книг <1>. Нидерландская Ассоциация издателей (**NUV**) потребовала от компании **Tom Kabinet** прекращения предоставления такого сервиса. Издатели заявляли, что электронные книги не могут перепродаваться, поскольку являются нематериальными товарами. По мнению компании **Tom Cabinet**, принципы, изложенные Европейским судом справедливости в деле **UsedSoft**, должны применяться и в этом случае. При этом учитывалось, что сервисом

были предприняты достаточные меры для предотвращения возможности повторной продажи первоначальным владельцем ранее проданной копии. Это обеспечивалось посредством специального программного кода, который внедрялся в экземпляр книги при ее загрузке на сервис с целью продажи. Данный код позволял отследить дальнейшую судьбу данного экземпляра. Апелляционный суд постановил, что веб-сайт должен прекратить свое функционирование, поскольку он позволяет продавать и копии, которые были получены нелегальными способами. Если компания **Tom Kabinet** внедрит на сервисе систему, которая позволит предотвратить подобные предложения о продаже нелегальных копий книг, то сервис сможет продолжить свой бизнес. И хотя суд прямо не заявил о применимости подходов, изложенных в деле **UsedSoft**, к электронным книгам, из содержания и духа решения можно сделать вывод о том, что они вполне применимы и в данном случае. По мнению голландского суда, в основе решения по делу **UsedSoft** лежат экономические соображения: практическое сходство материальных и нематериальных товаров, а также тот факт, что правообладатель получает определенное вознаграждение при первой продаже. Следовательно, указанные доводы вполне применимы и к электронным книгам <2>.

<1> Gerechtshof Amsterdam 20-01-2015,
ECLI:NL:GHAMS:2015:66 (NUV/Tom Kabinet).

<2> Подробный анализ данного дела на русском языке см.: Доротенко Д. Суды в Нидерландах применяют правило UsedSoft в делах по перепродаже электронных книг. 6 февраля 2015 г. URL:

<https://goo.gl/NbydKp>.

Вопрос о том, какой подход является наиболее правильным - немецкий догматический или голландский экономический, скорее всего, рано или поздно будет должен разрешить Европейский суд справедливости. А пока рассмотрим, как данный вопрос может быть 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 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 экземпляр, 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 цифрового объекта. Соответствующие ограничения, установленные в лицензионном соглашении, являются правомерными, а их несоблюдение является нарушением авторских прав со всеми вытекающими последствиями.

<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 на его создание. 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).

Таким образом, по российскому праву ответ на вопрос о допустимости применения положений об

исчерпанию прав к цифровым произведениям аналогичен тому, который дают право и судебная практика США: отчуждение правомерно приобретенного произведения в цифровой форме возможно лишь вместе с тем носителем, на который оно было изначально записано.

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 <1>. Некоторые авторы заходят настолько 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 <2>.

<1> 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. 2011. N 93. P. 175.

<2> Newman J. Selling the Right to License: Examination of the First Sale Doctrine Through the Lens of UMG Recordings & Quanta Computer // Journal of

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 обуславливает 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 <1>. Очевидно, что реализация данной идеи на практике является крайне непростой задачей. Получившаяся в итоге система неизбежно будет допускать значительные перегибы в процессе функционирования, 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.

<1> US Copyright Office, Dmca Section 104 Report
19 (Aug. 2001) // <http://www.copyright.gov/reports/studies/dmca/sec-104-report-vol-1.pdf>.

Поскольку в случае с применением положений об исчерпании прав к цифровым объектам возникает та же проблема "двойной траты", которая типична для электронных денег, можно обратиться к опыту ее решения в сфере электронных платежей. Забегая немного вперед, следует отметить, что там она решается посредством вовлечения третьей стороны (эмитента, процессингового центра и т.п.), которая контролирует каждую транзакцию. Теоретически такую роль мог бы играть онлайн-сервис, посредством которого может быть реализован цифровой контент на вторичном рынке. Однако, учитывая роль "сетевых

эффектов" и эффекта масштаба для успешного функционирования подобного рода сервисов (чем больше пользователей и контента, тем более он становится популярным и, соответственно, получает еще больше пользователей и контента), их имплементация под силу крупным площадкам. В то же время такие площадки, скорее всего, будут осуществлять распространение подобного рода контента на "первичной основе", за счет чего смогут, в частности, контролировать хотя бы отчасти юридическую чистоту распространяемого "б/у" контента. Предоставление возможности продажи такого контента на "вторичном" рынке будет подрывать продажи первичного контента: ведь в отличие от произведений на материальном носителе качество "б/у" цифрового контента ничем не отличается от качества изначально приобретенного. В этой связи не очень понятно, зачем крупным площадкам по дистрибуции цифрового контента связываться с его "б/у" эквивалентами. А небольшие площадки не будут обладать достаточным "набором" (репутация, контент и количество пользователей) для обеспечения успешного функционирования сервиса без особых рисков предъявления претензий со стороны правообладателей.

Другой вариант, который может подсказать опыт из сферы электронных платежей - использование технологии Блокчейн, подобной той, которая используется в криптовалюте **Bitcoin** <1>. Если история "владения" соответствующим цифровым объектом будет общедоступной и верифицируемой, а возможность неоднократного распоряжения им будет заблокирована на уровне применяемых алгоритмов, то основной риск правообладателей, возникающий при цифровой дистрибуции, будет устранен. А цифровой экземпляр по своим свойствам будет мало чем

отличаться от экземпляра на материальном носителе для целей применения доктрины исчерпания прав.

<1> Данный вопрос будет подробно рассмотрен в § 4 гл. 7 настоящей работы.

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 прав в существующих

технологических реалиях. 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. Раньше для того чтобы взять фильм на прокат или купить его, необходимо было идти в магазин, надеясь на то, что этот фильм имеется там в наличии, в настоящее время достаточно воспользоваться специализированным сервисом вроде **iTunes** в Интернете: 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.

Представляется, что вышеизложенные аргументы свидетельствуют о нецелесообразности распространения положений об исчерпании права на цифровой контент на данном этапе развития технологий. Вместо этого целесообразно продолжение использования лицензирования как основного регулятора отношений в данной области, хотя, возможно, с большим 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 двух 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 большую 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 завершение необходимо отметить, что и в рамках существующего подхода (речь идет о недопустимости распространения на цифровой контент принципа исчерпания прав) можно построить бизнес-модели, позволяющие пользователям "продавать" ранее приобретенный цифровой контент или, по крайней мере, некоторые его виды. Показателен в этой связи пример сервиса **ReDigi**. После проигранного спора с компанией **Capital Records**, упомянутого выше, данный сервис изменил свою модель функционирования. Пользователь может записать приобретенные им посредством сервиса

iTunes музыкальные композиции на сервер **ReDigi**. После этого он вправе пользоваться ими по своему усмотрению, в том числе прослушивая их из облака либо копируя на переносное устройство. При желании продать соответствующую песню пользователь размещает данные об этом в специальном разделе сервиса. Покупатель композиции, также зарегистрированный в **ReDigi**, оплатив песню, получает доступ к тому же самому файлу, что изначально был загружен с **iTunes**. Предыдущий пользователь, соответственно, утрачивает доступ к такой песне и с помощью технических средств она удаляется с его синхронизируемого переносного устройства (в случае, если она была туда ранее загружена). Таким образом, происходит не появление нового экземпляра файла, а изменение прав доступа к нему <1>. Как видно, решение рассматриваемой проблемы достаточно "элегантное", особенно в условиях развития популярности облачных сервисов хранения данных и потокового аудио.

<1> <https://en.wiMpedia.org/wiM/ReDigi>

§ 6. Виртуальная "собственность"

Рынок цифрового контента не ограничивается лишь предоставлением электронных экземпляров традиционных объектов авторских и смежных прав, а также удаленного доступа к ним. Существует еще один сегмент, который долгое время находился в тени, но в последнее время начинает получать все больше внимания со стороны юристов <1>. Речь идет о различного рода персонажах (аватарах) онлайн-игр, внутриигровых объектах, виртуальных аналогах реальных объектов, реализуемых в виртуальных мирах

вроде **Second Life**, которые приобретаются прямо или косвенно за реальные деньги.

<1> Наиболее подробный и обстоятельный анализ вопросов, связанных с правовым регулированием виртуального контента и отношений, возникающих в связи с онлайн-играми, содержится в работах В.В. Архипова. См., например: Архипов В.В. **Виртуальная собственность**: системные проблемы в контексте развития индустрии компьютерных игр // Закон. 2014. N 9. С. 69 - 90; Он же: Виртуальное право: основные проблемы нового направления юридических исследований // Известия высших учебных заведений. Правоведение. 2013. N 2. С. 93 - 114.

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>. При этом есть все основания полагать, что она будет с каждым годом только расти.

<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/>.

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 объектов. В качестве инструмента регламентации используются уже знакомые соглашения с конечным пользователем (**End User License Agreement, Terms of Service, Terms of Use**) <1>.

<1> Fairfield J. Virtual Property // Boston University Law Review. 2005. N 85. P. 1050; Benjamin Tyson Duranske. Virtual Law: Navigating the Legal Landscape of Virtual Worlds. Chicago: ABA Publishing, 2008. P. 27.

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 ссылаясь на то, что подобные действия ответчика составляют деликт, именуемый "конверсия" (**conversion**), суть которого сводится к неправомерному присвоению чужого имущества <1>. К сожалению, суду не была предоставлена возможность вплотную заняться вопросами квалификации существующих отношений, поскольку, после того как он признал недействительной арбитражную оговорку в Пользовательском соглашении, дело завершилось мировым соглашением <2>.

<1> Restatement (second) of Torts. § 222A (1965).

<2> Bragg v. Linden Research, Inc. 487 F. Supp. 2d

593, 603 (E.D. Pa. 2007).

Другой пример также связан с проектом **Second Life**, но касается уже нарушения интеллектуальных прав на виртуальные объекты посредством действий, совершенных другим пользователем в виртуальном 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>.

<1> Eros, LLC v. Simon. 1:07-cv-04447-SLT-JMA (E.D.N.Y., 2008).

Как видно из указанных примеров, отношения, возникающие в виртуальных мирах, весьма схожи с теми, которые имеют место в реальном мире: соответствующие 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, - это их виртуальный характер.

В связи с этим один из главных вопросов, требующих своего разрешения, это вопрос о том, насколько право 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 <1>. 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.

<1> Duranske B. Op. cit. P. 60.

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 <1>. Например, если речь идет о совершении кражи в игре, условия которой допускают возможность существования персонажей, которые крадут, как это имеет место во многих многопользовательских онлайн-играх <2>, то факт совершения кражи в рамках игрового процесса является проявлением игры и не выходит за рамки "волшебного круга". В противном случае игра перестанет быть игрой. 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.

<1> Duranske B. Op. cit. P. 75.

<2> Например, в известной многопользовательской игре **Ultima Online** есть специальный класс персонажей - "Вор" (**Thief**), существуют гильдии воров и прочие атрибуты, свойственные данному виду деятельности.

Некоторые правовые порядки 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>. И это далеко не единичное решение, касающееся виртуальной собственности.

<1> Fairfield J. Op. cit. P. 1085.

<2> Will Knight, Gamer Wins Back Virtual Booty in Court Battle, newscientist.com. 2003. Dec. 23 // <http://www.newscientist.com/artide.ns?id=dn4510>.

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 <1>. 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 только год было рассмотрено около 22000 заявлений по поводу кражи объектов виртуальной собственности <2>.

<1> Taiwan Ministry of Justice Official Notation N 039030 (90). Цит. по: Fairfield J. Op. cit. P. 1086.

<2> Mark Ward. Does Virtual Crime Need Real Justice? BBC NEWS. 2003. Sept. 29 // <http://news.bbc.co.uk/2/hi/technology/3138456.stm>.

Однако, если абстрагироваться от практики азиатских государств, пока оборот виртуальных объектов является "относительно неурегулированным в законодательстве большинства стран" <1>. Правоприменителям обычно достаточно сложно провести параллели между реальной собственностью и математическими алгоритмами, эмулирующими внешний вид и функционал объектов реального мира <2>.

<1> 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. 2009. N 37. P. 384.

<2> Westbrook T. Op. cit. P. 779 - 780.

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 представителя с организатором игр или пари, а также требований, указанных в п. 5 ст. 1063 ГК РФ <1>. Рассмотрим подробнее, насколько корректна такая квалификация.

<1> См., например: [Постановление](#) Президиума Московского городского суда от 24 мая 2013 г. по делу N 44г-45; Определения Костромского областного суда от 12 мая 2010 г. по делу N 33-562, от 31 мая 2010 г. по делу N 33-672; решение Басманного районного суда от 17 августа 2010 г. по делу N 2-2360/10; решение Лефортовского районного суда г. Москвы от 5 октября 2010 г., решение мирового суда судебного участка N 352 Басманного района г. Москвы от 1 февраля 2011 г. N 2-01/11.

ГК РФ не содержит определения понятий "игра" и "пари". В настоящее время дефиниции указанных понятий содержатся в Федеральном [законе](#) от 29 декабря 2006 г. N 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 основанного 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 правовые порядки <2>.

<1> Федотов А.Г. [Игры и пари](#) в гражданском праве // Вестник гражданского права. 2011. N 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. 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").

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 непользности 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 о его прагматизме: соответствующие платежи имеют немалое фискальное значение. Так что есть основания полагать, что причина может крыться в чем-то ином.

<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 онлайн-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.

Автор одного из наиболее интересных исследований по тематике игр и пари А.Г. Федотов

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 недействительной 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 распушенности.

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.

Примечательно, что отечественные суды постепенно начинают чувствовать различия между отношениями, возникающими в связи с виртуальным контентом в онлайн-играх, и азартными играми в контексте [ст. 1062](#) ГК РФ. Например, Ленинский районный суд г. Кемерово в своем определении отметил, что "в интерактивной компьютерной онлайн-игре... отсутствует условие о "выигрыше", т.е. о денежных средствах или ином имуществе, в том числе имущественных правах, подлежащих выплате или передаче участнику азартной игры при наступлении результата азартной игры, предусмотренного правилами, установленными организатором азартной игры, в связи с чем отсутствует существенное условие "азартной игры" или "пари" В связи с тем что интерактивная компьютерная онлайн-игра... не является азартной игрой или пари, положения [главы 58](#) ГК РФ, в том числе и [ст. 1062](#) ГК РФ, применению не подлежат" <1>. Насколько подобный подход найдет поддержку у иных судов, покажет время. Но сам факт его появления уже внушает сдержанный оптимизм.

<1> Апелляционное определение Ленинского районного суда г. Кемерово от 26 апреля 2013 г. по делу N 11-59/2013. URL: <http://goo.gl/v9c8dc>.

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 сделок с виртуальными объектами.

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 объекты 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. Дело в том что правообладатели заинтересованы в защите произведенных в разработку виртуального мира инвестиций, а также в осуществлении контроля над тем, что там происходит <4>. 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 такой собственности <5>. Например, в результате 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 какого-либо виртуального объекта будет равнозначно признанию за ним определенного долга по отношению к пользователю - владельцу такого объекта, к чему вряд ли готово большинство правообладателей <6>.

<1> Duranske B. Op. cit. P. 80.

<2> Lastowka G., Hunter D. The Laws of the Virtual Worlds // California Law Review. 2004. N 92. 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. 2007. N 9. P. 172.

<4> Westbrook T. Owned: Finding a Place for Virtual World Property Rights // Michigan State Law Review. 2006. N 2006. P. 788 - 789.

<5> Bartle R. Bartle of Virtual Property. The Themis Group. April 2004 // <http://www.themis-group.com/uploads/Bartle%20of3/o20Virtual%20Property.pdf>.

<6> Duranske B. Virtual Law. ABA Publishing. 2008. P. 96.

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 <1>, поэтому виртуальные объекты не могут быть регламентированы нормами о праве собственности ввиду их явно выраженного нематериального характера <2>.

<1> См., например: Суханов Е.А. **О понятии и видах вещных прав** в российском гражданском праве //

<2> 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 быть с виртуальными земельными участками, доступ к которым невозможен без согласия правообладателя программного продукта.

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 нередко это и происходит на практике, когда соответствующие отношения рассматриваются в контексте лицензионных отношений между правообладателем (администратором) и лицензиатом (пользователем). Приобретение виртуальных 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 некоторое время назад внушал определенные симпатии 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](#). Однако после решения судов по делу ООО **"Мэйл.ру Геймз"** вопрос о возможности использования конструкции лицензионного договора для дистрибуции виртуального контента можно считать решенным, хотя и в отрицательном для правообладателей ключе.

В указанном споре компания ООО **"Мэйл.ру Геймз"** выступала в качестве владельца (провайдера) интерактивных многопользовательских компьютерных онлайн-игр, размещенных на сайтах в сети Интернет, право пользования которыми предоставлялось физическим лицам без внесения абонентской платы на основании лицензионного договора. Одновременно с этим компания предоставляла возможность использования дополнительного функционала игры за плату. Суд вслед за налоговым органом квалифицировал лицензионное соглашение с конечным пользователем как смешанное - с элементами как лицензионного соглашения, так и договора возмездного оказания услуг. Лицензионный элемент был выражен в возможности пользователя установить на свой компьютер клиентскую часть игры и играть в нее без внесения лицензионного платежа (**free-to-play**). Элемент услуги - в предоставлении пользователю возможности использования дополнительного функционала игры в целях облегчения игрового

процесса. В равной степени в качестве услуги по организации игрового процесса были квалифицированы сопутствующие действия провайдера - выполнение услуг по доведению до всеобщего сведения, распространению, оперированию, обслуживанию, администрированию, управлению компьютерными онлайн-играми, регистрации учетной записи персональных данных пользователя, блокировке игрового аккаунта, ведению игрового лицевого счета. Общий подход судов метко обобщен в статье Д. Бабинера и А. Аракеляна, в которой указано, что "валюта, предметы и возможности игрового мира, включенные в компьютерную игру, а также степень их доступности - это элементы игровой механики, определяющей свойства предоставляемого игрового продукта (например, сложности игрового процесса), которая, однако, не может квалифицироваться как способ определения условий пользования им (границ предоставляемой лицензии)" <1>. Поскольку услуга по организации игрового процесса подлежит налогообложению НДС, применение льготы по НДС в отношении полученных за дополнительный контент платежей было признано неправомерным, и компания была привлечена к налоговой ответственности <2>.

<1> Бабинер Д., Аракелян А. НДС при реализации компьютерных игр // Legal Insight. 2016. N 4. С. 63.

<2> [Постановление](#) ФАС Московского округа от 18 июня 2015 г. по делу N А40-91072/14. [Определением](#) ВС РФ от 30 сентября 2015 г. N 305-КГ15-12154 суду было отказано в передаче кассационной жалобы для рассмотрения в судебном заседании Судебной коллегии по экономическим спорам ВС РФ.

Данное решение нельзя считать бесспорным с точки зрения корректности переложения технических аспектов дистрибуции виртуальных объектов на юридическую материю. Один из основных аргументов провайдера - о том, что виртуальный контент не существует вне онлайн-игры, которая является компьютерной программой, а представляет собой дополнительный программный код, - не был убедительным образом опровергнут налоговой службой или судом. Налоговый характер спора и фигурировавшие в нем большие денежные суммы не могли не наложить своего отпечатка на глубину анализа природы возникающих отношений. Однако одно является очевидным для целей рассмотрения вопросов, затронутых в данном параграфе: суд согласился с подходом, согласно которому регулирование вопросов распространения виртуальных объектов осуществляется в договорно-правовом порядке. Разногласия с провайдером касались лишь правовой квалификации такого договора. По мнению суда, такого рода отношения представляют собой услугу по организации игрового процесса и не охватываются предметом лицензионного договора.

Основным недостатком договорно-правового подхода к регулированию вопросов, связанных с виртуальными объектами, является потенциальный регуляторный вакуум, который может возникнуть по причине того, что соответствующие соглашения 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

соглашение никак не регламентирует его или такого соглашения просто нет, в том числе по причине признания его недействительным?

<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.

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.

<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.

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. ст. 18, 24](#), [п. 1 ст. 56](#), [п. 1 ст. 126](#), [ст. ст. 209, 336](#), [п. 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. 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 имуществу, ценные бумаги, права, удостоверенные бездокументарными ценными бумагами, исключительные права и другое имущество, причем деньги (в подобном понимании) в

состав имущества не входят (п. п. 1, 2 ст. 1013 ГК РФ) <1>.

<1> Лысенко А.Н. [Имущество в гражданском праве России](#). М., 2010.

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.) <1>. В столь же широком смысле предлагают понимать имущество и некоторые отечественные юристы <2>.

<1> См.: Лапач Л.В. [Понятие "имущество" в российском праве](#) и в Конвенции о защите прав человека и основных свобод // Российская юстиция. 2003. N 1.

<2> См.: Гражданское право России: Общая часть: Курс лекций / Отв. ред. О.Н. Садиков. М., 2001. С. 262.

Существующий в законодательстве и доктрине плюрализм в понимании имущества наталкивает на вывод, что оно носит конъюнктурный 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 <1>. 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".

<1> См., например: Суханов Е.А. Осторожно: гражданско-правовые конструкции // Законодательство. 2003. N 9.

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. ст. 1102, 1104 , 1105 ГК РФ). Таким образом, кража чужого аккаунта 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 дела **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>. Пойдет ли по данному пути практика, покажет время. На данный момент некоторый сдержанный оптимизм по данному вопросу внушает тот факт, что вышеобозначенный подход нашел поддержку в отечественной доктрине <2>.

<1> См.: п. 2 информационного письма Президиума ВАС РФ от 11 января 2000 г. N 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. N 49.

<2> Архипов В.В. **Виртуальная собственность:** системные проблемы в контексте развития индустрии компьютерных игр // Закон. 2014. N 9. С. 81.

В любом случае со временем неизбежно возникнет необходимость переосмысления традиционных представлений о праве собственности, его объектах и порядке их защиты с целью причисления к ним виртуальных объектов. 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. 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 "серый" 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.

§ 7. Проблемы защиты прав потребителей цифрового контента

Специфика цифрового контента и использование модели лицензионного договора для его распространения вызывают ряд вопросов о применимости традиционных механизмов защиты прав потребителей к таким отношениям.

К числу основных проблем, которые могут возникнуть при использовании цифрового контента в B2C-отношениях, можно отнести следующие:

1) доступность и прозрачность информации об условиях предоставления контента (о совместимости с программным и аппаратным обеспечением; существующих ограничениях, обусловленных техническими средствами защиты информации);

2) несправедливые условия договора на предоставление цифрового контента (непрозрачные условия оплаты контента со "скрытыми" комиссиями; возможность в одностороннем порядке менять условия предоставления контента и его содержание; необходимость повторной оплаты контента при его загрузке на то же устройство; неограниченное право провайдера на расторжение договора с потребителем);

3) качество контента (низкое разрешение видео, наличие помех и прерываний при воспроизведении приобретенного аудио- или видео контента);

4) информационная безопасность (наличие вирусов и троянов в приобретенном контенте, наличие

специального программного обеспечения, которое устанавливается на устройство пользователя с целью отслеживания его действий).

Российский закон о защите прав потребителей не содержит специальных норм, защищающих потребителей от указанных рисков. Правда, нельзя сказать, что это проблема лишь российского законодательства. Как отмечается, европейское законодательство о защите прав потребителей также "с трудом применяется к таким транзакциям, а национальное законодательство практически всех стран - участниц ЕС не адаптировано к данным видам объектов" <1>. Сложившаяся ситуация не должна вызывать удивления, если принять во внимание то, что большая часть положений, составляющих основу законодательства о защите прав потребителей, была заложена в прошлом веке и "заточена" под куплю-продажу товаров и услуг.

<1> European Commission's Public Consultation on Contract Rules for Online Purchases of Digital Content and Tangible Goods. BEUC Response. 2015. The European Consumer Organization. P. 2. URL: <http://goo.gl/ejW4v5>.

Согласно **преамбуле** Закона о защите прав потребителей данный **Закон** "регулирует отношения, возникающие между потребителями и изготовителями, исполнителями, импортерами, продавцами при продаже товаров (выполнении работ, оказании услуг)". Буквальное толкование данного положения приводит к выводу о том, что отношения, которые не связаны с продажей товаров, выполнением работ и оказанием услуг, находятся за рамками закона безотносительно к

их субъектному составу. При таком подходе получается, что приобретение цифрового контента потребителем для личных и домашних нужд, опосредуемое лицензионным договором, не охватывается положениями [Закона](#) о защите прав потребителей.

В настоящее время отсутствуют какие-либо разъяснения Верховного Суда РФ по данному поводу. Однако существует прецедент, когда Верховный Суд РФ отказался распространять нормы законодательства о защите прав потребителей на отношения, которые не укладываются в полной мере в триаду **товары - работы - услуги**. Так, Верховный Суд в свое время указал, что отношения по имущественному страхованию не подпадают под предмет регулирования [Закона](#) о защите прав потребителей и положения данного [Закона](#) к отношениям имущественного страхования не применяются. В качестве аргумента суд сослался на наличие специального регулирования данных отношений, а также на то, что целью страхования при заключении договора имущественного страхования является погашение за счет страховщика риска имущественной ответственности перед другими лицами или риска возникновения иных убытков в результате страхового случая <1>.

<1> 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. ([вопрос N 2](#)). Данное разъяснение было отозвано Верховным Судом в [Обзоре](#) судебной практики Верховного Суда Российской Федерации за второй квартал 2012 года, утв. Президиумом Верховного Суда РФ 10 октября 2012 г. Впоследствии Верховный Суд РФ все же установил,

что к имущественному страхованию применяются общие положения [Закона](#) о защите прав потребителей (см. [п. 2](#) Постановления Пленума Верховного Суда РФ от 28 июня 2012 г. N 17 "О рассмотрении судами гражданских дел по спорам о защите прав потребителей"; см. также: [п. 2](#) Постановления Пленума Верховного Суда РФ от 27 июня 2013 г. N 20 "О применении судами законодательства о добровольном страховании имущества граждан").

Еще больше оснований для подобного рода размышлений дает положение [п. 19 преамбулы](#) Директивы ЕС 2011/83/ЕС "О правах потребителей", в котором отмечается, что договоры на предоставление цифрового контента в электронной форме не являются ни договорами купли-продажи, ни договорами услуг, но на них распространяются отдельные гарантии, предусмотренные [Директивой](#) (право на отказ от договора, право на информацию о функциональности, совместимости, технических средствах защиты и т.п.). В отсутствие подобного рода оговорок, но при такой квалификации договора применять российский [Закон](#) о защите прав потребителей в условиях действия триады **товар - работа - услуга** может быть достаточно тяжело.

Попробуем разобраться, как именно [Закон](#) о защите прав потребителей применяется к отношениям, связанным с приобретением физическим лицом цифрового контента в различных формах для личных нужд. Анализ существующих положений и судебной практики позволяет сделать следующие выводы.

Во-первых, в тех случаях, когда приобретение цифрового контента осуществляется на материальном носителе, такой носитель может быть квалифицирован как товар, что открывает возможности для

использования средств защиты, доступных на случай предоставления некачественного товара. В качестве примера данного подхода можно привести разъяснение Верховного Суда РФ, в соответствии с которым "требования граждан к качеству программного обеспечения, используемого в технически сложном товаре (например, к операционной системе, которая служит для обеспечения его функционирования), должны рассматриваться как требования к качеству товара в целом с учетом его потребительских свойств в соответствии со [статьей 469 ГК РФ](#)" ^{<1>}. Правда, есть определенные сомнения относительно универсальности данного разъяснения, так как в случаях с более простыми материальными носителями вполне возможен дифференцированный подход, согласно которому требования о качестве могут предъявляться лишь к внешнему виду такого носителя (отсутствие царапин, иных внешних повреждений), а не к его содержанию. В обоснование такого формального подхода вполне можно сослаться на [п. 1 ст. 1227 ГК РФ](#), закрепляющий отдельный правовой режим интеллектуальных прав и материальных носителей. Все это лишний раз показывает целесообразность специального регулирования в указанной области: если потребитель скачал на специализированной платформе музыкальный файл, он должен воспроизводиться, соответствовать заявленному описанию и битрейту. Непонятно, почему такого рода отношения должны регулироваться иначе, чем требованиями к качеству материального объекта.

^{<1>} См.: [п. 39](#) Постановления Пленума Верховного Суда РФ от 28 июня 2012 г. N 17. Схожего мнения придерживаются немецкие и голландские суды

(см.: Comparative analysis, Law & Economics analysis, assessment and development of recommendations for possible future rules on digital content contracts. Final Report. 2011. URL: <http://goo.gl/ugQqvq>).

Во-вторых, в случае приобретения потребителем цифрового контента в рамках безвозмездных онлайн-сервисов **Закон** о защите прав потребителей не применяется, что следует из дефиниции понятия "исполнитель" ("организация независимо от ее организационно-правовой формы, а также индивидуальный предприниматель, выполняющие работы или оказывающие услуги потребителям по **возмездному** договору"). При этом предоставление потребителем своих персональных данных или иной пользовательской информации такому сервису не может рассматриваться в качестве встречного предоставления по смыслу **ст. 423** ГК РФ, которая придает качество встречного предоставления лишь объектам гражданских прав <1>. Согласие стороны договора на обработку персональных данных в рамках специально установленного правового режима защиты персональных данных, положения которого носят ярко выраженные черты публичного права <2>, ни к одному из поименованных объектов гражданских прав отнести нельзя. Сами персональные данные, выступая разновидностью информации и не являясь при этом объектом интеллектуальной собственности, не входят в число признаваемых **ст. 128** ГК РФ видов информации, которая может выступать объектом гражданских прав. Еще меньше оснований относить персональные данные или согласие на их обработку к разновидности встречного предоставления, в случае если придерживаться концепции, согласно которой персональные данные представляют собой выражение личного неимущественного блага (личной и семейной

тайны), упомянутого в [п. 1 ст. 150](#) ГК РФ. Как известно, личные нематериальные блага носят неотчуждаемый и непередаваемый характер, будучи фактически изъятыми из оборота <3>.

<1> См., например: [Постановление](#) ФАС Московского округа от 27 сентября 2007 г. N КА-А40/9911-07-П; Научно-практический [комментарий](#) к Гражданскому кодексу Российской Федерации, части первой (постатейный) / Под ред. В.П. Мозолина, М.Н. Малеиной. М.: НОРМА, 2004 (комментарий к ст. 423); СПС "КонсультантПлюс"; [Комментарий](#) к Гражданскому кодексу Российской Федерации, части первой (постатейный)/ Под ред. О.Н. Садикова. 3-е изд., испр., перераб. и доп. М.: Контракт; Инфра-М, 2005; СПС "КонсультантПлюс".

<2> См. подробнее: [гл. 9](#) настоящей книги; а также: Савельев А.И. Направления эволюции свободы договора под влиянием современных информационных технологий // [Свобода договора](#): Сборник статей / Отв. ред. М.А. Рожкова. М.: Статут, 2016. С. 537 - 541.

<3> См., например: Малеина М.Н. [Право на тайну и неприкосновенность](#) персональных данных // Журнал российского права. 2010. N 11.

Примечательно, что в Рекомендациях ОЭСР по защите прав потребителей в сфере электронной коммерции отмечается, что такая защита должна распространяться на все транзакции с участием потребителей, независимо от наличия в них встречного предоставления денежного характера. При этом соглашения в отношении цифрового контента прямо поименованы в числе возможных потребительских

договоров (разд. I) <1>.

<1> Consumer Protection in E-commerce. OECD Recommendation. 2016. Paris. P. 9.

В-третьих, понятие "услуга", применяемое в разъяснениях Верховного Суда РФ, является достаточно широким и формально позволяет отнести к услугам многие соглашения, в рамках которых предоставляется цифровой контент: "под услугой следует понимать действие (комплекс действий), совершаемое исполнителем в интересах и по заказу потребителя в целях, для которых услуга такого рода обычно используется, либо отвечающее целям, о которых исполнитель был поставлен в известность потребителем при заключении возмездного договора" <1>. Например, к договорам об оказании услуг могут быть отнесены соглашения, заключаемые пользователями онлайн-игр, по условиям которых осуществляется оплата реальными деньгами. Однако, как было показано ранее, судебная практика судов общей юрисдикции, находясь "в плену" положений [ст. 1062](#) ГК РФ, пока в большинстве своем не разделяет указанный подход. Правда, квалификацию отношений, связанных с организацией игрового процесса и предоставлением платного цифрового контента в рамках онлайн-игр, в качестве возмездного оказания услуг поддерживают арбитражные суды в налоговых спорах <2>, что само по себе не очень помогает защите потребителей.

<1> См.: [п. 3](#) Постановления Пленума Верховного Суда РФ от 28 июня 2012 г. N 17.

<2> [Постановление](#) ФАС Московского округа от 18 июня 2015 г. по делу А40-91072/2014.

В-четвертых, в случае приобретения цифрового контента в электронной форме на основании лицензионного договора потребитель практически никак не защищен. В частности, по вопросам качества такого контента. Суды, как отмечалось ранее, исходят из того, что предметом лицензионного договора является предоставление имущественного права, которое, будучи нематериальным объектом, не может быть некачественным. Кроме того, в обоснование данного подхода можно привести [п. 1 ст. 1259](#) ГК РФ, согласно которому объекты авторских прав, к которым относится большая часть цифрового контента, охраняются независимо от их достоинства и назначения. Соответственно, если потребитель, к примеру, приобрел фильм, в описании к которому фигурировала оригинальная звуковая дорожка, а по факту имелся только перевод (или наоборот), такой потребитель не имеет законодательно закрепленного средства защиты и может рассчитывать только на наличие соответствующих положений в соглашении с провайдером контента.

В этой связи в настоящее время российское законодательство о защите прав потребителей не обеспечивает защиту потребителя от наиболее актуальных рисков в сфере оборота цифрового контента. У потребителя нет возможности предъявлять требования к качеству и информационной безопасности такого контента. Возможности предъявления требования о предоставлении конкретной информации, касающейся совместимости и порядка функционирования технических средства защиты авторских прав, весьма ограничены, так как, с одной

стороны, вопрос о применимости законодательства о защите прав потребителей к такого рода отношениям является спорным, а с другой стороны, даже при положительном решении данного вопроса [ст. 10](#) Закона о защите прав потребителей не содержит соответствующих положений и перечня видов информации, подлежащих предоставлению потребителям. Кроме того, в отсутствие специальных положений о правах потребителя при приобретении цифрового контента существенно затруднено оспаривание несправедливых условий договоров с провайдером. Для признания договорного условия недействительным в порядке [ст. 16](#) Закона о защите прав потребителей необходимо наличие соответствующего права, прописанного в нормативно-правовом акте, которое ущемляется таким договорным условием. Для оспаривания договорного условия в порядке [ст. 428](#) ГК РФ необходимо, чтобы оно лишало сторону прав, обычно предоставляемых потребителю по договорам такого типа, либо содержало явно обременительные условия. И то, и другое достаточно проблематично доказывать в отсутствие специального нормативного регулирования соответствующих отношений, которое могло бы выступить в качестве ориентира при оценке спорного условия.

Все это приводит к выводу о необходимости внесения изменений в законодательство о защите прав потребителей с целью отражения в нем специфики отношений, возникающих при дистрибуции цифрового контента. В Европе уже инициирован процесс подготовки изменений в европейское законодательство о защите прав потребителей <1>. Результаты данной инициативы, равно как и рекомендации ОЭСР, вполне могут быть использованы для совершенствования

российского законодательства, чтобы "не изобретать велосипед". А пока целесообразно применять к договорам о возмездном приобретении цифрового контента в электронной форме физическим лицом для собственных личных нужд хотя бы общие положения [Закона](#) о защите прав потребителей.

<1> Commission Proposes Modern Digital Contract Rules to Simplify and Promote Access to Digital Content and Online Sales across the EU. 9 December 2015. URL: http://europa.eu/rapid/press-release_IP-15-6264_en.htm.

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 так называемые электронные деньги. Их широкое распространение является одной из наиболее значимых инноваций в сфере денежного обращения и отражает устойчивую тенденцию к дематериализации денег - 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 и электронными деньгами основываются на двух ключевых характеристиках: 1) местонахождении денежной стоимости и 2) используемом механизме для перевода такой стоимости <1>.

<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.

Инструменты электронного доступа к банковским счетам (дебетовые и кредитные карты, инструменты мобильного банкинга, электронные чеки) позволяют осуществлять в удаленном режиме распоряжение средствами, размещенными в традиционных кредитных учреждениях. Механизм совершения платежа носит трехсторонний характер: помимо плательщика и получателя в нем участвует платежный посредник (кредитное учреждение). Таким образом, инструменты электронного доступа хотя 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.

<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.

Следует особо подчеркнуть, что ни один из существующих платежных механизмов не является идеальным и подходящим для всех типов платежей в сети Интернет <1>. Например, многие из них не очень

подходят для совершения микроплатежей, осуществления расчетов между физическими лицами в Интернете или для осуществления расчетов несовершеннолетними лицами, не обладающими счетами в банках. При этом отсутствие удобного для конкретного клиента способа оплаты для интернет-магазина означает потерю клиента. Все это обуславливает сосуществование и конвергенцию различных платежных инструментов.

<1> Graham Smith. Op. cit. P. 874.

Также необходимо учитывать, что с недавних пор законодательство о защите прав потребителей возложило на предпринимателей обязанность по обеспечению возможности оплаты потребителем товаров (услуг) не только посредством наличных денежных средств, но и с использованием национальных платежных инструментов в рамках национальной системы платежных карт (ст. 16.1 ЗоЗПП). Данное требование не распространяется на предпринимателей, размер активов или выручка которых за вычетом НДС не превышает 120 млн. рублей в год. Несмотря на то что не все интернет-магазины затронуты данным предписанием, тенденция к переводу платежей в сфере B2C-сегментов на безналичные формы оплаты становится все более выраженной, что помимо удобства для потребителя должно создать условия для более прозрачного налогообложения электронной коммерции.

§ 2. Особенности регулирования расчетов банковскими картами в сфере электронной коммерции

В настоящее время пластиковые карты (дебетовые и кредитные) получили наибольшее распространение в интернет-коммерции <1>. По данным платежной системы **ChronoPay** общий объем платежей банковскими картами в сети Интернет в 2015 г. достигал 1 трлн. рублей <2>.

<1> Юрасов А.В. Указ. соч. С. 218.

<2> Материалы 6-й международной конференции по защите персональных данных. 10 ноября 2015 г. URL: <http://2016.zpd-forum.com/programa/>.

Под пластиковой картой понимается персонифицированный платежный инструмент, используемый для автоматизации безналичных расчетов, а также для обналчивания 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 аутентификации).

В самом общем виде последовательность совершения действий оплаты в интернет-магазине посредством банковской карты выглядит следующим образом.

Участники процесса:

1. Интернет-магазин.
2. Покупатель (держатель банковской карты).

3. Банк-эмитент (банк, выпустивший карту покупателя).

4. Банк-эквайер (банк, принимающий оплату от лица продавца).

5. Оператор платежной системы (например, **MasterCard, Visa**).

6. Оператор услуг платежной инфраструктуры (операционный центр платежной системы, платежный клиринговый центр, расчетный центр).

Процедура прохождения платежа:

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 банку-эмитенту через операционный центр платежной системы.

4. Банк-эмитент, получив запрос через операционный центр платежной системы, проверяет наличие средств на карте и при их достаточности дает платежной системе положительный ответ на запрос.

5. При наличии множества операций между банком-эмитентом и банком-эквайером привлекается Платежный клиринговый центр, который производит зачет взаимных требований по транзакциям и направляет полученный результат в расчетный центр.

6. Расчетный центр осуществляет взаимопереводы средств между банком-эквайером и банком-эмитентом.

7. Банк-эквайер сообщает результат интернет-магазину и производит с ним расчеты.

8. Интернет-магазин доставляет товар (оказывает услугу).

Как видно, процесс оплаты товара (услуги) в сети Интернет связан с участием множества лиц. При этом следует уделить особое внимание таким ключевым участникам, как банк-эквайер, оператор платежной системы и оператор платежной инфраструктуры.

Для того чтобы интернет-магазин мог принимать платежи от клиентов, совершенные с использованием банковских карт, необходимо заключение договора об оказании эквайринговых услуг. В рамках данного договора банк-эквайер обязуется осуществить комплекс действий по организации и производству расчетов с торгово-сервисным предприятием заказчика (с интернет-магазином) по операциям, совершаемым с использованием банковских карт в сети Интернет, а интернет-магазин обязуется соблюдать правила, установленные банком-эквайером и платежной системой, а также уплачивать соответствующую комиссию.

Размер комиссии может составлять около 2 - 5% от выручки интернет-магазина. Этот тариф в основном обусловлен размером комиссии, взимаемой международными платежными системами (**VISA, MasterCard**). Кроме того, он включает наценку банка-эквайера. Также могут взиматься

дополнительные комиссии за ведение счета и повышенные комиссии при недостижении установленного уровня выручки. Для каждого интернет-магазина при заключении договора комиссия считается отдельно, при росте оборота она, как правило, снижается. Как следствие, принятие интернет-магазином платежей с использованием банковских карт может быть достаточно недешевым мероприятием, особенно для низкомаржинального бизнеса (например, перепродажа компьютерной техники). В связи с этим на практике иногда торговые точки пытаются переложить установленные по данным комиссии торговые риски на клиента, устанавливая повышенную цену при расчетах посредством банковских карт или отказывая в принятии банковских карт для оплаты определенных видов товаров, реализуемых с незначительной торговой наценкой. Следует отметить, что такая практика противоречит положениям о публичном договоре (см. [п. 2 ст. 426](#) ГК РФ, где говорится о необходимости обеспечения равенства цен для потребителей одной категории), а также законодательству о защите прав потребителей (см. [ч. 4 ст. 16.1](#), которая предусматривает запрет установления различных цен в зависимости от применяемого способа оплаты).

Основные обязанности банка-эквайера заключаются в обработке поступающих запросов на авторизацию карты; перечисление на расчетный счет интернет-магазина денежных средств за товары и услуги, оплаченные по карте; прием, сортировка и пересылка электронных и бумажных документов, подтверждающих совершение сделок с использованием банковских карт и др. При выполнении операций по банковским картам, эмитированным другими кредитными организациями, банк-эквайер осуществляет

перевод денежных средств через платежную систему из банка, выпустившего карту (банка-эмитента) в точку ее обслуживания (интернет-магазин).

На практике система расчетов участников процесса нередко значительно сложнее. Так, проведение взаиморасчетов между эквайером и эмитентом часто обеспечивает расчетный банк, в котором эти кредитные организации открывают корреспондентские счета. Кроме того, нередко технические операции по обслуживанию карт могут передаваться банками-эквайерами специализированной сервисной организации - процессинговому центру, который осуществляет обеспечение безопасности платежей с использованием протокола аутентификации **3-D Secure** и **SSL**, а также анализ обрабатываемой транзакции на предмет возможного мошенничества (**fraud monitoring**). Применительно к платежам, совершаемым в сети Интернет, такой процессинговый центр в основном выполняет функции "платежного шлюза", предоставляя программно-аппаратные средства для автоматизированной обработки платежей. В таком случае после выбора формы оплаты на сайте интернет-магазина происходит переадресация на веб-страницу платежного шлюза, где вводятся необходимые платежные данные, а впоследствии сообщаются сведения о статусе платежа (платеж произведен успешно или в совершении платежа отказано).

Оператор платежной системы является одним из ключевых участников всей цепочки взаимоотношений, возникающих в связи с осуществлением расчетов с использованием банковских карт. Его статус, порядок взаимодействия с иными субъектами платежной системы закреплен в Федеральном [законе](#) от 27 июня

2011 г. N 161-ФЗ "О национальной платежной системе" (далее - Закон об НПС). В соответствии с данным **Законом** оператор платежной системы - это организация, определяющая правила платежной системы, а также выполняющая иные обязанности, предусмотренные этим **Законом**. Например, применительно к системе **Visa** таким оператором является ООО "Платежная система "Виза" <1>, а для системы **MasterCard** это ООО "МастерКард". Правила платежной системы в силу требований **ч. 6 ст. 20** Закона об НПС должны быть публично доступными <2>.

<1>

<http://www.visa.com.ru/ru/ru-ru/aboutvisa/legislation/rules.shtml>

<2> См., например: Правила платежной системы "Виза" по осуществлению операций на территории Российской Федерации (ред. от 31 июля 2015 г.). URL: <http://www.visa.com.ru/ru/ru-ru/aboutvisa/legislation/include/VPSORR-31.07.15.pdf>; Правила платежной системы "МастерКард" (ред. от 1 января 2016 г.). URL: <http://goo.gl/mE6Qfl>.

Банки-эмитенты и банки-эквайеры действуют на основании специальных соглашений с операторами платежной системы (обычно именуемых "лицензионными соглашениями" или договорами о присоединении к правилам платежной системы), в рамках которых им предоставляется право использования платежной инфраструктуры.

Инфраструктура каждой платежной системы состоит из трех частей - операционного, клирингового и

расчетного центров.

1. **Операционный центр** - это организация, обеспечивающая обмен запросами на авторизацию между банками и иными электронными сообщениями, шифрование, а также доступ к услугам по переводу денежных средств. До недавнего времени информация о любых операциях граждан РФ по картам международных платежных систем **Visa** и **MasterCard** отправлялась на обработку в процессинговые центры, расположенные за рубежом (в США и Бельгии соответственно). В связи с обострением геополитической обстановки и введением рядом иностранных государств антироссийских санкций возник риск приостановления операций по картам данных систем на территории России. Данный риск материализовался в прекращении со стороны платежных систем **Visa** и **MasterCard** обслуживания ряда российских банков, попавших под санкции США <1>. Впоследствии данные платежные системы объявили о приостановке операций с банковскими картами на территории Крыма <2>. В результате поправок, внесенных в [Закон](#) об НПС, внутрироссийские операции по международным платежным картам теперь подлежат обработке внутри страны <3>. В качестве операционного центра в настоящее время выступает АО "Национальная система платежных карт" (НСПК), инфраструктура которой расположена на территории РФ. Таким образом, на данный момент процессинг внутрироссийских банковских платежей локализован территорией Российской Федерации.

<1> Официальный представитель платежной системы "Visa" отметил: "Казначейство США ввело

санкции против некоторых российских физических лиц и организаций. В целях соответствия законодательству США компания Visa International Service Association обязана приостановить доступ к сети Visa для таких организаций" (21.03.2014. РИА Новости. URL: <http://goo.gl/Ksttk4>).

<2> **MasterCard** вслед за **Visa** прекратила обслуживание своих карт в Крыму (26.12.2014. URL: <http://goo.gl/FfyYsX>). Подробнее об антироссийских санкциях и их правовом статусе в контексте российского права см.: Савельев А.И. Односторонние экономические санкции США: взгляд со стороны американского и российского права // Закон. 2015. N 5. С. 108 - 131.

<3> Федеральный **закон** от 22 октября 2014 г. N 319-ФЗ "О внесении изменений в отдельные законодательные акты Российской Федерации".

2. Платежный клиринговый центр представляет собой организацию, которая в условиях огромного количества платежных транзакций определяет объем взаимных обязательств банка-эмитента и банка-эквайера и осуществляет взаимозачет надлежащих платежей. В настоящее время он также представлен в виде АО "НСПК".

3. Расчетный центр представляет собой организацию, в которой банк-эквайер и банк-эмитент имеют открытые корреспондентские счета и которая на основании распоряжения платежного клирингового центра, сделанного от имени банка-эмитента или банка-эквайера, осуществляет перевод надлежащей суммы. В настоящее время одним из основных расчетных центров выступает Банк России, что не

исключает возможности параллельного существования в рамках платежной системы и иных расчетных центров.

Такова роль основных участников процесса совершения платежа с использованием банковской карты в сети Интернет. Теперь необходимо вкратце осветить основные проблемы, которые возникают у субъектов электронной коммерции в связи с их использованием.

Одной из основных проблем является возможность совершения платежа неавторизованным лицом, например, с использованием украденной банковской карты или ее данных. В принципе данный риск возник с появлением самих банковских карт, т.е. задолго до появления онлайн-платежей, но в связи с развитием электронной коммерции приобрел особую актуальность.

По общему правилу данный риск призваны минимизировать технологии аутентификации, которые зависят 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.

В качестве средства аутентификации при совершении покупки через интернет-магазин выступают следующие данные карты: номер, срок действия, имя владельца и особый код на обороте карты: **CVV2 (card verification value)** - для **Visa**, **CVC2 (card verification code)** - для **MasterCard**. Такой код расположен на

обороте карты и представляет собой трехзначное число, получаемое с помощью специального алгоритма с использованием номера карты и срока ее действия. Этот алгоритм использует пару секретных ключей, известных эмитенту карты, поэтому, даже зная номер карты и срок ее действия, вычислить секретный код без знания секретного ключа невозможно.

В последнее время все большее распространение получает технология **3-D Secure (MasterCard SecureCode и Verified by Visa)**. Суть ее сводится к привлечению для целей аутентификации плательщика дополнительных средств из "реальной жизни", например мобильного телефона. Каждый раз, когда клиент совершает покупки в интернет-магазинах, происходит запрос на ввод пароля. Пароль является одноразовым (действующим 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 и при условии наличия достаточного остатка на счете плательщика платеж будет одобрен. Подобно ПИН-коду банковской карты, такой пароль может рассматриваться как "аналог 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". Таким образом, технология **3-D Secure** обеспечивает двухфакторную идентификацию плательщика - посредством ввода необходимых данных карты, а также

дополнительного запроса на подтверждение использования карты. Правда, данная технология обеспечивает дополнительную защиту только в том случае, если интернет-магазин (привлеченный им банк-эквайер или процессинговый центр) ее поддерживает.

Однако технические и организационные средства позволяют лишь минимизировать случаи совершения платежных транзакций неуполномоченными лицами <1>. В тех случаях, когда они не сработали, на первый план выступает специальное регулирование, которое призвано ответить на вопрос: кто должен нести ответственность за совершение таких транзакций?

<1> Как будет показано далее, такие средства служат скорее средством **перераспределения** рисков между различными субъектами - участниками процесса проведения платежа в сети Интернет.

Закон о НПС содержит нормы специального регулирования на случай совершения платежных операций без согласия плательщика. В соответствии с **ч. 15 ст. 9** Закона о НПС оператор по переводу денежных средств (в данном случае банк-эмитент) обязан возместить клиенту средства, списанные с его карты. Данное общее правило действует при определенных условиях, которые зависят от исполнения сторонами информационных обязанностей, в основе которых лежит общий принцип "рискует тот, кто не информирует". Если банк в порядке, предусмотренном в договоре, исполняет свою обязанность по уведомлению клиента о совершенной платежной операции, то клиент вправе требовать

возврата соответствующей суммы при условии уведомления банка не позднее одного дня, следующего за днем получения уведомления от банка о спорной транзакции. Если банк исполнил обязанность по уведомлению клиента, но тот уведомил банк о спорной транзакции позже, то банк не обязан возмещать соответствующую сумму. Если же и банк, и клиент своевременно исполнили свою обязанность по уведомлению друг друга, то банк обязан вернуть средства, списанные без согласия клиента, в отношении платежей, совершенных **после** получения уведомления от клиента, - без каких-либо условий, а в отношении платежей, совершенных **до** такого уведомления, - во всех случаях, когда банк не докажет, что списание было вызвано нарушением правил использования карты, например, при сообщении **PIN**-кода третьему лицу <1>. Таким образом, риски, связанные с использованием скимминга <2> и фишинга <3> в соответствии с [Законом](#) о НПС, по общему правилу возлагаются на банк, обслуживающий клиента.

<1> Поскольку все банковские договоры предусматривают обязанность клиента сохранять PIN-код в тайне от третьих лиц, использование правильного PIN-кода при расчете банковской картой обычно служит основанием для отказа в возмещении. См., например: Апелляционное [определение](#) Мосгорсуда от 30 июня 2015 г. по делу N 33-18320/15; Апелляционное [определение](#) Верховного суда Республики Татарстан от 16 марта 2015 по делу N 33-3775/2015. Интересно, что суды встают на сторону банка и в случаях, когда клиент был вынужден передать банковскую карту третьим лицам и сообщить PIN-код к ней при угрозе его жизни, указывая, что разбойное нападение не может являться основанием для

возложения бремени негативных последствий на банк и признания незаконными его действий по списанию денег. См., например: Апелляционное [определение Мосгорсуда от 20 мая 2013 г. по делу N 11-13233](#).

<2> Под скиммингом (от англ. **skim** - снимать сливки) понимается разновидность мошеннических действий, при совершении которых происходит установка на банкомат устройства, считывающего данные с магнитной полосы банковской карты, а также видеокамеры, направленной на клавиатуру. Первое позволяет скопировать информацию о карте для изготовления ее дубликата, а вторая - выяснить PIN-код. После этого мошенники изготавливают копию карты, с помощью которой можно снять деньги с соответствующего счета, введя правильный PIN-код.

<3> Под фишингом (англ. **phishing**, искаженное **fishing** - рыбалка) понимается схема, при которой мошенники создают интернет-сайт, вызывающий доверие у пользователя, например, сайт, похожий на сайт банка пользователя или известного интернет-магазина, через который и происходит похищение реквизитов платежных карт.

Приведенный механизм возмещения средств, списанных со счета клиента без его согласия, вызвал неоднозначную реакцию и критику со стороны банков <1>, но, по мнению Центрального банка РФ, данные положения соответствуют существующей мировой практике регулирования платежных услуг, в связи с этим рассматривать вопрос об их изменении можно лишь после анализа практики их применения <2>.

<1> Письмо Ассоциации российских банков от 18 февраля 2013 г. N А-01/5-87 "О проблемах применения Федерального закона "О национальной платежной системе".

<2> **Информация** Банка России "Ответы на вопросы, связанные с применением отдельных норм Федерального закона от 27 июня 2011 года N 161-ФЗ "О национальной платежной системе".

Однако соответствующие нормы **Закона** об НПС при всей их прогрессивности не могут в полной мере покрыть все риски, которые связаны с использованием банковских карт в качестве средства платежа в онлайн-среде. Кроме мошеннических действий, со стороны третьих лиц возможны и недобросовестные действия со стороны интернет-магазина, в частности, когда предоплаченный товар или услуга не были впоследствии предоставлены либо был предоставлен совсем иной товар (услуга). Такого рода ситуации, как впрочем и случаи совершения платежа неуполномоченным лицом, регламентируются правилами платежных систем, предусматривающих процесс оспаривания платежных транзакций (**chargeback**) <1>. В частности, такие процедуры предусмотрены платежными системами **Visa** <2> и **MasterCard** <3>.

<1> Следует отметить, что термин "chargeback" используется в практике самих платежных систем. Банк-эмитент во взаимоотношениях с клиентом может использовать иные термины, например "заявление о спорной операции по карте" в Сбербанке РФ. См.: http://www.sberbank.ru/ru/person/bank_cards/faq (п. 2.10).

<2>

<https://usa.visa.com/dam/VCOM/download/merchants/chargeback-management-guide-lines-for-visa-merchants.pdf>

<3>

http://www.mastercard.com/us/merchant/pdf/TB_CB_Manual.pdf

Указанные процедуры содержат закрытый перечень оснований для оспаривания совершенных транзакций (**reason code**). Например, в случае неполучения предоплаченного товара (услуги) код будет 30 для **Visa** и 4855 для **MasterCard**; в случае предоставления некачественного товара (услуги) или совсем иного товара код будет 53 для **Visa** и 4853 для **MasterCard**.

В самом общем виде процедура **chargeback** выглядит следующим образом. Как правило, она инициируется владельцем банковской карты через банк-эмитент, который, собрав необходимые документы и доказательства по спорной транзакции, адресует их через платежную систему в банк-эквайер. Банк-эквайер, получив данную информацию, адресует ее интернет-магазину для принятия решения. В случае если интернет-магазин согласен с претензией, спорная сумма перечисляется банку-эмитенту для последующего зачисления на счет владельца банковской карты. Если интернет-магазин не согласен с претензией, то инициируются специальные процедуры арбитража с участием самой платежной системы <1>. В случае если претензия будет признана обоснованной, соответствующий платеж должен будет совершить банк-эквайер, который впоследствии в порядке регресса сможет требовать данные суммы с интернет-магазина. Сам интернет-магазин будет еще оштрафован за

необоснованный отказ от удовлетворения претензии. Риски, связанные с возможной неплатежеспособностью интернет-магазина или его "исчезновением" обычно закладываются в комиссии, которые банк-эквайер взимает в рамках договоров на предоставление соответствующих услуг.

<1> Правила платежных систем предусматривают очень детальное регулирование различных спорных ситуаций. В частности, существуют специальные правила перераспределения рисков в зависимости от использованных технологий авторизации платежа. Например, при использовании технологии 3-D Secure осуществляется перенос риска совершения операций краденной банковской картой с интернет-магазина (на котором такой риск лежит по общему правилу) на банк, выпустивший карту, или в ряде случаев - на самого клиента. В соответствии с правилами платежных систем, если банк-эмитент одобряет платеж в интернет-магазине, где имплементирована система 3-D Secure, то он берет на себя ответственность за легитимность операции и не вправе требовать обратно деньги у продавца по основаниям, связанным с совершением платежа неуполномоченным лицом.

Процедура **chargeback** имеет ограничения по времени. Для банковской карты, выпущенной платежной системой **Visa**, срок составляет 180 дней, а для системы **MasterCard** - не более 120 дней. Данный период исчисляется с момента совершения транзакции или с момента, когда обязательство по предоставлению товара (услуги) было исполнено или должно было быть исполнено. Но в любом случае максимальный срок инициации процедуры **chargeback** ограничен 540 днями

(примерно 18 месяцев) с момента проведения платежа.

Следует отметить, что процедура **chargeback** доступна лишь при условии совершения расчета самой картой, т.е. с использованием ее номера и иных реквизитов. При расчетах с использованием онлайн-банкинга или при переводах с расчетного счета, к которому открыта банковская карта, данная процедура неприменима, поскольку при таких расчетах платежная система не задействуется. Но к ним в полной мере применимы рассмотренные ранее положения [Закона](#) об НПС, относящиеся к распределению рисков совершения платежей без согласия плательщика.

Безусловно, помимо процедуры **chargeback** существует возможность непосредственного обращения клиента с соответствующим требованием к интернет-магазину, однако перспективы удовлетворения данного требования крайне незначительны в случаях, если такой интернет-магазин находится в другой юрисдикции и не обладает высокой репутацией, которую он ценит. В связи с этим **chargeback** является наиболее реальным и отработанным способом возврата денежных средств, уплаченных банковской картой, в случае недобросовестности контрагента.

§ 3. Правовое регулирование расчетов, осуществляемых с использованием электронных денег

Как отмечалось ранее, электронные деньги характеризуются тем, что их использование не сопряжено с открытием банковского счета. По идее, это обеспечивает облегченный и более доступный порядок совершения платежных операций с такого рода платежными инструментами. Для того чтобы

определить место электронных платежей в системе современной электронной коммерции, необходимо указать их преимущества по сравнению с платежами банковскими картами.

Рассмотрим преимущества электронных денег, которые традиционно принято выделять, 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 <1>.

<1> 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 проблематичным. Так что любые иные механизмы, позволяющие минимизировать распространение персональных данных в сети Интернет, являются весьма востребованными.

Вместе с тем возможность совершения анонимных платежей может быть использована с целью отмыwania 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. Как будет показано далее, в свете недавно принятого в Российской Федерации законодательства данное преимущество электронных денег практически сведено на нет.

Во-вторых, использование электронных денег позволяет 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" <1>. Реализация микроплатежей посредством платежных карт по общему правилу неэффективна, так как комиссии, которые необходимо будет уплатить банку-эквайеру за обслуживание такого платежа, сопоставимы или даже превышают его размер, что делает произведенные микроплатежи убыточными для получателя.

<1> См., например: Юрасов А.В. Указ. соч. С. 266.

Долгое время считалось, что потенциально высокий спрос на микроплатежи в интернет-коммерции способен оказать значительное влияние на развитие электронных денег <1>. Особенно ценной возможностью осуществления микроплатежей виделась 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. Однако и это часто упоминаемое преимущество электронных денег также далеко от современных реалий электронной коммерции. Ориентация большинства современных бизнес-моделей интернет-сервисов на

использование возможности обработки персональных данных пользователей в качестве "средства оплаты" за предоставленный контент или сервис фактически превратило такие данные в "валюту", устранив тем самым необходимость создания и обслуживания громоздкой и дорогостоящей инфраструктуры электронных денег для обеспечения микроплатежей.

<1> Себестоимость розничного платежа для кредитного учреждения составляет в среднем около 1 долл. См.: Технологии **CyberPlat(R)** ("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.

В-третьих, отмечается, что 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. Здесь следует отметить тот факт, что завести электронный кошелек может даже несовершеннолетнее лицо, которое просто так не сможет открыть банковский счет. Данная возможность особенно ценна при осуществлении расчетов в онлайн-играх.

В целом можно отметить, что феномен электронных денег как некоего альтернативного платежного инструмента в сфере электронной коммерции зародился и получил распространение преимущественно в период, когда онлайн-банкинг был редкостью, а использование банковских карт не имело массового характера. В настоящее время все более стираются границы между использованием электронных денег и банковских карт. Происходит конвергенция данных платежных инструментов: пополнить кошелек можно с банковской карты, равно как существуют возможности "вывода" средств с электронного кошелька на банковскую карту. За многими известными системами электронных денег стоят крупные банки. Если бы не определенные различия в публично-правовом регулировании расчетов электронных денег (особенности бухгалтерского учета, требований к эмитентам, требования идентификации плательщика и связанные с этим ограничения на размеры платежей и т.п.), то разграничивать их было бы крайне сложно. Особняком стоят так называемые криптовалюты ^{<1>}, которые функционируют на иных принципах, чем классические электронные деньги, и которые никак не урегулированы [Законом](#) об НПС. Не исключено, что со временем понятие электронных денег будет ассоциироваться именно с криптовалютами.

^{<1>} Под криптовалютой можно понимать разновидность электронных денег, эмиссия и учет которых базируется на криптографических методах, а функционирование самой платежной системы происходит децентрализованно в компьютерной сети. При этом внутренняя стоимость денежных единиц криптовалюты обычно неразрывно связана со

значительными затратами на совершение соответствующих операций.

Правовое регулирование электронных денег по [Закону](#) об НПС

До недавнего времени электронные деньги в России не имели специального правового регулирования, по крайней мере на уровне законов и иных нормативных правовых актов <1>.

<1> Обзор правового регулирования электронных денег в США и Европейском союзе см. в первом издании настоящей книги. С. 399 - 410.

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 другими документами с использованием в них аналогов собственноручной подписи, кодов, паролей и иных средств, подтверждающих, что распоряжение дано уполномоченным на это лицом <1>.

<1> См.: Мартынов В.Г., Андреев А.Ф., Кузнецов В.А., Шамраев А.В. и др. Указ. соч. С. 5.

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. N 277-У "О порядке выдачи регистрационных свидетельств кредитным организациям-резидентам на осуществление эмиссии предоплаченных финансовых продуктов" <1>. Данный документ был в течение долгого времени практически единственным источником правовых норм об электронных деньгах в России <2>. 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 договорной модели. В период действия данного [указания](#) регистрационное свидетельство было выдано лишь одному эмитенту электронных денег - банку "Таврический".

<1> Отменено в связи с принятием [Положения](#) Банка России от 24 декабря 2004 г. N 266-П "Об эмиссии банковских карт и об операциях, совершаемых с использованием платежных карт".

<2> См. подробнее: Башкатов М. Правовая природа "электронных денег" // Хозяйство и право. 2003. N 8. С. 85.

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 кардинально 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. N 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>}.

^{<1>} См., например: Лисицын А.Ю. [Систематизация в эмиссионном праве](#) // Реформы и право. 2012. N 4.

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) <1>.

<1> 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" является широко распространенным в юридических и экономических кругах в России и за рубежом.

Исходя из приведенной дефиниции можно выделить следующие существенные признаки электронных денег: (1) в их основе лежат денежные средства, которые (2) были предварительно предоставлены одним лицом другому лицу (3) с целью исполнения обязательств их владельца перед третьими лицами; данные денежные средства (4) учитываются без открытия банковского счета, распоряжение (5) осуществляется исключительно с использованием электронных средств платежа.

В приведенных признаках выражена квинтэссенция специального правового режима электронных денег. Так, первый признак создает основания для разграничения электронных денег и иных систем расчетов, оперирующих не денежными средствами, а иными объектами, например, имущественными правами на титульные знаки (**Webmoney**) <1> или различного рода "миллями". Во

втором признаке предусматривается запрет на кредитование электронными деньгами и подчеркивается их статус - исключительно для предоплаты. Третий признак позволяет отграничить электронные деньги от отдельных видов подарочных и бонусных карт. Четвертый признак дает возможность разграничить электронные деньги и инструменты онлайн-банкинга. Пятый признак позволяет лишний раз подчеркнуть тесную взаимосвязь функционирования системы платежей электронными деньгами с информационными технологиями: в платежных системах электронных денег нельзя осуществить платежи или иные операции с денежными средствами в отрыве от электронного средства платежа, например, позвонив в колл-центр оператора и дав ему указание совершить определенную транзакцию. Указанные признаки будут подробно рассмотрены далее.

<1> Представители **Webmoney** заявляют, что данная система не является эмитентом электронных денежных средств, а осуществляет выпуск так называемых титульных знаков. 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 (условная сетевая стоимость) устанавливается его держателями, а порядок передачи и учета соответствует процедурам обращения сообщений формата "Титульные знаки" в **Webmoney Transfer**. Данные титульные знаки различаются 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, а 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, публикует на веб-сайте системы оферту по купле-продаже 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 договора хранения имущественных прав (**WMX**). Таким образом, по мнению **Webmoney**, [Закон](#) об НПС не распространяется на данную систему (см. подробнее: **WebMoney** обозначила свою позицию по поводу [Закона](#) об НПС. 23.08.2011. URL:

<http://owebmoney.ru/inform/pozitsia-po-povodu-zakona/>).

Следует отметить, что многие из приведенных аргументов были в свое время подтверждены судом (см.: [Постановление](#) Девятого арбитражного апелляционного суда от 22 ноября 2010 г. N 09АП-26842/2010-АК по делу N А40-71965/10-140-346). Однако это было до вступления в силу Закона об НПС. Позиция автора по данному вопросу изложена в первом издании настоящей книги. С. 422 - 427.

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>.

<1> Шамраев А.В. [Законодательство о национальной платежной системе](#) и его влияние на развитие платежных инноваций // Банковское право. 2011. N 5.

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) <1>. 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. рублей. Фактически НКО можно рассматривать в качестве некой упрощенной формы банка, функционирующего в сфере электронных платежей.

<1> 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. N 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). Использование размещенных на счете абонента оператора мобильной связи денежных средств для расчетов с третьими лицами возможно на условиях [ст. 13](#) Закона об НПС при наличии соглашения такого оператора связи с оператором электронных денежных средств, который фактически осуществляет конвертацию средств абонента на счете оператора сотовой связи, представляющих собой аванс за услуги

связи <2>, в электронные деньги. На практике абонент для совершения мобильных платежей с использованием остатка денежных средств на своем лицевом счете также должен заключить отдельное соглашение с оператором связи и соответствующим оператором электронных денежных средств. Такое соглашение заключается в порядке акцепта публичной оферты посредством конклюдентных действий <3>.

<1> См.: [разъяснения](#) ЦБ РФ по вопросам применения отдельных положений Федерального закона от 27 июня 2011 г. N 161-ФЗ "О национальной платежной системе" от 28 февраля 2013 г. // http://cbr.ru/press/Archive_get_blob.aspx?doc_id=130228_1809533.htm.

О правовой природе подарочных карт и сертификатов см.: Брагинец А. [Подарочные карты и сертификаты](#): практические проблемы юридической квалификации // Закон. 2015. N 11.

<2> По мнению судов, поскольку денежные средства, размещенные на расчетном счете абонента оператора сотовой связи, представляют собой предварительную оплату услуг, оказываемых оператором связи, они не могут быть предметом ареста (см.: [Определение](#) ВС РФ от 28 октября 2015 г. N 84-КГ15-9). Это также свидетельствует о различных правовых режимах средств на лицевом счете оператора связи и электронных денег, на которые вполне может быть обращено взыскание.

<3> См., например: условия оказания услуги "Мобильные платежи" ПАО "Мегасон" // https://moscow.megaфон.ru/download/~federal/oferts/oferta_

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 поднадзорными организациями, которые влияют на бесперебойность функционирования платежной системы либо на услуги, оказываемые участникам платежной системы и их клиентам, ЦБ РФ может приостановить оказание таковыми 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" <1>.

<1> 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. N 6. P. 59 - 60.

Указанное ограничение существенно ограничивает рыночные возможности эмитентов электронных денег. В отличие от банков они не могут организовывать партнерские акции с иными организациями, создавая кобрендинговый продукт (карту), и предусматривать возврат определенной суммы в электронный кошелек при совершении покупок в этих организациях. Это однако не препятствует возможности таких организаций предоставлять скидки на свои товары (услуги) при оплате электронными деньгами.

Законом об НПС 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 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. 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 которых есть иностранная валюта, 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. N 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 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.

<1> РГ. 2003. 17 дек.

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 ко 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 самым 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 касаются **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 и объем переводов в течение месяца. В рамках так называемого антитеррористического пакета законов, подготовленных после терактов в Волгограде в 2013 г., регулирование в указанной сфере было существенно расширено по сравнению с первоначально заложенным в Законе об НПС <1>. В настоящее время в ст. 10 данного Закона предусматривается три степени идентификации физического лица - владельца

электронного кошелька. При проведении полной идентификации такого владельца, максимальный размер остатка в его персонализированном электронном кошельке не может превышать 600 тыс. рублей, а ограничения на объем совершаемых им платежей не устанавливаются. Правда, конкретная платежная система может устанавливать свои лимиты и ограничения.

<1> Федеральный [закон](#) от 5 мая 2014 г. N 110-ФЗ "О внесении изменений в отдельные законодательные акты Российской Федерации".

Неперсонифицированные (анонимные) электронные кошельки, владельцы которых не прошли идентификацию, и анонимные переводы электронных денег с таких кошельков хотя и не запрещены **per se**, но имеют весьма ограниченную платежную способность: их лимит остатка не может превышать 15 тыс. рублей. При этом общая сумма переводимых электронных денежных средств с использованием одного неперсонифицированного электронного средства платежа не может превышать 40 тыс. рублей. в течение календарного месяца. Платежная система может устанавливать дополнительные ограничения, например, по географии платежа (получателем может выступать только российский интернет-магазин), характеру платежа (невозможность перевода средств между различными платежными системами) и т.п.

Существует и определенное "промежуточное" состояние электронных кошельков рассматриваемых видов. В случае прохождения физическим лицом упрощенной идентификации электронный кошелек

может использоваться для перевода электронных денежных средств в пользу юридических лиц и индивидуальных предпринимателей при условии, что остаток таких средств в любой момент не превышает 60 тыс. рублей, а общая сумма переводимых электронных денежных средств с использованием такого неперсонифицированного электронного средства платежа - 200 тыс. рублей в течение календарного месяца.

При этом неперсонифицированный электронный кошелек не может использоваться клиентом - физическим лицом, не прошедшим упрощенную идентификацию, для осуществления перевода электронных денежных средств другому физическому лицу либо для получения переводимых электронных денежных средств от другого физического лица. Платежи с анонимного электронного кошелька могут совершаться лишь в адрес российских коммерческих и некоторых некоммерческих (например, религиозных, благотворительных, ТСЖ и т.п.) организаций, но не могут совершаться в адрес других граждан, иностранных организаций и физических лиц.

Порядок идентификации и упрощенной идентификации установлен Федеральным [законом](#) от 7 августа 2001 г. N 115-ФЗ "О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма". Идентификация может производиться как самой кредитной организацией (эмитентом электронных денег), так и привлеченными ею лицами. Так, в соответствии с [ч. 1.5 ст. 7](#) указанного Закона процесс прохождения идентификации или упрощенной идентификации клиента - физического лица можно поручить другой кредитной организации, организации

федеральной почтовой связи, банковскому платежному агенту, оператору сотовой связи, аккредитованному удостоверяющему центру. В частности, идентификация может осуществляться посредством личного предоставления владельцем электронного кошелька необходимых документов в офисе эмитента электронных денег или уполномоченного им представителя, например, в офисах партнеров. Также многие эмитенты электронных денег предусматривают возможность отправки по почте нотариально заверенного заявления на идентификацию с копией паспорта.

Упрощенная процедура идентификации предполагает необходимость установления сведений о физическом лице: Ф.И.О. и реквизитах документа, удостоверяющего личность такого лица, и их подтверждения посредством предоставления оригинала такого документа или его надлежащим образом заверенной копии. Правда, появляется возможность проверки такой достоверности посредством авторизации на портале Госуслуги через систему ЕСИА или использования информации из государственных информационных систем, предусмотренных Правительством РФ. Однако, учитывая что в сфере электронной коммерции такого рода средства идентификации используются весьма нечасто, получается, что порядок прохождения упрощенной идентификации мало чем отличается от процедуры прохождения полной идентификации.

Организации и индивидуальные предприниматели могут использовать электронные кошельки лишь при условии прохождения полной идентификации. Остаток электронных денежных средств на таком корпоративном кошельке не должен

превышать 600 тыс. рублей либо сумму в иностранной валюте, эквивалентную 600 тыс. рублей по официальному курсу Банка России на конец рабочего дня оператора электронных денежных средств (допускаются некоторые отклонения от данной суммы, вызванные колебаниями курса валюты).

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. При этом ограничений на объем операций, совершаемых при помощи корпоративного кошелька, не предусмотрено.

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. В связи с этим, несмотря на 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. N 48; Генкин А., Суворова Е. Указ. соч. С. 247; Шахунян М. **Кошелёк или веб-суррогат?** // ЭЖ-Юрист. 2010. N 24.

<3> Балкаров А. **Реальный оборот виртуальных денег** // ЭЖ-Юрист. 2012. N 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 **clip-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. В данном случае применяются те же правила, что и при расчетах банковскими картами. Распределение рисков построено на основе принципа "рискует тот, кто не уведомляет". В случае обнаружения факта несанкционированного использования 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 в порядке, установленном договором, 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>. Важно отметить, что взимание платы за информирование клиента является неправомерным, что, однако, не исключает возможности взимания платы за способы информирования, дополнительные (например, за информирование посредством **sms**) по отношению к основным, предусмотренным в договоре (например, посредством предоставления выписки по счету в офисе

оператора, звонка на службу поддержки клиентов, предоставления данных о транзакции в онлайн-банкинге и пр.).

<1> Положения **ч. ч. 4 - 8 ст. 9** Закона о НПС, посвященные распределению рисков совершения несанкционированных операций, вступили в силу с 1 января 2014 г.

Правовая природа электронных денег

До принятия **Закона** о НПС в юридической литературе было высказано множество различных толкований понятия электронных денег, в числе которых можно выделить следующие:

- юридически значимые информационно-цифровые импульсы или же определенная последовательность цифр, символизирующих (заменяющих) банкноты и монеты <1>;

<1> Тедеев А.А. Электронная коммерция. М., 2002. С. 136 - 137.

- разновидность ценных бумаг на предъявителя <1>;

<1> В качестве особой формы бездокументарного векселя интерпретирует электронные деньги В.Н.

Назаров (см.: Назаров В.Н. [Деньги как категория финансового права](#) // Финансовое право. 2009. N 7). Ранее уже отмечалось, что данной точки зрения и поныне придерживаются в системе **Webmoney**, рассматривая оборот титульных знаков, номинированных в рублях, в качестве расчетов чеками в электронной форме.

- особый инструмент, средство распоряжения правом требования выплаты денежных средств <1>;

<1> Башкатов М. Правовая природа "электронных денег". С. 90.

- согласованный сторонами иной способ исполнения денежного обязательства <1>.

<1> Калятин В.О. Право в сфере Интернета. С. 380.

[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. Можно согласиться с мнением М. Башкатова в том, что 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 <1>.

<1> Башкатов М. Правовая природа "электронных денег". С. 90.

Некоторые авторы идут еще дальше, признавая электронные деньги в качестве законного платежного средства между участниками платежной системы <1>. Представляется, что все же данный вывод несколько преждевременный.

<1> Шевчук М.В. [Правовая природа электронных денежных средств](#) // Юрист. 2012. N 12.

Ключевым признаком законного платежного средства является возможность погашения должником своего денежного обязательства без предварительного согласования его использования с кредитором. К примеру, если кредитор не участвует в системе **"ЯндексДеньги"**, его нельзя обязать принять в качестве платежа электронные денежные средства, 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 рамках существующих ограничений

по их использованию. В условиях, когда на и без того урегулированную сферу их применения накладываются дополнительные ограничения по характеру их использования, сложно говорить о повышенной хозяйственной обращаемости, имманентной закону средству платежа.

Таким образом, на данном этапе развития и регулирования электронных денег в России признать их законным средством безналичного платежа нельзя <1>. Их использование является сугубо добровольным и сопряжено с рядом значительных ограничений. Однако потенциально не исключена возможность придания электронным деньгам статуса законного средства платежа, о чем свидетельствует практика некоторых зарубежных стран. Но для этого должны "созреть" участники оборота и регуляторы, инфраструктура, 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 общества.

<1> В соответствии со [ст. 29](#) Федерального закона от 10 июня 2002 г. N 86-ФЗ "О Центральном банке Российской Федерации (Банке России)" банкноты и монеты Банка России являются единственным законным средством наличного платежа на территории Российской Федерации. В данной [статье](#) говорится о законном платежном средстве **наличного** платежа, что тем самым подразумевает возможность существования законного 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, трактовка которых в качестве "незаконного средства платежа" вряд ли будет соответствовать здравому смыслу. К тому же согласно НК РФ налоги могут быть уплачены безналичными денежными средствами, что лишний раз подтверждает их законный характер. А ведь, как известно, "налоги делают деньги деньгами" (Wray R. Modern Money Theory: A Primer on Macroeconomics for Sovereign Monetary Systems. Palgrave Macmillan. 2012. P. 49).

§ 4. Виртуальная валюта как особый вид электронных денег

Понятие и виды виртуальной валюты

Не успели регуляторы разобраться с регламентацией существующих систем электронных денег, как появились новые виды валюты, основанные на принципиально иных подходах, нежели классические системы электронных денег. К таким новым видам валюты можно отнести внутриигровую валюту, которая используется в популярных онлайн-играх, и криптовалюту. Обобщенно данные виды "денег" обычно именуются "виртуальная валюта" (**virtual currency**).

В докладе Европейского центрального банка (ЕЦБ) под виртуальной валютой понимаются "нерегулируемые цифровые денежные средства, которые эмитируются и контролируются их разработчиками, используются и принимаются членами определенного виртуального сообщества" <1>.

<1> Virtual Currency Schemes. ECB Report. October 2012. P. 13. URL: <https://goo.gl/TKIFap>.

Виртуальные валюты ЕЦБ разделил на три вида: 1) системы виртуальных валют закрытого типа, используемые в онлайн-играх (например, в **Worlds of Warcraft**). Ко второму виду относятся системы, где обмен возможен только в одну сторону, как правило, допускается покупка виртуальной валюты (в качестве примера приводится **Facebook Credits**, просуществовавшая до сентября 2013 г., или "мили", приобретаемые в рамках программ лояльности авиакомпаний). К третьему виду относятся системы с возможностью двустороннего обмена, т.е. речь идет о конвертируемой виртуальной валюте, имеющей обменный курс покупки и продажи (**Linden Dollars, Bitcoin**).

При этом в докладе ЕЦБ особо подчеркивается, что по мере развития данного вида валюты дефиниция потребует уточнений. И действительно, сейчас уже можно говорить о том, что данное определение не в полной мере отражает признаки виртуальных валют. В частности, как будет показано далее, основанные на математических принципах децентрализованные валюты, такие как **Bitcoin**, не выпускаются (не эмитируются) и не контролируются центральным разработчиком, а в некоторых странах (например, в США и Таиланде) в настоящее время осуществляется регулирование виртуальных валют.

В новой редакции доклада ЕЦБ, подготовленной в феврале 2015 г., дается уже иная дефиниция виртуальной валюты: "Цифровое представление ценности, не эмитированное центральным банком, кредитным учреждением или эмитентом электронных

денег, которая может при определенных обстоятельствах служить в качестве альтернативы деньгам" <1>. Из данной дефиниции видно, что в настоящее время ЕЦБ не рассматривает виртуальную валюту ни в качестве денежных средств (экономический аспект), ни в качестве платежного средства (юридический аспект), что, по-видимому, является следствием рассмотрения феномена **Bitcoin** и иных виртуальных валют через призму традиционных представлений о деньгах и законных платежных средствах, а также обозначенной ЕЦБ малой распространенности виртуальных валют. Как будет продемонстрировано далее, данная позиция ЕЦБ и подход к понятию виртуальных валют являются спорными, а в свете недавнего решения Европейского суда справедливости, по сути признавшего **Bitcoin** валютой для целей налогообложения <2>, - в значительной степени устаревшими.

<1> Virtual Currency Schemes: Further Analysis. ECB Report. February 2015. P. 25. URL: <https://goo.gl/UExD0p>.

<2> Skatteverket v. David Hedqvist, ECJ, 20 October 2015, C-264/14.

Более удачным представляется определение виртуальной валюты, данное ФАТФ (Группа разработки финансовых мер борьбы с отмыванием денег; от англ. **FATF - The Financial Action Task Force**), которое дано через призму анализа классических функций денег <1>. В соответствии с ним виртуальная валюта представляет собой "средство выражения стоимости, которым можно торговать в цифровой форме и которое функционирует

в качестве (1) средства обмена; и/или (2) расчетной денежной единицы; и/или (3) средства хранения стоимости, но не обладает статусом законного платежного средства (т.е. не является официально действующим и законным средством платежа при расчетах с кредиторами) ни в одной юрисдикции". Как отмечает ФАТФ, виртуальная валюта не эмитируется и не обеспечивается ни одной юрисдикцией и выполняет вышеуказанные функции только по соглашению в рамках сообщества пользователей виртуальной валюты. Виртуальная валюта тем самым отличается от фиатной <2> валюты (также называемой "реальными деньгами" или "национальной валютой"), представляющей собой монеты и бумажные деньги страны, которые являются ее законным средством платежа, обращаются и повсеместно используются и принимаются в качестве средства обмена в стране-эмитенте.

<1> Виртуальные валюты: ключевые определения и потенциальные риски в сфере ПОД/ФТ. Отчет ФАТФ. Июнь 2014. С. 6. URL: <https://goo.gl/xa0HYM>.

<2> Фиатные деньги (от лат. **fiat** - декрет, указание "да будет так") - это деньги, номинальная стоимость которых устанавливается и гарантируется государством вне зависимости от стоимости материала, из которого деньги изготовлены, или находящиеся в хранилище банка (необеспеченные деньги).

Достаточно интересной является дефиниция виртуальной валюты, закрепленная в законе штата Нью-Йорк. Данная дефиниция состоит из трех частей. В первой дается общее определение: "Под виртуальной

валютой понимаются любые цифровые единицы, которые используются в качестве средства обмена или формы хранения стоимости в цифровой форме". Вторая часть дефиниции приводит возможные виды виртуальных валют, которые охватываются специальным регулированием, к ним относятся цифровые единицы, которые: i) имеют централизованную систему администрирования или репозиторий; ii) являются децентрализованными и не имеют централизованного репозитория или администратора или iii) создаются/приобретаются в результате компьютерных вычислений. Наконец, третья часть дефиниции предусматривает перечень исключений. Так, понятие виртуальной валюты не включает: 1) внутриигровую валюту, которая не имеет применения за пределами игры, не может быть конвертирована в фиатные деньги или виртуальную валюту и не может выступать в качестве средства платежа за какие-либо товары, услуги, скидки или приобретения в реальном мире; 2) скидки и бонусы, используемые в рамках программ лояльности, которые не могут быть конвертированы в фиатные деньги или виртуальную валюту; 3) цифровые единицы стоимости, являющиеся частью "предоплаченных" карт.

Далее имеет смысл подробнее остановиться на рассмотрении Bitcoin как наиболее интересного и популярного вида виртуальной валюты, учитывая, что отдельные вопросы, связанные с правовым статусом внутриигровой валюты, были рассмотрены ранее <1>.

<1> См. [гл. 6](#) настоящей работы.

Криптовалюта Bitcoin: основные черты и основы функционирования

В самом обобщенном виде криптовалюту можно определить как разновидность электронного средства обмена, имеющего анонимный и децентрализованный характер, в основе которого лежат криптографические алгоритмы. Наиболее известным видом криптовалюты является **Bitcoin** (в русской версии - **биткойн** или **биткойн**). Существуют и иные виды криптовалют: **Litecoin**, **Namecoin**, **PPcoin** и др., которые иногда обобщенно называют **Altcoin** (от англ. **alternative coin**), но пока их популярность и рыночная капитализация не идут ни в какое сравнение с **Bitcoin**, поэтому имеет смысл остановиться на рассмотрении именно этой валюты, принимая во внимание, что все иные децентрализованные платежные системы построены на схожих принципах.

Bitcoin был разработан программистом или группой программистов под псевдонимом **Сатоши (Сатоси) Накомото**, за авторством которого в ноябре 2008 г. была опубликована "Белая книга" с описанием механизма функционирования **Bitcoin** и его протокола <1>. **Bitcoin** представляет собой основанную на свободном программном обеспечении (**open source**), децентрализованную пиринговую (**peer to peer**) цифровую валюту. Отличительными чертами криптовалюты **Bitcoin** являются:

<1> Satoshi Nakamoto. Bitcoin: A Peer-to-Peer Electronic Cash System. P. 3 // www.bitcoin.org.

1) **анонимность**. Для использования **Bitcoin** не требуется прохождения регистрации или идентификации. Достаточно установить специальное приложение ("кошелек"), чтобы начать использовать

данную валюту. Каждый кошелек состоит из содержащихся в нем единиц **Bitcoin**, публичного и частного ключей. Публичный ключ (адрес) необходим для того, чтобы другие участники могли отправить **Bitcoin** на данный кошелек. Частный ключ используется для перевода **Bitcoin** на другой кошелек. Сам платеж осуществляется путем указания владельцем единицы **Bitcoin** нового публичного адреса на ней и ее подписания своим частным ключом. Все транзакции с использованием **Bitcoin** публичны и информация о них мгновенно распространяется в сети Интернет, означая, что все могут видеть баланс и транзакции любого **Bitcoin**-адреса, хотя формально реальная личность, стоящая за ними, является скрытой. Однако анонимность платежей с использованием **Bitcoin** не стоит переоценивать. Как только определенный публичный адрес использован, можно проследить все транзакции, в которых он участвовал. Каждый может посмотреть баланс и все транзакции любого из адресов. В связи с этим деанонимизация может произойти при анализе сопутствующих транзакции обстоятельств. Например, при расчетах биткоинами в интернет-магазине пользователь для получения товаров или услуг, как правило, должен раскрыть определенную информацию о себе, например, сообщить свое местонахождение. Установление связи между совершенной **Bitcoin**-транзакцией и конкретной личностью может быть осуществлено и иными способами, например, на стадии конвертации **Bitcoin** в национальную валюту <1>. В связи с этим **Bitcoin**-адреса не могут быть **полностью** анонимными <2>, корректнее говорить о "псевдоанонимности";

<1> См. подробнее: Как сохранить анонимность при выводе BTC в фиат? // Bitcoin Journal. 29.12.2013.

URL: <http://bitcoinjournal.ru/vyvod-bitkoinov/>.

<2> В связи с этим для поддержания анонимности обычно рекомендуется не использовать один и тот же публичный адрес для получения платежа. Кроме того, рекомендуется создавать множество кошельков и использовать сервисы "миксеров", которые предлагают уменьшить отслеживаемость платежа, обменивая одинаковые суммы между разными пользователями с независимыми биткоин-адресами. "Миксеры" принимают биткоины с нескольких адресов и пересылают их на несколько других. В итоге получается единая транзакция, у которой получатели известны, плательщики тоже, но при этом неизвестно, кто именно из них кому и что именно передал (об этом знает только сам "миксер"). При этом возможно последовательное использование сразу нескольких "миксеров".

2) **децентрализованный характер.** Система **Bitcoin** не имеет единого эмиссионного центра либо централизованного органа управления и контроля. С технической точки зрения **Bitcoin** представляет собой некий файл, содержащий шифр, вычисляемый по определенному алгоритму. При этом появление такого файла происходит в результате функционирования вычислительных мощностей сообщества пользователей **Bitcoin**. Разработчики протокола **Bitcoin** также не имеют контроля над Bitcoin-транзакциями: соответствующий программный код является открытым и распространяется на условиях open source лицензии MIT <1>. Каждый может анализировать соответствующий код на предмет отсутствия скрытых возможностей контроля у разработчиков, а также создавать свои модификации. При этом они могут стать стандартом только будучи принятыми большинством пользователей, что обеспечивает необходимость

консенсуса **Bitcoin**-сообщества по ключевым вопросам функционирования данной системы.

<1> <https://github.com/bitcoin/bitcoin>. Подробнее о понятии open source и условиях лицензии MIT см.: Савельев А.И. Лицензирование программного обеспечения в России. Законодательство и практика. М.: Инфотропик, 2012. С. 335 - 362.

Отсутствие централизованного контроля над **Bitcoin**-транзакциями создает существенные проблемы для их государственного регулирования. Как отмечается Росфинмониторингом, "процесс выпуска и обращения наиболее распространенных криптовалют полностью децентрализован и отсутствует возможность его регулирования, в том числе со стороны государства"

<1>;

<1> Информационное сообщение Росфинмониторинга от 6 февраля 2014 г. "Об использовании криптовалют". URL: <http://www.fedsfm.ru/news/957>.

3) **математический алгоритм - основа ценности Bitcoin**. В качестве обеспечения **Bitcoin** выступает не какая-либо ценность физического мира (например, золото) или авторитет государственного органа (как в случае с фиатными деньгами), а математические расчеты. Единицы **Bitcoin** создаются в результате деятельности, получившей название **mining** (добыча). Любое лицо, установившее специальное программное обеспечение, может "заработать", а точнее, создать определенное количество валюты **Bitcoin** по факту

решения его компьютером сложных вычислительных задач (**hashes**), связанных с верификацией транзакций, совершаемых в платежной системе **Bitcoin**. Такие лица обычно именуются майнерами. Нередко майнеры объединяют свои вычислительные мощности в единый пул с последующим распределением "заработка". Сложность решения задачи обуславливает сложность заработка единицы **Bitcoin**, а тем самым и ее ценность, предотвращая возможные манипуляции с "эмиссией". Алгоритмы функционирования **Bitcoin**, предопределяют наличие максимального размера единиц, находящихся в обращении (порядка 21 млн.). Таким образом, данная валюта защищена от инфляции в отличие от обычных фиатных денег, которые потенциально могут быть напечатаны в неограниченном объеме. Ожидается, что последняя единица **Bitcoin** будет создана в районе 2040 г. <1>. По состоянию на 31 мая 2016 г. в обороте находилось около 15,6 млн. единиц **Bitcoin** <2>. При этом суммарное выражение стоимости **Bitcoin** на указанный момент составляло примерно 8,4 млрд. долл. <3>.

<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> <https://markets.blockchain.info>

Таким образом, подобно тому, как затраты, связанные с добычей и обработкой золота,

способствуют его ценности, затраты на производство соответствующих вычислений (главным образом траты на необходимое оборудование и электричество) и наличие предельного размера эмитированных единиц обуславливают 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;

4) **отсутствие доверенной третьей стороны для верификации транзакций.** Любые электронные деньги имплицитно содержат в себе риск двойного расходования. В условиях отсутствия у электронной единицы валюты физической сущности, свойственной наличным деньгам и обеспечивающей посредством владения возможность исключать одновременную их передачу нескольким лицам, для исключения возможности одновременной передачи электронной единицы валюты нескольким лицам необходимо привлечение доверенной третьей стороны. В традиционных системах 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 синхронно 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. Полная

история всех транзакций, совершенных с **Bitcoin** с момента возникновения данной системы, и представляет собой базу данных **Blockchain**.

По сути **Blockchain** представляет собой распределенную между всеми участниками сети **Bitcoin** учетную книгу. Каждый пользователь **Bitcoin**-кошелька хранит на своем компьютере такую базу данных, содержащую историю всех операций, когда-либо осуществленных в системе. Это обеспечивает прозрачность каждой транзакции и возможность верификации происхождения каждого **Bitcoin** любым заинтересованным пользователем.

Участники сети **Bitcoin** делятся на четыре группы: 1) обычные пользователи, которые создают новые записи; 2) майнеры, которые создают из записей о транзакциях блоки; 3) предприниматели, которые принимают **Bitcoin** в оплату за предоставляемые товары и услуги; и 4) биржи, которые позволяют осуществлять обмен **Bitcoin** на обычную валюту и наоборот.

В рассматриваемом контексте нас интересуют первые две группы, поскольку именно они формируют данные **Blockchain**. Обычные пользователи создают и распространяют по сети записи о денежных переводах. Майнеры собирают записи, проверяют их и записывают в блоки, а затем рассылают эти блоки по сети. Участники сети проверяют созданный блок, после чего он становится подтвержденным и занимает свое место в **Blockchain** и каждый последующий блок должен будет включать в себя его хэш. Новые блоки всегда добавляются в конец цепочки.

Используемая при создании блоков технология

шифрования предотвращает возможные манипуляции данными, "увековечивая" каждую произведенную транзакцию. Технически это достигается при помощи последовательного шифрования данных о каждой последующей транзакции. При этом каждой заносимой в блок транзакции присваивается криптографический идентификатор (хэш), который добавляется в заголовок записи о следующей транзакции и так далее, так что хэш транзакции на вершине цепочки содержит зашифрованные данные обо всех предыдущих операциях, записанных в блоке. Вмешаться и изменить уже записанную транзакцию нельзя, так как это скомпрометирует всю цепочку: надо будет пересчитывать хэш не только меняемого блока, но и всех последующих. Таким образом, всегда можно определить, кому и в какой момент времени принадлежит конкретный **Bitcoin**, а благодаря технологии **Blockchain** существует единая для всех версия "правды" относительно его принадлежности, которая не может быть пересмотрена по инициативе какого-либо пользователя или посредника <1>.

<1> Таким образом, ситуация, при которой некое лицо вдруг объявит о том, что "нельзя прикрываться бумажками о праве собственности", невозможна в рамках существующей технологии **Bitcoin**.

Неподтвержденная большинством участников системы транзакция будет отвергнута и не станет частью **Blockchain**, в связи с чем **Blockchain** иногда именуется системой, основанной на консенсусе - **consensus-based system**. Все это создает беспрецедентный уровень доверия между пользователями криптовалюты **Bitcoin**, обеспеченной

математическими алгоритмами и невозможностью внесения изменений в данные **Blockchain** в отсутствие у злоумышленника вычислительных мощностей в объеме, превышающем 50% всех вычислительных мощностей, задействованных в платежной системе **Bitcoin** <1>. Таким образом, чем больше лиц использует **Bitcoin**, тем сложнее скомпрометировать данные **Blockchain**.

<1> Tim Swanson. Great Chain of Numbers. 2014. P. 18. URL: <https://goo.gl/IBDVE5>.

Поскольку валидация платежа и сопутствующие ей математические операции требуют значительных вычислительных мощностей, в отсутствие централизованного органа управления системой единственный вариант их обеспечения заключается в том, чтобы пользователи сами предоставляли собственные компьютерные ресурсы для осуществления таких вычислений. Упомянутый 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>. Таким образом, эмиссия единиц **Bitcoin** неразрывно связана с осуществлением заинтересованными пользователями данной платежной системы деятельности по верификации транзакций в интересах всех ее участников.

<1> Satoshi Nakamoto. Bitcoin: A Peer-to-Peer Electronic Cash System. P. 3 // www.bitcoin.org.

Преимущества и риски использования Bitcoin

Основные преимущества **Bitcoin** для плательщика можно свести к следующим:

1) отсутствие необходимости прохождения каких-либо формальностей перед использованием: не требуется заключать договор, проходить идентификацию и пр.;

2) анонимность и отсутствие необходимости передачи третьим лицам "чувствительных" данных, содержащих персональные данные или сведения об объекте покупки;

3) низкие транзакционные издержки: отсутствие обязательных комиссий за перевод. По сути, отправить **Bitcoin** также просто и дешево, как отправить **e-mail**. Возможно добавление небольшой суммы к транзакции, которая отойдет к майнеру, успешно создавшему блок для этой транзакции. Такая комиссия устанавливается исключительно по усмотрению плательщика и ускоряет проведение транзакции, но не является необходимым условием ее проведения. Значение такой комиссии по умолчанию - 0,0001 **Bitcoin** (исходя из курса 528,56 USD за 1 **Bitcoin** на 31 мая 2016 г. это порядка 0,05 USD);

4) глобальный характер **Bitcoin** обуславливает легкость осуществления платежей в любую точку земного шара;

5) идея использования электронных денег для микроплатежей находит свое логическое завершение: **Bitcoin** допускает возможность дробления до восьмого знака после запятой, что позволяет совершать транзакции на крайне небольшие суммы без комиссий.

Кроме того, для получателей средств указанные преимущества дополняются еще и тем, что платежи в рамках системы **Bitcoin** являются окончательными и неоспоримыми. Соответственно, если речь идет об интернет-магазине, то он не связан какими-либо процедурами, подобными **chargeback**, и комиссиями эквайера. Однако данные преимущества для добросовестного интернет-магазина в значительной степени компенсируются высокими колебаниями курса биткоина и неопределенностью его правового статуса.

Риски использования **Bitcoin** в целом сводятся к следующим <1>:

<1> С полным перечнем рисков, связанных с использованием виртуальных валют, подготовленным Управлением европейских банков (**European Banking Authority**), можно ознакомиться на сайте: EBA Opinion on Virtual Currencies. EBA/Op/2014/08, 4 July 2014. URL: <http://goo.gl/G1vc1h>.

1) высокая волатильность. Курс **Bitcoin** по отношению к основным валютам подвержен резким изменениям, что делает его малоприспособленным в качестве средства сбережения капитала и малопривлекательным для инвестирования <1>;

<1> Например, курс **Bitcoin** 2 октября 2013 г. составлял порядка 104 USD за один биткоин, а 4 декабря того же года он составил 1151 USD, а 21 февраля 2014 г. - 566 USD // <https://goo.gl/oe9UW4>.

2) риски мошенничества. То, что является преимуществом в одних случаях (например, анонимность), может являться недостатком в других: в условиях, когда личность контрагента неизвестна, существует вероятность неисполнения им своего встречного обязательства (поставки товара, оказания услуги, оплаты товара). Система **Bitcoin** не предлагает механизмов компенсации в таких случаях;

3) риски утраты **Bitcoin** вследствие кражи, мошенничества или иных непредвиденных обстоятельств. Несмотря на то что сама по себе сеть **Bitcoin** является весьма защищенной, кошельки конкретных пользователей по-прежнему являются уязвимыми. Утрата средств из кошелька по различным причинам (хакерская атака, потеря компьютера, неисправность жесткого диска) влечет утрату виртуальных единиц, сохраненных на нем;

4) отсутствие механизмов компенсаций на случай совершения ошибочных платежей, например, в случае ошибок в адресе (адресате) или размере платежа;

5) неясный правовой статус данного вида валюты: осуществление расчетов с ее использованием в отдельных странах может быть сопряжено с рядом рисков. Именно на данном аспекте хотелось бы сосредоточить дальнейшее внимание при рассмотрении вопросов использования криптовалюты **Bitcoin** для расчетов в сети Интернет.

Правовой статус **Bitcoin**

Феномен **Bitcoin** вызвал немалый интерес со стороны регуляторов и правоохранительных органов в значительной степени благодаря таким его качествам, как децентрализованный характер и анонимность.

Основные претензии со стороны государственных органов вызывает возможность использования данной валюты для совершения противоправных действий: финансирования терроризма; отмыwania средств, полученных преступным путем; приобретения изъятых из оборота товаров вроде наркотиков, оружия и т.п.

Еще в начале 2014 г. ЦБ РФ сделал заявление, согласно которому "в связи с анонимным характером деятельности по выпуску "виртуальных валют" неограниченным кругом субъектов и по их использованию для совершения операций граждане и юридические лица могут быть, в том числе непреднамеренно, вовлечены в противоправную деятельность, включая легализацию (отмывание) доходов, полученных преступным путем, и финансирование терроризма. Банк России предупреждает, что предоставление российскими юридическими лицами услуг по обмену "виртуальных валют" на рубли и иностранную валюту, а также на товары (работы, услуги) будет рассматриваться как потенциальная вовлеченность в осуществление сомнительных операций в соответствии с законодательством о противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма" <1>.

<1> Информация ЦБ РФ "Об использовании при совершении сделок "виртуальных валют", в частности, Биткойн" от 27 января 2014 г. URL: http://www.cbr.ru/press/pr.aspx?file=27012014_1825052.htm. Аналогичного мнения придерживается и Росфинмониторинг (см.: Информационное сообщение Росфинмониторинга "Об использовании криптовалют"

от 6 февраля 2014 г. URL: <http://www.fedsfm.ru/news/957>).

По мнению Генеральной прокуратуры РФ, "анонимные платежные системы и криптовалюты, в том числе наиболее известная из них - Биткойн, являются денежными суррогатами и не могут быть использованы гражданами и юридическими лицами" <1>. После появления этих разъяснений многие российские интернет-магазины и иные организации, которые до этого принимали **Bitcoin** к оплате, прекратили принимать эту криптовалюту, опасаясь возможного преследования.

<1> В Генеральной прокуратуре РФ 6 февраля 2014 г. состоялось совещание по вопросу правомерности использования анонимных платежных систем и криптовалют. URL: <http://genproc.gov.ru/smi/news/news-86432/>. Интересно, что Генеральная прокуратура так отмечает еще одну проблему **Bitcoin**, по-видимому, обуславливающую ее нелегитимный статус: "Более того, отличительной особенностью Биткойна как виртуального средства для взаиморасчетов и накопления является отсутствие обеспеченности реальной стоимостью. Цена на него определяется исключительно спекулятивными действиями, что влечет за собой высокий риск потери стоимости и, как следствие, нарушение прав держащих его граждан и организаций". Интересно было бы узнать, в каком российском законе закреплено право гражданина на отсутствие высокого риска потери стоимости при инвестициях в различного рода финансовые инструменты. Ведь если такого права нет, то говорить о нарушении в таком случае сложно. Еще

сложнее говорить о наличии каких-либо нарушений по данному основанию со стороны пользователей **Bitcoin** после значительного обвала курса российской валюты вследствие политики ЦБ РФ в конце 2014 - 2015 гг., принимая во внимание, что в силу **ч. 2 ст. 75** Конституции РФ "защита и обеспечение устойчивости рубля - основная функция Центрального банка Российской Федерации".

Уже существуют решения судов РФ, в которых данные идеи получают свое логическое развитие. Так, в решении Невьянского городского суда Свердловской области от 13 января 2015 г. отмечается, что "свободное распространение информации об электронной валюте обуславливает активное использование криптовалют в торговле наркотиками, оружием, поддельными документами и иной преступной деятельности. Данные факты, а также возможность бесконтрольного трансграничного перевода денежных средств и их последующего обналичивания служат предпосылками высокого риска потенциального вовлечения криптовалют в схемы, направленные на легализацию (отмывание) доходов, полученных преступным путем, и финансирование терроризма. Как следствие, данным решением в единый реестр запрещенных сайтов было включено 7 сайтов, связанных с тематикой биткойн, в том числе сайт bitcoin.org <1>.

<1> См.: решение Невьянского городского суда Свердловской области от 30 сентября 2014 г. по делу N 2-978/2014. URL: <http://bits.media/images/news/15.01.2015/bitcoin.pdf>. Как отмечается в литературе, данное решение было

отменено в мае 2015 г. Свердловским областным судом (см.: Сухаренко А. [Суррогаты вредные?](#) // ЭЖ-Юрист. 2015. N 41). К сожалению, текст решения не удалось найти в общедоступных источниках.

Данный случай не является единственным. В одном из недавних решений в реестр запрещенных сайтов по заявлению прокуратуры попал интернет-сайт одной из крупных виртуальных бирж - btc-e.com <1>. Учитывая, что подобного рода решения повышают показатели деятельности прокуратуры, а также общий настрой по отношению к **Bitcoin** со стороны российских правоохранительных органов, есть все основания считать, что реестр запрещенных сайтов и впредь будет пополняться за счет появления новых решений районных судов в различных регионах Российской Федерации.

<1> Решение приморского районного суда г. Санкт-Петербурга от 10 ноября 2015 г. по делу N 2-10750/2015.

Позиция российских государственных органов по отношению к **Bitcoin** может найти свое логическое развитие в случае реализации инициативы Минфина РФ по введению административной и уголовной ответственности за использование криптовалют в России, а также блокировке сайтов, распространяющих информацию и программное обеспечение, обеспечивающих возможность их использования <1>. Административная ответственность предусматривается за недобросовестную эмиссию, оборот и содействие распространению денежных суррогатов <2>. При этом под денежным суррогатом предлагается понимать

"выпускаемые (эмитируемые) на территории Российской Федерации объекты имущественных прав, в том числе в электронном виде, предназначенные для использования в качестве средства платежа и (или) обмена и непосредственно не предусмотренные в качестве официального средства платежа законодательством Российской Федерации". Данная дефиниция сопровождается рядом изъятий. Не признаются денежными суррогатами, в частности, электронные деньги, обращение которых осуществляется в соответствии с [Законом](#) об НПС, законодательством стран СНГ, Евросоюза и Великобритании (sic!); внутриигровая валюта в многопользовательских компьютерных играх и ряд других объектов. Примечательно, что в приведенной дефиниции прямо указано, что денежный суррогат, к которому, очевидно, относится **Bitcoin**, является "объектом имущественных прав", что может быть истолковано как признание его также объектом гражданских прав, а, следовательно, признание оборотоспособности такого объекта, что входит в явное противоречие с установлением административной ответственности за введение его в оборот. Кроме того, данная дефиниция никак не затрагивает инвестиционную функцию **Bitcoin**. Исходя из существующих формулировок можно сделать вывод, что инвестирование в данный объект и его хранение не являются наказуемыми деяниями. Вполне возможно, что дефиниция претерпит ряд трансформаций, но, по-видимому, можно ожидать того, что в какой-то форме ограничения на оборот **Bitcoin** могут быть введены в рамках [КоАП](#), поскольку вряд ли существующий в современной России законодательный процесс способствует глубокому анализу столь объемных документов.

<1> См.: Шадрина Т. За использование криптовалюты в России будут уголовно наказывать // Российская газета. 23 сентября 2015 г. URL: <http://www.rg.ru/2015/09/25/kriptovaluta-site-anons.html>. См. также: Сухаренко А. [Указ. соч.](#)

<2> См. [ст. ст. 30.38 - 30.40](#) проекта нового Кодекса об административных правонарушениях. URL: http://static.consultant.ru/obj/file/doc/codexadm_291015.pdf.

За введение ответственности, в том числе уголовной, за операции с **Bitcoin** выступил и глава Следственного комитета РФ Александр Бастрыкин, который, повторяя аргументы, ранее высказанные Генеральной прокуратурой РФ, добавил, что "о необходимости запрета подобного рода платежных средств указано и в рекомендациях, подготовленных по итогам экстренной встречи министров юстиции стран ЕС, прошедшей в ноябре прошлого года в Брюсселе. Встреча прошла после терактов во Франции" <1>. В связи с этим, прежде чем перейти к рассмотрению высказанных аргументов за введение уголовной ответственности за использование Bitcoin, следует сразу прояснить следующее: нигде в итоговых резолюциях и рекомендациях чиновников ЕС, на которые ссылается глава СК РФ, не говорится о необходимости запрета криптовалют, в них отмечается лишь необходимость усиления контроля над небанковскими платежными системами, в том числе криптовалютами <2>. Оставим столь вольную интерпретацию данных положений на совести чиновника.

<1> Козлова Н. Глава СК предложил ужесточить

ответственность за валютные спекуляции // Российская газета. 2016. 14 января. URL: <http://www.rg.ru/2016/01/14/sk-site.html>.

<2> См. п. 8 Conclusions of the Council of the EU and of the Member States meeting within the Council on Counter-Terrorism, European Council. 20 November 2015 (URL: <http://goo.gl/Rtqlgz>): "...to strengthen controls of non-banking payment methods such as electronic/anonymous payments, money remittances, cash-carriers, virtual currencies, transfers of gold or precious metals and pre-paid cards in line with the risk they present and to curb more effectively the illicit trade in cultural goods".

В целом, безусловно, нельзя отрицать факт использования **Bitcoin** для осуществления отдельных видов запрещенной деятельности. Существуют определенные интернет-площадки, торгующие нелегальными товарами (крадеными реквизитами банковских карт, фальшивыми деньгами, детской порнографией, персональными данными, запрещенными психоактивными веществами), на которых осуществляются расчеты с использованием **Bitcoin**, наиболее известной из которых до недавнего времени был **Silk Road** (в пер. с англ. - "Шелковый путь") <1>. Но для приобретения нелегальных товаров намного шире используется также вполне легальная валюта, что не является основанием для ее запрещения.

<1> Данная площадка была закрыта в октябре 2013 г. в результате расследования ФБР; ее основатель, Росс Ульбрихт (Ross Ulbricht), был

арестован. Интересно, что количество положительных отзывов о ней составляло 97,8%, т.е. подавляющее большинство всех заключенных на ней сделок исполнялось надлежащим образом.

Кроме того, есть основания предполагать, что существует возможность использования **Bitcoin** для легализации денежных средств, полученных преступным путем, и финансирования терроризма. Но и тут тоже необходимо реалистично смотреть на вещи. Как показывает отчет Министерства финансов Великобритании, данный риск является достаточно низким в силу невысокого уровня хождения **Bitcoin**, но в то же время он вполне схож с теми рисками, которые характерны для использования наличных денежных средств и электронных денег <1>. Наконец, по заявлению Европейского центрального банка, криптовалюты и **Bitcoin**, в частности, не несут рисков для устойчивости банковской и финансовой системы <2>. Таким образом, можно говорить о том, что в настоящее время отсутствуют достаточные, документально подтвержденные основания для установления уголовной или административной ответственности за совершение транзакций с **Bitcoin**.

<1> UK National Risk Assessment of Money Laundering and Terrorist Financing. October 2015. URL: <https://goo.gl/h55C1t>.

<2> Virtual Currency Schemes. ECB Report. October 2012. P. 39, 42. URL: <https://goo.gl/TKIFap>.

В связи с вышеизложенным неудивительно, что запретительный регулятивный подход по отношению к

Bitcoin в настоящее время является скорее исключением и не практикуется практически нигде, даже в Китае и Таиланде, которые обычно приводятся в качестве примеров как страны, где якобы запрещены операции с **Bitcoin**.

В Китае запрет на операции с **Bitcoin** касается лишь финансовых учреждений. Такие учреждения не могут устанавливать цены в **Bitcoin**; использовать его в качестве платежного инструмента; осуществлять конвертацию **Bitcoin** в иные валюты и наоборот; предоставлять страховые продукты, связанные с **Bitcoin**; использовать **Bitcoin** в качестве средства инвестирования или создания фондов и т.д. Совершение транзакций частными лицами не запрещено, такие лица несут все связанные с ними риски самостоятельно <1>.

<1> The People's Bank of China and Five Associated Ministries Notice: "Prevention of Risks Associated with Bitcoin". Bank Notice. 3 December 2013 N 289. URL: <https://exchange.btcc.com/page/bocnotice2013>.

Что же касается Таиланда, то слухи о запрете **Bitcoin**, распространяемые в сети Интернет, были вызваны отказом Центрального банка Таиланда в выдаче лицензии одной из компаний, специализирующихся на транзакциях в данной валюте. Однако сам Центральный банк Таиланда никогда не делал заявлений о незаконности такого рода операций <1>. Примечательно, что в обеих странах успешно функционируют крупные виртуальные биржи, осуществляющие обмен **Bitcoin** на иные виды валют, и наоборот. В соответствии с рядом исследований ни в одной юрисдикции **Bitcoin** не признан незаконным

объектом как таковым <2>.

<1> Buntinx JP. The Legal Status of Bitcoin in Thailand // The Merkle. 31 December 2015. URL: <http://themerke.com/news/legal-status-bitcoin-thailand>.

<2> См., например: Bryans D. Bitcoin and Money Laundering: Mining for an Effective Solution // Indiana Law Journal Vol. 89, 2014. P. 455; Turpin J. Bitcoin: The Economic Case for a Global Virtual Currency Operating in an Unexplored Legal Framework // Indiana Journal of Global Legal Studies. Vol. 21.2014. P. 368.

Позиция большинства стран по поводу использования **Bitcoin** носит осторожный характер. Как правило, уполномоченные органы власти ограничиваются информационными сообщениями, адресованными участникам оборота, с предостережениями о рисках, связанных с использованием данного платежного инструмента <1>. Но ни в одной относительно цивилизованной стране пока не задумаются о введении уголовной ответственности за совершение операций с криптовалютами и уж тем более об ограничении доступа к информации о них. В этой связи сложно не согласиться с мнением, высказанным Германом Грефом на форуме в Давосе: "Криптовалюты - это очень интересный международный эксперимент, который ломает парадигму валютной эмиссии. И их определенно не стоит запрещать, но следует попытаться понять, изучить и, возможно, начать правильно регулировать" <2>. Поэтому целесообразно обратиться к опыту зарубежных стран, которые уже предпринимают попытки регулирования отношений, связанных с использованием **Bitcoin**.

<1> Virtual Currency Schemes: Further Analysis.
ECB Report. February 2015. P. 30. URL:
<https://goo.gl/UExD0p>.

<2> Герман Греф о криптовалютах в Давосе. URL:
<http://newmoneyfeed.com/news/german-gref-o-kriptovalyuta-h-v-davose>.

Достаточно важной вехой по пути признания **Bitcoin** легитимным объектом гражданского оборота в Европе стало решение Европейского суда справедливости, в соответствии с которым **Bitcoin** был приравнен к валюте для целей налогообложения налогом на добавленную стоимость <1>. Поскольку налоговые органы отдельных стран ЕС по-разному подходили к налогообложению транзакций, связанных с обменом **Bitcoin** на национальную валюту, и наоборот, перед Судом был поставлен вопрос: подлежат ли такого рода сделки обложению налогом на добавленную стоимость или нет <2>? Европейский суд постановил, что такие транзакции освобождены от НДС, поскольку **Bitcoin** является не обычным товаром, а средством платежа (**currency**). Как следствие, транзакции с **Bitcoin** были отнесены к платежным операциям, осуществляемым с валютами, монетами и банкнотами, которые не подлежат обложению НДС. Суд сослался на позицию Генерального адвоката, согласно которой "виртуальная валюта не имеет другого назначения, кроме как быть средством платежа". Конечно, здесь имеет место некоторое упрощение ситуации со стороны Суда: **Bitcoin** может использоваться и в иных качествах, например, в качестве средства инвестирования или способа приобщения к

определенной субкультуре. Но, несмотря на это основной посыл, решения Суда прослеживается достаточно определенно: операции с **Bitcoin** не являются разновидностью незаконных операций, и **Bitcoin** представляет собой вполне легальный актив, который по своему правовому статусу эквивалентен договорным средствам платежа (то есть таким объектом, который стороны соглашения договорились принимать в качестве средства платежа по своему договору).

<1> Skatteverket v. David Hedqvist, ECJ, 20 October 2015, C-264/14.

<2> В соответствии со [ст. 135 \(1\)\(e\)](#) Директивы ЕС 2006/112/ЕС об общей системе налогообложения налогом на добавленную стоимость, страны - члены ЕС освобождают от НДС транзакции, связанные с валютой, банкнотами и монетами, выступающими законными средствами платежа (**legal tender**), за исключением коллекционных их видов, которые обычно не выступают в качестве законного средства платежа, а также монет, представляющих нумизматический интерес. В связи с ней возник вопрос: требуется ли наличие статуса законного платежного средства у соответствующего платежного инструмента, чтобы применить данное исключение? По мнению Генерального адвоката, чья позиция легла в основу решения Суда, поскольку формулировка данного [пункта](#) до - пускает различные толкования на разных языках государств - членов ЕС, целесообразно использовать телеологическое толкование. В связи с тем что основная цель введения данного положения состояла в том, чтобы не наносить ущерба конвертируемости различных средств платежа, а **Bitcoin** выполняет именно эту функцию, то и на него

должно распространяться указанное исключение. См.: Opinion of Advocate General Kokott delivered on 16 July 2015. Skatteverket v. David Hedqvist. p. 29, 32 // <http://goo.gl/W0aZpv>.

В США в настоящее время правовой статус **Bitcoin** также приобретает более-менее четкие очертания, что во многом предопределяется налоговыми соображениями. Так, по мнению Федеральной налоговой службы CIF (**Internal Revenue Service**), **Bitcoin** представляет собой имущество (**property**), а не валюту и подлежит соответствующему налогообложению <1>. Например, если лицо приобрело 1 биткойн за 600 долл., впоследствии он вырос в цене до 1000 долл. и за данный биткойн был приобретен товар стоимостью 1000 долл., то плательщик должен заплатить налог с 400 долл., которые составляют его доход от прироста капитала (положительная разница между ценой продажи капитального актива и ценой его покупки, возникшая в результате роста рыночной стоимости актива). С точки зрения налоговой службы США, даже несмотря на то, что **Bitcoin** нередко выполняет в реальной жизни те же функции, что и деньги, он не является валютой <2>, поскольку не является законным платежным средством ни в одной юрисдикции. По своей природе **Bitcoin** скорее ближе к акциям: по мере того, как их стоимость варьируется в положительную сторону, их владелец должен платить налог на доход от прироста капитала. В отличие от европейского подхода, позиция налоговой службы США фактически превращает выгоду от каждой транзакции, совершенной с использованием **Bitcoin**, в объект налогообложения, требующий тщательных подсчетов и сохранения данных о времени приобретения **Bitcoin** и его рыночной цене на тот момент.

<1> IRS Notice 2014-21, 25 March 2014. URL:
<https://www.irs.gov/pub/irs-drop/n-14-21.pdf>.

<2> Следует отметить, что в литературе иногда ссылаются на решение суда штата Техас по делу **SEC v. Shavers & Bitcoin Savings and Trust**. N 4:13-CV-416. 18 September 2014 (E.D. Tex), в котором суд использовал термин **currency (валюта)** применительно к **Bitcoin**. Однако данное дело касалось обвинений в незаконном присвоении имущества, в связи с чем упоминание этого термина носило эпизодический характер и не сопровождалось каким-либо анализом правовой природы **Bitcoin**. Поэтому указанное дело не диссонирует с общим подходом регуляторов США к криптовалютам.

Взгляд на **Bitcoin** как на товар особого рода разделяет и Комиссия США по срочной биржевой торговле (**Commodity Futures Trading Commission**), по мнению которой **Bitcoin** представляет собой биржевой товар (**commodity**), в силу чего опционы на приобретение или продажу **Bitcoin**, размещенные на специализированных площадках, должны соответствовать требованиям законодательства США о биржевой торговле <1>.

<1> CFTC Orders Bitcoin Options Trading Platform Operator and its CEO to Cease Illegally Offering Bitcoin Options and to Cease Operating a Facility for Trading or Processing of Swaps without Registering. 17 September 2015. URL:
<http://www.cftc.gov/PressRoom/PressReleases/pr7231-15>.

К числу сторонников взгляда на **Bitcoin** как на биржевой товар инвестиционно-спекуляционной направленности относятся власти Гонконга. Regulation of Trading Activities of Bitcoins. LCQ4. 25 March 2015. URL: <http://goo.gl/pTIN3U>.

Как видно, ЕС и США придерживаются разных взглядов на природу **Bitcoin**: первый делает акцент на его платежной функции, в то время как вторые - на инвестиционной. Представляется, что данная ситуация является следствием того, что **Bitcoin** может использоваться в обеих ипостасях. В конечном счете, как представляется, основной вопрос, обуславливающий выбор между описанными подходами, сводится к выбору государства между возможностью подвергать тщательному анализу и контролю каждую транзакцию с **Bitcoin** и возможностью установить общие рамочные требования.

Но в любом случае не следует забывать: желания должны быть соразмерны возможностям, что в контексте рассматриваемой проблематики означает необходимость учета специфики процессов эмиссии и расчетов с использованием **Bitcoin**.

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 обуславливает 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.

<1> Наиболее известными биржами является **Bitstamp**, **1Bse.com**, **BTCChina**. До 2014 г. самой известной и крупной биржей была Mt.gox. Однако в конце февраля 2014 г. эта биржа была закрыта в связи с тем, что с ее счетов несанкционированно вывели средства пользователей и владельцев биржи в сумме около 700 тыс. биткоинов, что по курсу на тот момент составляло порядка 350 млн. долл. США.

Примечательно, что существующие законодательные инициативы по регулированию виртуальных валют концентрируются именно на виртуальных биржах. Одним из пионеров в области специального регулирования виртуальных бирж является штат Нью-Йорк, где 8 августа 2015 г. вступил в силу специальный закон, получивший на практике

наименование **BitLicense**. Данный закон на момент подготовки настоящей книги является единственным в своем роде, предусматривая лицензирование коммерческой деятельности в сфере виртуальных валют (**Virtual Currency Business Activity**), осуществляемой на территории штата Нью-Йорк или с участием резидента данного штата. Указанная деятельность включает в себя, в частности, хранение и управление виртуальной валютой в интересах иных лиц, предоставление услуг обмена виртуальной валюты на фиатные деньги или иные виды виртуальной валюты, и наоборот, администрирование и эмиссию виртуальной валюты для целей последующей передачи. Под лицензируемый вид деятельности не подпадает разработка и распространение программного обеспечения, необходимого для функционирования виртуальных валют, а также деятельность потребителей и интернет-магазинов, связанная с использованием виртуальных валют в качестве средства платежа или инвестирования. Рассматриваемый закон устанавливает требования к капиталу, порядку ведения отчетности, проведения контроля и надзора над за их деятельностью виртуальных бирж. Кроме того, на виртуальные биржи возложена обязанность реализовывать программу противодействия легализации денежных средств, полученных преступным путем, и программу кибербезопасности с детализацией мер, которые необходимо принять <1>.

<1> См.: New York Codes, Rules and Regulations, Title 23. Part 200 "Virtual Currencies". URL: <http://goo.gl/He4ml5>.

К числу стран, которые планируют в ближайшее

время ввести специальное регулирование виртуальных бирж с целью обязания их соблюдать требования законодательства о противодействии легализации доходов, полученных преступным путем, относятся Сингапур <1>, Великобритания <2>, а также остров Джерси <3>. Как видно, многие страны предпринимают попытки регулирования деятельности по использованию **Bitcoin** и иных видов виртуальных валют, а не идут по пути ее запрета, причем субъектами регулирования являются не обычные пользователи и даже не интернет-магазины, принимающие **Bitcoin** к оплате, а профессиональные участники виртуального рынка.

<1> Monetary Authority of Singapore to Regulate Virtual Currency Intermediaries for Money Laundering and Terrorist Financing Risks. 13 March 2014. URL: <http://goo.gl/9LsZgX>.

<2> Digital Currencies: Response to the Call for Information. HM Treasury. March 2015. URL: <https://goo.gl/xNnpdm>.

<3> Regulation of Virtual Currency. Consultation. Chief Minister's Department. States of Jersey. 9 July 2015. URL: <http://goo.gl/PJWkHE>.

Насколько эффективным будет данное регулирование, покажет время, но представляется, что это наиболее удачная отправная точка для формирования правового поля в отношении виртуальных валют. Конечно, сохраняется возможность обмена биткоинов на реальные деньги и минуя виртуальные биржи, например, путем совершения обменов между частными лицами <1>. Даже несмотря на то, что многие продвинутые пользователи и хакеры

смогут обойти установленные запреты 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.

<1> Существуют специальные сайты, которые помогают таким лицам найти друг друга, например: **Bitcoin.local**.

В завершение необходимо рассмотреть вопрос о правовом статусе **Bitcoin** сквозь призму гражданского права, поскольку большая часть изложенных выше мнений и позиций государственных органов различных стран в отношении виртуальной валюты на данном этапе касается все же публично-правовой составляющей (налогообложение; законодательство о противодействии легализации денежных средств, полученных преступным путем; законодательство о биржевой торговле и т.п.).

Первое, что можно сказать с достаточной степенью определенности, это что **Bitcoin**, как и любая

иная виртуальная валюта, в Российской Федерации не является ни деньгами, ни законным платежным средством. В соответствии со [ст. 29](#) Федерального закона от 10 июня 2002 г. N 86-ФЗ "О Центральном банке Российской Федерации (Банке России)" (далее - Закон о Банке России) банкноты и монеты Банка России являются 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. Но в любом случае **Bitcoin** не удовлетворяет ни одному из указанных критериев. Как следствие, кредитора по денежному обязательству нельзя обязать принять платеж, произведенный посредством данной "валюты", если только он сам не выразил своей воли на принятие **Bitcoin** в уплату долга. Таким образом, платежи посредством **Bitcoin** не могут погашать денежное обязательство по умолчанию. Кроме того, никто не может быть принужден к принятию **Bitcoin** по его нарицательной стоимости, поскольку у него ее просто нет.

Нельзя относить **Bitcoin** и к разновидности имущественного права, в качестве которого по общему правилу можно рассматривать безналичные денежные средства и электронные деньги по [Закону](#) об НПС. Ведь в данном случае отсутствуют какие-либо договорные отношения с оператором (эмитентом) электронных денег по причине отсутствия одного. Кроме того, **Bitcoin** не может рассматриваться в качестве электронных денежных средств, как это определено в [Законе](#) об НПС, по причине отсутствия признака "предоплаченности", поскольку эмиссия **Bitcoin** осуществляется самими пользователями на основе криптографических алгоритмов <1>.

<1> Здесь следует сделать важную ремарку. Поскольку криптовалюта **Bitcoin**, а также лежащая в ее основе технология **Blockchain** неразрывно связаны с шифрованием, их использование может требовать получения лицензии ФСБ на использование криптографических средств в информационных системах. См.: [Постановление](#) Правительства РФ от 16 апреля 2012 г. N 313 "Об утверждении Положения о лицензировании 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)".

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 обменяны 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, подобный договор нельзя будет рассматривать по российскому праву как договор мены, поскольку квалифицирующим признаком последнего является обмен одного товара на другой, что обуславливает необходимость наличия перехода права собственности по нему <1>. Представляется, что такой договор является смешанным с элементами соответствующего договора, опосредующего предоставление товара, работы или услуги, а также элемента непоименованного договора, опосредующего передачу биткоинов в качестве оплаты <2>.

<1> Так, ВАС РФ не квалифицирует в качестве мены договор, по которому осуществляется обмен товара на услуги или на имущественное право. См. п. п. 1 и 3 информационного письма Президиума ВАС РФ от 24 сентября 2002 г. N 69 "Обзор практики разрешения споров, связанных с договором мены", рассматривая такие договоры в качестве смешанных.

<2> 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. N 4.

В заключение необходимо отметить, что социально-экономическое значение виртуальной

валюты **Bitcoin** не стоит недооценивать. 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** <1>. А "сердце" технологии **Bitcoin** - **блокчейн** - имеет все шансы стать основной для ряда новых решений, ведь в своей основе это ничто иное, как технология распределенного хранения и доступа к данным, синхронизированная между различными участниками.

<1> 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. N 41. 2008. Известный пиратский торрент-трекер **Pirate Bay** успешно существует более пяти лет, несмотря на многочисленные попытки его закрытия.

В частности, **блокчейн** может стать основной для Интернета вещей, традиционная модель которого предполагает наличие централизованного пункта обработки данных, собранных подключенными устройствами, что обуславливает существенные издержки, в значительной степени сдерживающие развитие данной технологии. Например, компания, которая производит "умные" телевизоры, должна

поддерживать необходимую инфраструктуру обработки поступающих с него данных в среднем в течение 20 лет, в то время как прибыль от его продажи она получает один раз - при продаже такого телевизора. Все это на настоящий момент ограничивает возможности применения данных технологий премиум-сегментами. Если же организовать работу устройств по принципам **блокчейна**, то это позволит решить указанную проблему. Каждое устройство сможет пользоваться для коммуникации с другими устройствами публичной распределенной инфраструктурой подобно тому, как это сейчас имеет место с **Bitcoin** <1>.

<1> IBM в настоящее время уже разрабатывает технологию, основанную на принципах **блокчейна**, применительно к Интернету вещей. См.: IBM: Биткоин-технология станет основной Интернета вещей // Bitnovosti. 15 сентября 2014 г. URL: <http://bitnovosti.com/2014/09/15/ibm-bitcoin-osnova-iot/>.

Компания **Visa** также заявила о ценности технологии **блокчейна** для улучшения существующих платежных систем, указав, что "блокчейн более не является вопросом выбора" <1>.

<1>
<http://vision.visaeurope.com/why-2015-was-the-year-for-payments/>

Как видно, у **Bitcoin** и технологий, лежащих в его основе, огромный потенциал, который крайне важно не загубить импульсивными законодательными мерами рестриктивного характера. В противном случае есть все

шансы проиграть конкурентную борьбу с другими странами на инновационно-технологическом рынке, а свой собственный загнать в тень. Причем в конечном счете такое законодательство все равно долго "не устоит" в борьбе с технологией. Для иллюстрации перспектив подобного рода борьбы как никогда уместно привести известное изречение Махатмы Ганди: "Сначала они тебя не замечают, потом смеются над тобой, затем борются с тобой. А потом ты побеждаешь". В конце концов будущее будет за тем регулированием, которое признает будущее за **Bitcoin**, а точнее - за стоящими за ним технологиями.

Глава 8. РЕКЛАМА В СФЕРЕ ЭЛЕКТРОННОЙ КОММЕРЦИИ

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 и доступности различного рода информации в Интернете 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>.

<1> Юрасов А.В. Указ. соч. С. 279.

В данной главе нас будут интересовать главным образом правовые аспекты интернет-рекламы, которую в зависимости от задействованных "носителей" 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. Кроме того, необходимо будет обозначить некоторые способы привлечения внимания к товару или продавцу, которые в ряде случаев, хотя и не являются "рекламой" в юридическом смысле, стали важным средством формирования интереса потребителей к интернет-экономике, а в случае с бизнес-моделями нового поколения, основанными на "экономике совместного использования", - одним из ключевых факторов, обеспечивающих их функционирование. Речь идет о так называемых рекомендациях или отзывах о товаре, продавце или сервисе, которые оставляют пользователи и на основе которых другие пользователи принимают решения о приобретении товара или отказе от его приобретения.

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;

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>;

<1> Кузнецов Р.В. Маркетинговые исследования баннерной интернет-рекламы: Дис. ... канд. экон. наук. М., 2008. С. 15 - 16.

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 или иное устройство, используемое для доступа к сети Интернет);

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 <1>.

<1> Это особенно справедливо в свете

существующих исследований, согласно которым около 60% пользователей ограничиваются лишь первой страницей, выдаваемой 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. Информация, размещенная на веб-сайте, и законодательство Российской Федерации о рекламе

Прежде чем перейти к анализу 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 какие последствия влечет положительный ответ на этот вопрос.

Основным и единственным нормативным актом в данной сфере является [Закон](#) о рекламе. Субъекты Российской Федерации не вправе принимать нормативные правовые акты по вопросам

регулирования рекламы, в том числе в Интернете (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>.

<1> Письмо ФАС России от 3 августа 2012 г. N АК/24981 "О рекламе алкогольной продукции в Интернете и печатных СМИ".

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.

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>, и специальных разъяснений ФАС РФ по вопросам применения законодательства о рекламе в сети Интернет <2>.

<1> Сеть Интернет относится к средствам электросвязи. См. [п. 2](#) письма ФАС России от 19 мая 2006 г. N АК/7654 "Об особенностях отдельных способов распространения рекламы".

<2> См., например: [письмо](#) ФАС России от 28 августа 2015 г. N АК/45828/15 "О рекламе в сети Интернет".

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 <1>. 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 <2>. 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 сайта 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 <3>. В таком случае вполне можно говорить о том, что получатель такой информации является заранее определенным лицом и ее распространение 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 <4>.

<1> Постатейный **комментарий** к Федеральному закону "О рекламе" / Д.С. Бадалов, И.И. Василенкова, Н.Н. Карташов и др. М., 2012. Комментарий к ст. 3.

<2> См.: [письмо](#) ФАС России от 5 апреля 2007 г. N АЦ/4624.

<3> См., например: [Постановление](#) Девятнадцатого арбитражного апелляционного суда от 5 марта 2011 г. по делу N А14-7904/2010/227/10, где говорится: "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 клиники является любой пользователь сети Интернет. Таким образом, информация на сайте Интернета направлена неопределенному кругу лиц".

<4> См., например: [Постановление](#) ФАС Западно-Сибирского округа от 17 мая 1999 г. N Ф04/945-188/А75-99.

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 привлечение внимания, формирование интереса к какому-либо объекту рекламирования, его продвижение на рынке. В соответствии с судебной практикой привлечение внимания представляет собой процесс обращения органов восприятия потребителя непосредственно на прием информации о товаре (с помощью яркости, красочности, звукового оформления, неординарности дизайна или текста). Формирование (поддержание) интереса - это целенаправленное

действие, которое порождает (делает устойчивым) у потребителя ощущение необходимости рекламируемого товара, побуждает его приобрести объект рекламирования. Продвижение товара - это эффект, которого старается добиться рекламодатель, выражающийся в образовании высокого спроса на товар и больших объемов продаж <1>.

<1> **Постановление** ФАС Московского округа от 5 августа 2009 г. по делу N A41-5137/08.

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, поскольку реклама представляет собой искусственное вмешательство в поведение человека извне с целью побуждения его к приобретению определенного товара (услуги) или формирования у него позитивного восприятия определенного предпринимателя. Эффективность рекламы напрямую связана со степенью эксплуатации психологических особенностей человека и присущих ему когнитивных искажений (**cognitive bias**), в связи с чем законодательные требования направлены на минимизацию манипулятивных факторов рекламы и обеспечение определенного уровня добросовестности при ее разработке и распространении <1>. Потребительские решения должны приниматься,

насколько это возможно, без недолжного влияния недобросовестных методов маркетинга. Среди общих законодательных требований, предъявляемых к рекламе, имеющих непосредственное отношение и к рекламе в сети Интернет, следует особо выделить следующие:

<1> Об используемых в рекламе манипулятивных практиках см. подробнее: Фельсер Г. Психология потребителей и реклама / Пер. с нем. Харьков, 2009. В соответствии с циничным, но метким утверждением одного из руководителей **General Motors**, реклама представляет собой инструмент "организованного создания чувства неудовлетворенности". См.: Skidelsky R., Skidelsky E. How Much Money Is Enough? N.Y.: Other Press. 2012. P. 56.

1) реклама 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, касающиеся 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 <1>. Таким образом, российское законодательство не запрещает сравнительной рекламы, но она определенно находится к зоне риска.

Некорректное сравнение с товарами (деятельностью) конкурентов может повлечь негативные последствия не только в сфере законодательства о рекламе, но и в рамках антимонопольного законодательства <2>. В соответствии со [ст. 14.3](#) Федерального закона "О защите конкуренции" не допускается недобросовестная конкуренция путем некорректного сравнения хозяйствующего субъекта и (или) его товара с другим хозяйствующим субъектом-конкурентом и (или) его товаром, в том числе путем использования слов "лучший", "первый", "номер один", "самый", "только", "единственный", иных слов или обозначений, создающих впечатление о превосходстве товара и (или) хозяйствующего субъекта, без указания конкретных характеристик или параметров сравнения, имеющих объективное подтверждение, либо в случае, если утверждения, содержащие указанные слова, являются ложными, неточными или искаженными. Кроме того, запрещено сравнение с другим хозяйствующим субъектом-конкурентом и (или) его товаром, основанное исключительно на незначительных или несопоставимых фактах и содержащее негативную оценку деятельности хозяйствующего субъекта-конкурента и (или) его товара;

<1> Постановление Пленума ВАС РФ от 8 октября 2012 г. N 58 "О некоторых вопросах практики применения арбитражными судами Федерального закона "О рекламе" ([п. 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](#) ФАС Поволжского округа от 6 мая 2011 г. по делу N A55-18530/2010; реклама BMWX5, 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 N 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. N 18АП-5539/2013 по делу N А76-20663/2012. Контекстная реклама, содержащая фразу "крупнейший игрок на рынке", была также признана ненадлежащей, поскольку "отсутствует указание на конкретный критерий, по которому возможно осуществить такое сравнение и который может быть подтвержден или опровергнут объективными данными". См.: решение Арбитражного суда Новосибирской области от 7 ноября 2015 г. по делу N А45-13590/2015. Аналогичным образом была квалифицирована фраза "Пластиковые окна Алькор - лучшие!". См.: решение Арбитражного суда Челябинской области от 17 августа 2015 г. по делу N А76-15385/2015.

<2> Вопрос о соотношении законодательства о рекламе и антимонопольного законодательства применительно к актам недобросовестной конкуренции является достаточно сложным и будет подробнее рассмотрен далее.

2) реклама должна соответствовать требованиям законодательства РФ 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. и Протоколом к нему), 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;

<1> [Определение](#) ВАС РФ от 18 февраля 2013 г. N ВАС-1040/13 по делу N 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 N А40-143417/10-153-966).

<2> [Постановление](#) Одиннадцатого арбитражного апелляционного суда от 23 августа 2012 г. по делу N А65-14800/2012.

<3> См. [ч. 3 ст. 3](#) Федерального закона от 1 июня 2005 г. N 53-ФЗ "О государственном языке Российской Федерации". См., например: [Постановление](#)

Тринадцатого арбитражного апелляционного суда от 31 августа 2011 г. по делу N A56-7201/2011.

3) реклама должна 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 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, такая реклама носит эротический характер и ограничивает потенциального потребителя рекламы в возможности ее игнорировать" <1>;

<1> **Постановление** Восьмого арбитражного апелляционного суда от 30 сентября 2011 г. по делу N A46-6175/2011.

4) реклама должна 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). Данная норма корреспондирует с положениями ст. 10 Закона о защите прав потребителей об обязанности продавца (изготовителя, исполнителя) предоставить необходимую и достоверную информацию о товарах (работах, услугах), обеспечивающую возможность их правильного выбора. Соответственно, предоставление недостоверной или вводящей в заблуждение информации о товаре, условиях его приобретения или использования может одновременно рассматриваться и в качестве ненадлежащей рекламы, и в качестве нарушения права потребителя на получение необходимой и достоверной информации (ч. 1 ст. 14.8 КоАП РФ);

5) использование в рекламе товарных знаков третьих лиц должно сопровождаться их согласием. Данное требование не содержится в [Законе](#) о рекламе и было выработано судебной практикой <1>. То же самое справедливо и в отношении использования в рекламе на веб-сайте иных объектов интеллектуальной собственности, принадлежащих третьим лицам. В частности, персонажей из известных мультфильмов <2>. Для полноты картины следует отметить, что судебное правотворчество на этом не остановилось и согласно недавнему решению Верховного Суда РФ простое размещение на сайте интернет-магазина фотографий товаров конкурентов, маркированных их товарными знаками, даже при отсутствии таких товаров в фактическом ассортименте интернет-магазина, может рассматриваться как недобросовестная конкуренция <3>;

<1> См.: [Постановление](#) ФАС Московского округа

от 5 августа 2009 г. по делу N А41-5137/08, которое устанавливает, что "обычаями делового оборота не принято использование для рекламы (продвижения) своей продукции товарных знаков, принадлежащих иным лицам, без согласия последних, учитывая коммерческий характер рекламных роликов, создаваемых с целью формирования или поддержания интереса к товару и его продвижению на рынке, использование в рекламе товарных знаков или изображений сходных до степени смешения, принадлежащих другим правообладателям, которые никаким образом не участвуют в создании рекламного ролика и не имеют отношения к рекламируемому товару, должно производиться только с их согласия".

<2> См.: [Постановление](#) Суда по интеллектуальным правам от 22 апреля 2016 г. N С01-243/2016 по делу N А63-8204/2015, в котором Суд, оставляя в силе [Постановление](#) УФАС о привлечении общества к административной ответственности, указал, что "вмененное обществу правонарушение ([пункт 4 части 2 статьи 5](#) и [часть 11 статьи 5](#) Закона о рекламе) выразилось в распространении рекламы, которая является актом недобросовестной конкуренции в соответствии с антимонопольным законодательством (незаконное использование образа персонажей мультфильма "Madagascar")".

<3> [Определение](#) Верховного Суда РФ от 9 декабря 2015 г. по делам N 304-КГ15-8874, А67-4453/2014.

6) стоимостные параметры рекламы должны быть выражены в рублях и лишь в качестве дополнения - в иной валюте ([ч. 7.1 ст. 5](#) Закона о рекламе);

7) реклама должна 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);

8) реклама должна соответствовать требованиям, установленным к рекламе отдельных видов товаров (услуг), указанным в [гл. 3](#) Закона о рекламе (например, лекарственных средств, медицинских услуг, БАДов, финансовых услуг, основанных на риске игр и пари). При этом необходимо иметь в виду, что некоторые виды товаров в принципе не могут выступать объектом рекламы, в том числе в сети Интернет. К таким товарам относятся табак, табачная продукция, табачные изделия и курительные принадлежности (включая кальян, зажигалки и т.п.); товары, подлежащие обязательной сертификации или подтверждению соответствия требованиям технических регламентов <1> в отсутствие такой сертификации (подтверждения соответствия); взрывчатых веществ (кроме пиротехнической продукции); наркотических веществ; объектов, изъятых из оборота;

<1> О понятии и процедурах сертификации и обязательном подтверждении соответствия см.:

Федеральный закон от 27 декабря 2002 г. N 184-ФЗ "О техническом регулировании".

9) при дистанционной купле-продаже товаров реклама должна содержать сведения о наименовании, месте нахождения и государственном регистрационном номере записи о создании юридического лица; Ф.И.О., ОГРН записи о государственной регистрации физического лица в качестве индивидуального предпринимателя (ст. 8 Закона о рекламе). Следует отметить, что данное правило формально применимо лишь к дистанционной купле-продаже товаров, но не к рекламе услуг. Однако предоставление подобного рода сведений все же необходимо и в данном случае в соответствии со ст. 9 Закона о защите прав потребителей, регламентирующей объем и порядок предоставления потребителю информации об изготовителе, продавце и исполнителе;

10) при распространении посредством сети Интернет информационной продукции необходимо также учитывать положения ч. 10.1 ст. 5 Закона о рекламе, согласно которым не допускается размещение рекламы информационной продукции, подлежащей классификации в соответствии с требованиями Федерального закона от 29 декабря 2010 г. N 436-ФЗ "О защите детей от информации, причиняющей вред их здоровью и развитию" (далее - Закон о защите детей), без указания знака возрастной категории данной информационной продукции <1>. Исходя из классификации, содержащейся в ч. 3 ст. 6 Закона о защите детей, возможны следующие варианты знаков: 0+, 6+, 12+, 16+, 18+ или "запрещено для детей". При этом отнесение продукции к соответствующей категории осуществляется ее производителем (распространителем) самостоятельно. Термин

"информационная продукция" раскрыт в [ч. 5 ст. 2](#) Закона о защите детей и охватывает не только предназначенную для оборота на территории РФ продукцию СМИ, печатную и аудиовизуальную продукцию на любых видах носителей, но и информацию, распространяемую посредством сети Интернет. Однако из этого не следует, что любой сайт в Интернете должен содержать знак возрастной категории. Согласно [п. 6 ч. 4 ст. 11](#) Закона о защите детей оборот информационной продукции без знака информационной продукции не допускается, за исключением информации, распространяемой посредством Интернета, кроме сетевых изданий. Исходя из этой не самым удачным образом (через двойное отрицание) сформулированной нормы, возрастной классификации подлежат лишь те интернет-сайты, которые зарегистрированы в качестве СМИ. Указания же возрастной категории на интернет-сайтах, которые не зарегистрированы в качестве СМИ, не требуется ^{<2>}. Однако даже если сам по себе интернет-сайт не требует маркировки, это не означает, что его владелец не должен соблюдать соответствующие требования применительно к рекламе информационной продукции, размещенной на таком интернет-сайте. Например, если посредством него осуществляется реклама концертов, фильмов, спектаклей или иных зрелищных мероприятий, она должна сопровождаться знаком информационной продукции;

^{<1>} Примечательно, что Закон о защите детей в [ч. 4 ст. 1](#) указывает, что он не распространяется на отношения в сфере рекламы. В то же время к нему отсылает Закон о рекламе и для применения

требований [ч. 10.1 ст. 5](#) необходимо обращение к понятиям и регулированию, содержащемуся в [Законе](#) о защите детей. Представляется, что такая несогласованность вызвана, с одной стороны, стремлением посредством положения [ч. 4 ст. 1](#) Закона о защите детей подчеркнуть эксклюзивность [Закон](#) о рекламе в плане регулирования отношений в сфере рекламы, а с другой - более поздним характером положений [ч. 10.1 ст. 5](#) Закона о рекламе, принятие которого не сопровождалось приведением в соответствие с ним иных положений законодательства. В любом случае положения [ч. 10.1 ст. 5](#) Закона о рекламе должны иметь приоритет и как более поздние, и как имеющие специальный характер.

<2> [Письмо](#) ФАС РФ от 5 сентября 2013 г. N АК/34774/13 "О применении Закона о рекламе в связи с вступлением в силу Закона о защите детей от информации, причиняющей вред их здоровью и развитию".

11) наконец, к информации, которая может быть квалифицирована как реклама, применяются специальные 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>. Первое правило преимущественно направлено на обеспечение доказательств по делам, связанным с нарушением законодательства о рекламе. В соответствии со [ст. 4.5](#) КоАП РФ постановление по делу о привлечении к административной ответственности за нарушение законодательства о рекламе может быть вынесено в течение одного года с момента совершения

административного правонарушения. Второе правило может быть большой неожиданностью для рекламодателей, размещающих рекламу в сети Интернет, учитывая, что двухмесячный срок действия обязанности заключить договор с каждым, кто откликнется, является достаточно продолжительным. И хотя судебная практика применения данного положения практически отсутствует, все же целесообразно ее принимать во внимание и по возможности ограничивать срок действия предложений о продаже товара (услуг), размещенных на интернет-сайтах, определенным сроком с учетом положений [ст. 190](#) ГК РФ.

<1> Как было отмечено в [§ 1 гл. 3](#) настоящей книги, практически любое предложение о продаже товара (услуги), размещенное на веб-сайте, является офертой с точки зрения российского законодательства.

Реклама, не соответствующая требованиям законодательства о рекламе, признается ненадлежащей. Надзор за соблюдением положений законодательства о рекламе осуществляют подразделения Федеральной антимонопольной службы <1>, которая периодически проводит мониторинг рекламы, распространяемой в сети Интернет. Порядок осуществления контроля регламентируется специальным [Законом](#) <2> и рядом подзаконных актов <3>. В числе возможных мер ответственности установлен административный штраф по [ст. 14.3](#) КоАП РФ: для граждан - 2 тыс. - 2,5 тыс. рублей; для должностных лиц - 4 тыс. - 25 тыс. рублей; для юридических лиц - 100 тыс. - 500 тыс. рублей. В соответствии с изменениями, внесенными в [КоАП](#) РФ, вступившими в силу 11 июля 2015 г., кредитные организации несут повышенную ответственность за

ненадлежащую рекламу услуг, связанных с предоставлением кредита или займа, если при этом не приводятся все условия, определяющие полную стоимость кредита (займа) для заемщика и влияющих на нее - 300 тыс. - 800 тыс. рублей (ч. 6 ст. 14.3 КоАП РФ) <4>. 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 <5>. 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. ч. 6 - 8 ст. 38 Закона о рекламе, где содержатся виды нарушений, за которые могут быть привлечены к ответственности рекламодатель, рекламораспространитель и рекламопроизводитель.

<1> См.: Постановление Правительства РФ от 30 июня 2004 г. N 331 "Об утверждении Положения о Федеральной антимонопольной службе".

<2> Федеральный закон от 26 декабря 2008 г. N

294-ФЗ "О защите прав юридических лиц и индивидуальных предпринимателей при осуществлении государственного контроля (надзора) и муниципального контроля".

<3> **Правила** рассмотрения антимонопольным органом дел, возбужденных по признакам нарушения законодательства Российской Федерации о рекламе, утв. Постановлением Правительства РФ от 17 августа 2006 г. N 508; Административный **регламент** Федеральной антимонопольной службы по исполнению государственной функции по рассмотрению дел, возбужденных по признакам нарушения законодательства Российской Федерации о рекламе, утв. Приказом ФАС России от 23 ноября 2012 г. N 711/12; **Положение** о государственном надзоре в области рекламы, утв. Постановлением Правительства РФ от 20 декабря 2012 г. N 1346; Административный **регламент** Федеральной антимонопольной службы по исполнению государственной функции по надзору за соблюдением законодательства о рекламе путем проведения проверок соблюдения законодательства Российской Федерации о рекламе, утв. Приказом ФАС России от 4 июня 2012 г. N 360.

<4> Федеральный **закон** от 29 июня 2015 г. N 175-ФЗ "О внесении изменений в статью 14.3 Кодекса Российской Федерации об административных правонарушениях".

<5> Постановление Пленума ВАС РФ от 8 октября 2012 г. N 58 "О некоторых вопросах практики применения арбитражными судами Федерального закона "О рекламе" (п. 10).

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 необходимость 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 **ч. 2 ст. 2** Закона о рекламе, обозначающие виды информации, которые не подпадают под действие данного **Закона**.

Во-первых, согласно **п. 2 ч. 2 ст. 2** Закона о рекламе он 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 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" <4>.

<1> Письма ФАС России от 13 сентября 2012 г. [N АК/29977](#) "О последних изменениях в требованиях к рекламе алкоголя"; от 29 июля 2010 г. [N АЦ/24295](#) "О ценовой информации, размещенной на сайте компании".

<2> [Постановление](#) Девятого арбитражного апелляционного суда от 31 августа 2011 г. [N 09АП-19239/2011](#) по делу [N А40-21958/11-147-169](#).

<3> [Постановление](#) Шестнадцатого арбитражного апелляционного суда от 6 ноября 2012 г. по делу [N 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.

<4> [Письмо](#) ФАС России от 29 июля 2010 г. N АЦ/24295 "О ценовой информации, размещенной на сайте компании".

Во-вторых, согласно [п. 3 ч. 2 ст. 2](#) Закона о рекламе, его положения 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 <1>.

<1> **Постановление** Восемнадцатого арбитражного апелляционного суда от 9 июля 2012 г. N 18АП-5796/2012 по делу N А07-4227/2012.

В-третьих, под действие законодательства о рекламе не подпадают объявления физических и юридических лиц, не связанные с осуществлением предпринимательской деятельности (п. 6 ч. 2 ст. 2 Закона о рекламе). Например, под данного рода исключение подпадают различного рода объявления о продаже товаров, размещенные физическими лицами на специализированных интернет-сайтах, вроде **ЛУНО**.

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, 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, размещенное в Интернете на сайте **www.nn.ru** сообщение следующего содержания: "Все [нецензурно], один ты классный", чередующееся с сообщением: "**nn.ru** понимает своих посетителей" было признано ненадлежащей рекламой <1>.

<1> **Постановление** Первого арбитражного апелляционного суда от 29 апреля 2013 г. по делу N А43-23179/2011.

В другом деле информация, размещенная на официальном сайте стоматологической клиники в Интернете, 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**" <1>. Данное дело иллюстрирует необходимость при наличии на веб-сайте интернет-магазина программ кредитования

максимально детально описывать их условия и соответствовать требованиям [ст. 28](#) Закона о рекламе.

<1> [Постановление](#) Первого арбитражного апелляционного суда от 18 мая 2011 г. по делу N A43-29149/2010. См. также Постановления ФАС Северо-Западного округа от 12 апреля 2012 г. по делу N [A56-30646/2011](#); Шестого арбитражного апелляционного суда от 10 февраля 2012 г. N [06АП-212/2012](#) по делу N A73-13859/2011.

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 <1>. Аналогичным образом будет признано недостоверной рекламой размещение на веб-сайте компании ложной информации относительно гарантий исполнения обязательств по договору вроде фразы "все вклады застрахованы" <2> или неполной информации о проводимой акции, из которой нельзя определить группы товаров, участвующих в ней <3>.

<1> См., например: [Постановление](#) Второго арбитражного апелляционного суда от 31 января 2013 г. по делу N A28-9625/2012. В данном деле основанием для такого 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.

<2> **Постановление** Шестого арбитражного апелляционного суда от 2 февраля 2011 г. N 06АП-6050/2010 по делу N А73-12012/2010. **Определением** ВАС РФ от 24 мая 2011 г. N ВАС-6179/11 отказано в передаче дела N 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.

<3> **Постановление** Девятого арбитражного апелляционного суда от 27 марта 2012 г. N 09АП-4440/2012-АК по делу N А40-127575/11-106-650.

Для признания информации в качестве рекламы необязательно, чтобы она была размещена на официальном сайте компании или на специализированных ресурсах, соответствующая информация может быть размещена и на страницах в социальных сетях. Вероятность квалификации в качестве рекламы информации, размещенной в социальных сетях, значительно повышается в случаях, когда на сайте компании содержатся кнопки быстрого доступа на соответствующую страницу в социальных сетях. В таком случае информация, содержащаяся на

сайте, и информация в социальных сетях при доказанности факта ее размещения работником организации или иным лицом по ее поручению, будет анализироваться в совокупности на предмет соответствия требованиям законодательства <1>.

<1> См., например: решения Тверского УФАС России от 11 марта 2015 г. по делу N 046/2-2-2015 на сайте: URL: <http://solutions.fas.gov.ru/to/tverskoe-ufas-rossii/04-6-2-2-2015>; Саратовского УФАС России по делу N 1-13/03 от 9 декабря 2013 г. на сайте: URL: <http://solutions.fas.gov.ru/to/saratovskoe-ufas-rossii/1-13-03>

.

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" <1>.

<1> **Постановление** Седьмого арбитражного апелляционного суда от 17 января 2011 г. N 07АП-10905/10 по делу N А45-15922/10.

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 вставляли 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 .ли, .рф, и на русскоязычных веб-сайтах под иными доменными именами. В частности, не допускать 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 применяться 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.

<1> **Постановление** ФАС Уральского округа от 27 декабря 2011 г. N Ф09-8458/11 (**Определением** ВАС РФ от 24 апреля 2012 г. N ВАС-4870/12 отказано в передаче дела N 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. Поисковая (контекстная) реклама

Одним из эффективных средств интернет-маркетинга является использование так называемой контекстной рекламы, под которой понимается "вид размещения интернет-рекламы, в основе которой лежит принцип соответствия появления рекламного материала в зависимости от контекста (содержания) просматриваемой пользователем интернет-страницы" <1>.

<1> **Постановление** Девятого арбитражного апелляционного суда от 13 июня 2012 г. N 09АП-14264/2012-АК по делу N А40-112441/11-90-469.

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 <1>.

<1> Jansen B. The Comparative Effectiveness of Sponsored and Nonsponsored Links for Web E-commerce Queries // ACM Transactions on the Web. Vol. 1. N 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>.

<1> Кузнецов Р.В. Указ. соч. С. 25.

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 <1>.

<1> См.: [письмо](#) ФАС России от 28 августа 2015 г. N АК/45828/15 "О рекламе в сети Интернет. Данный

вывод разделяется и в судебной практике. См., например: [Постановление](#) Девятого арбитражного апелляционного суда от 2 августа 2011 г. N 09АП-17064/2011-АК по делу N А40-21456/11-72-121.

Соглашение на размещение контекстной рекламы заключается между рекламодателем и поисковой системой или ее партнером (агентом). Такое соглашение обычно заключается посредством использования автоматизированного интерфейса, который становится доступным после регистрации рекламодателя в соответствующей поисковой системе. С точки зрения законодательства о рекламе поисковая система выступает как рекламодатель (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 информационной системы контекстной рекламы.

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.); установки географического и временного таргетинга <1>. В совокупности указанные параметры, образующие своего рода "техническое задание" рекламодателя, на практике именуются как "рекламная кампания".

<1> Юрасов А.В. Указ. соч. С. 306.

Если объявление соответствует требованиям провайдера услуг контекстной рекламы, что подтверждается фактом прохождения предварительной проверки, такое объявление может появиться рядом с результатами поисковой выдачи в рекламном блоке поисковой системы при введении соответствующих ключевых слов. При этом выбор того или иного объявления из всего массива объявлений будет зависеть от ряда показателей, в частности, установленной рекламодателем ставки цены за "клик", а также релевантности рекламируемого сайта, ссылка на который указана в объявлении, определяемой по алгоритмам поисковой системы.

В связи с тем что неотъемлемой частью размещения контекстной рекламы в Интернете является указание определенных ключевых слов, на

практике весьма актуален вопрос: насколько правомерно использование таких слов в тех случаях, когда они текстуально совпадают с товарными знаками или фирменными наименованиями, принадлежащими иным лицам? При этом подразумевается, что такие товарные знаки или фирменные наименования не воспроизводятся непосредственно в тексте самого объявления и (или) доменном имени интернет-сайта рекламодателя, поскольку в таком случае факт нарушения по общему правилу был бы налицо. Речь идет именно об использовании таких обозначений в качестве ключевых слов, которые визуально незаметны для пользователя.

Согласно [п. 4 ч. 2 ст. 5](#) Закона о рекламе недобросовестной признается реклама, которая является актом недобросовестной конкуренции в соответствии с антимонопольным законодательством. В свою очередь, Закон о защите конкуренции прямо указывает в качестве разновидности актов недобросовестной конкуренции совершение субъектом действий, способных вызвать смешение с деятельностью хозяйствующего субъекта - конкурента либо с товарами (услугами), вводимыми им в гражданский оборот на территории РФ, в том числе незаконное использование обозначения, тождественного товарному знаку или фирменному наименованию либо сходного с ними до степени смешения, в сети Интернет ([ст. 14.6](#) данного Закона). Поскольку товарные знаки и фирменные наименования являются охраняемыми средствами индивидуализации, вопросы их законного или незаконного использования регламентируются [ГК РФ](#).

В итоге возникает достаточно любопытная взаимосвязь трех нормативных актов: [Закона](#) о

рекламе, [Закона](#) о защите конкуренции и [ГК РФ](#). Для того чтобы определить факт наличия нарушения по одному из них, необходимо обратиться к другому, который в свою очередь предполагает применение третьего. Кроме того, такая ситуация порождает вопрос о соотношении ответственности по данным актам и допустимости одновременного привлечения к ответственности за нарушения, вызванные размещением контекстной рекламы. Рассмотрим данные проблемы подробнее.

1. Размещение контекстной рекламы и нарушение прав на товарный знак (фирменное наименование). Поскольку большое значение для наступления всех трех упомянутых ранее видов ответственности имеет наличие факта **незаконного использования** данных объектов, гражданско-правовой анализ отношений, возникающих при применении в контекстной рекламе обозначений, тождественных или схожих до степени смешения со средствами индивидуализации, принадлежащими конкурентам, играет важную роль.

В соответствии со ст. 1484 [ГК РФ](#) правообладателю товарного знака принадлежит исключительное право использования товарного знака любым не противоречащим закону способом, в частности, в предложениях о продаже товаров, объявлениях и в рекламе, а также в сети Интернет, в том числе в доменном имени и при других способах адресации ([подп. 4 и 5 п. 2 ст. 1484 ГК РФ](#)). Таким образом, формальное толкование закона на первый взгляд 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. Кроме того, такое использование имеет место в сети Интернет, поскольку системы контекстной рекламы функционируют в неразрывной связи с поисковыми интернет-сервисами. Однако ответ на поставленный вопрос не так однозначен, как может показаться на первый взгляд. Прежде чем обратиться к практике российских судов, целесообразно остановиться на зарубежных подходах к решению данного вопроса.

Одними из первых с данным вопросом столкнулись суды США. Первым по данной тематике стало дело **Playboy Enterprises, Inc. v. Netscape Communications and Excite, Inc.** <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 признал наличие нарушения прав на товарные знаки в виде заманивания покупателей, заинтересованных в приобретении товаров истца, на свой сайт (так называемая доктрина **initial interest confusion**) <2>, приняв во внимание следующие факты: 1) введение в заблуждение потребителей вследствие возникновения у них впечатления о связи рекламы и (или) продуктов с компанией **Playboy**, что было подтверждено заключением эксперта; 2) широкая известность торговых знаков, принадлежащих компании **Playboy**; 3) их использование для продвижения однородных товаров; 4) низкий уровень внимания потребителей к обозначениям при приобретении товаров "для

взрослых". При этом суд особо отметил, что если бы соответствующая реклама четко обозначала ее источник, никакого введения в заблуждение потребителей не было бы, как не было бы и нарушения правил использования товарных знаков. Однако поскольку ответчик не требовал такого обозначения, это и обусловило признание его виновным в соответствующем нарушении.

<1> 354 F.3d 1020 (9th Cir. 2004).

<2> Данная доктрина ранее уже применялась указанным судом к случаям использования обозначений, воспроизводящих товарный знак истца в HTML-коде интернет-сайта ответчика с целью заманивания потребителей к себе на сайт. См.: **Brookfield Communications, Inc. v. West Coast Entertainment Corporation**, 174 F.3d 1036 (9th Cir. 1999). Другие дела, связанные с применением данной доктрины: **Australian Gold, Inc. v. Hatfield**, 436 F.3d 1228 (10th Cir. 2006); **Storus Corp. v. Aroa Mktg, Inc.**, N C-06-2454 MMC, 2008 WL 449835 (N.D. Cal. Feb. 15, 2008).

Другим известным в указанной сфере стало дело **Google, Inc. v. American Blind and Wallpaper Factory, Inc** <1>. В данном споре истец, компания по производству обоев и занавесок, обвинила компанию **Google** в нарушении правил использования товарных знаков, поскольку посредством **Google Adwords** иные лица могли "привязать" показ своей рекламы к ее товарным знакам и тем самым вводить в заблуждение потребителей, заманивая их к себе (**initial interest confusion**). Судебная тяжба длилась около четырех

лет. Позиция **Google** сводилась к тому, что компания сама не использует спорный товарный знак, это делают рекламодатели. Кроме того, использование товарного знака ограничено внутренними процессами функционирования **Google Adwords**. По мнению суда, сославшегося на прецедент в деле **Playboy Enterprises, Inc. v. Netscape Communications**, действия **Google** все же могли быть квалифицированы как использование товарного знака в соответствии с Lanham Act. Впоследствии дело было завершено мировым соглашением, условия которого конфиденциальны. Тем не менее эксперты сходятся во мнении, что благодаря данному соглашению компания **Google** по сути выиграла дело, поскольку воспрепятствовала созданию негативного прецедента.

<1> N 03-cv-05340 JF (RS) (N.D. Cal. Apr. 18, 2007).

Окончательная победа **Google** в споре о возможности привлечения к ответственности провайдера контекстной рекламы была закреплена в деле **Rosetta Stone Ltd. v. Google, Inc.** <1>, суть которого такова: истец, являвшийся продавцом продуктов для удаленного изучения языков, обратился с иском к **компании Google**, приведя доводы, схожие с теми, которые фигурировали в предыдущих делах: ответчик якобы осуществлял непосредственное нарушение правил использования товарного знака истца путем продажи зарегистрированного обозначения в качестве ключевого слова иным лицам, что вводило в заблуждение потребителей. Кроме того, было заявлено требование о нарушении правил использования товарного знака посредством его "размывания" (dilution). Суд первой инстанции отказал в удовлетворении

данных 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. Отказывая в удовлетворении требования, связанного с "размыванием" товарного знака, суд указал, что **Google** не занимается продажами продуктов, конкурирующих с продуктами истца, поэтому не мог нарушить права на его товарный знак таким способом. Окружной суд изменил решение суда первой инстанции, указав на наличие оснований для наступления ответственности за непосредственное нарушение правил использования товарного знака истца, поскольку ряду доказательств, свидетельствующих о возможном введении в заблуждение потребителей, не была дана должная оценка <2>. Однако так же, как и в предыдущем случае, дело было завершено мировым соглашением. Таким образом, с юридической точки зрения компания **Google** не выиграла и не проиграла данный спор, однако, по мнению экспертов, решение по этому делу практически поставило точку в вопросе о легитимности практик **AdWords**, решив этот вопрос в пользу **Google** <3>.

<1> Rosetta Stone Ltd. v. Google, Inc., 730 F. Supp. 2d 531 (E.D. Va. 2010), *aff'd in part and vacated in part* 676 F.3d 144 (4th Cir. 2012).

<2> 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

(с).

<3> Goldman E. More Confirmation That Google Has Won the AdWords Trademark Battles Worldwide // Forbes Tech. 22 March 2013. URL: <http://goo.gl/EVGv5H>.

В тех спорах, где в качестве ответчика выступал непосредственно рекламодатель, использующий в своей рекламе ключевые слова, американские суды обычно признают его виновным в нарушении товарного знака посредством заманивания покупателей, заинтересованных в приобретении товаров истца, на свой сайт (**initial interest confusion**) <1>. Особо следует отметить дело **Orion Bancorp, Inc. v. Orion Residential Finance LLC and others** <2>, где 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 будущем.

<1> См., например: *Australian Gold, Inc. v. Hatfield*, 436 F.3d 1228 (10th Cir. 2006); *Storus Corp. v. Aroa Mktg., Inc.*, N 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, N 8:07-cv-1753-T-26 MAP.

В Европе судебная практика по данному вопросу долгое время отличалась значительным разнообразием даже в пределах одной страны. Во Франции некоторые суды признавали поисковые системы, "продающие" ключевые слова, нарушающими права третьих лиц на

товарный знак <1>. Другие суды не находили нарушений со стороны поисковых систем, указывая, что нарушителем является рекламодаделец <2>.

<1> Cour D'Appel de Paris, 01.02.2008, Case N 06/13884, GIFAM et autres/SARL Google France et Google Inc.

<2> 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.

Показательна также и немецкая практика, где мнения судов различных земель по рассматриваемой проблематике долгое время различались. Одни суды (земель Брауншвейг <1>, Мюнхен <2>, Штутгарт <3>, Дрезден <4>) сочли использование в качестве ключевых слов обозначений, воспроизводящих товарный знак третьих лиц, нарушением исключительного права на такой товарный знак. Суды Франкфурта <5>, Дюссельдорфа <6>, Кельна <7>, напротив, сочли такое использование допустимым. Точку в данном 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 <8>. Суд также отметил, что нанесение ущерба правообладателю товарного знака имеет место тогда, когда среднестатистическому пользователю неясно, исходят ли рекламируемые товары от правообладателя товарного знака (или от связанного с ним предприятия) либо от третьей стороны. В частности, такое нарушение имеет место в случаях, когда может сложиться впечатление, что между

рекламодателем и владельцем товарного знака существует хозяйственная связь. Кроме того, выбор известного товарного знака в отношении рекламы однородных товаров способен наносить ущерб правообладателю товарного знака, в связи с чем предполагается, что его использование без достаточных оснований недобросовестно или причиняет вред и служит в целях использования различительной способности и накопленной ценности товарного знака.

<1> Oberlandesgericht Braunschweig. 05.12.2006. N 2 W 23/06; Oberlandesgericht Braunschweig. 11.12.2006. N 2. W 177/06; Oberlandesgericht Braunschweig. 12.07.2007. N 2 U 24/07.

<2> Oberlandesgericht Minchen. 06.12.2007. N 29 U 4013/07.

<3> Oberlandesgericht Stuttgart. 09.08.2007. N 2 U 23/07.

<4> Oberlandesgericht Dresden. 09.01.2007. N 14 U 1958/06.

<5> Oberlandesgericht Frankfurt. 26.02.2008. N 6 W 17/08.

<6> Oberlandesgericht Dusseldorf. 23.01.2007. N 1-20 U 79/06.

<7> Oberlandesgericht Koln. 31.08.2007. N 6 U 48/07.

<8> Bundesgrerichtshof. 13.12.2012. N I ZR 217/10.

Отсутствие единообразной практики применения положений о товарном знаке к новым способам рекламирования товаров в сети Интернет, а также общеевропейский характер законодательства о товарных 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>.

<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.

В первом деле, где предметом рассмотрения была практика французских судов, Европейский суд пришел к следующим выводам. Во-первых, использование в качестве ключевого слова обозначения, идентичного товарному знаку конкурента, для рекламы собственных однородных товаров (услуг) является незаконным использованием товарного знака в соответствии с европейским законодательством, если

соответствующая реклама не позволяет среднему пользователю сети Интернет сделать без особых усилий вывод о том, какие именно товары рекламируются: принадлежащие владельцу товарного знака или третьему лицу. Во-вторых, провайдер сервиса контекстной рекламы, который хранит в своей информационной системе данные о ключевых словах и организывает показ рекламы на их основе как таковой, не осуществляет использования товарного знака. В-третьих, провайдер такого сервиса может рассматриваться в качестве информационного посредника и пользоваться иммунитетом интернет-провайдера, предусмотренным [ст. 14 Директивы об электронной коммерции](#), в тех случаях, когда он не играет такой активной роли в отношении контента, которая позволила бы говорить о том, что он знает и контролирует содержание хранимых им данных, а по получении уведомления от правообладателя товарного знака безотлагательно удаляет соответствующую рекламу. 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 для владельцев товарных знаков должны выступать рекламодатели.

Во втором деле Европейский суд уже детально рассмотрел условия, при которых рекламодателя возможно привлечь к ответственности за размещение контекстной рекламы, в которой используются обозначения, воспроизводящие товарный знак конкурента. Суд рассмотрел данный вопрос через призму трех основных функций товарного знака: индивидуализирующей, рекламной и репутационной. При этом нарушение права на товарный знак имеет место тогда, когда наносится ущерб одной из указанных

функций товарного знака. Индивидуализирующая функция товарного знака заключается в том, чтобы потребители при помощи товарного знака могли отличить определенные товары от аналогичных товаров, маркированных иным товарным знаком. 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 представляет собой **способ** приобретения, усиления и защиты репутации товарного знака. Указанная функция, по мнению суда, как правило, не нарушается в том случае, когда в качестве ключевого слова используется обозначение, зарегистрированное как товарный знак конкурента, поскольку правообладатель может использовать то же самое ключевое слово для своей рекламы и потеснить рекламу конкурента, предложив большую цену за клик. Законодательство о товарном знаке не имеет своей целью предоставить правообладателю полный иммунитет от конкурентных практик на рынке. Репутационная функция товарного знака предполагает защиту инвестиций правообладателя в поддержание его имиджа и выражается в привлекательности для потребителя, обуславливающей их лояльность и постоянство их выбора, а также отличие товара начинающего бизнеса от товара, уже зарекомендовавшего себя на рынке. Данная функция может быть серьезно затронута такой практикой, поскольку использование соответствующих 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. Однако о

нарушении репутационной функции товарного знака можно говорить лишь в тех случаях, когда рекламодатель предлагает не просто альтернативу товарам (услугам) обладателя товарного знака, а их имитацию, либо когда имеет место "размывание" товарного знака с риском утраты его различительной способности или очернения репутации такого товарного знака.

Указанные решения Европейского суда легли в основу последующих решений национальных судов. Так, Высокий суд Англии в деле **Interflora, Inc. v Marks & Spencerplc** <1> признал использование в качестве ключевого слова в сервисе **Google AdWords** 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.

<1> **Interflora Inc. & Anor v Marks and Spencer Plc & Anor**. 21.05.2013. EWHC 1291.

Российская судебная практика также может похвастаться наличием судебных решений, в которых затрагивается проблематика возможности квалификации указания ключевых слов при размещении контекстной рекламы в качестве незаконного использования средства индивидуализации. При этом

отечественные суды в большинстве своем исходят из того, что ключевые слова, используемые при размещении контекстной рекламы, употребляются **исключительно в технических целях**, в связи с чем о нарушении исключительного права на товарный знак говорить нельзя. Данный подход обычно мотивируется тем, что: 1) одно и то же ключевое слово может быть выбрано для рекламных объявлений различных рекламодателей; 2) ключевые слова не являются частью самого рекламного объявления, не входят в его содержание и не демонстрируются пользователям; 3) пользователь не обладает информацией о том, по каким ключевым словам размещается показанное ему поисковой системой рекламное объявление, а также не может соотнести определенное объявление с конкретными ключевыми словами. Из этого делается вывод, что ключевые слова, используемые при размещении контекстной рекламы, не обладают индивидуализирующей способностью по отношению к каким-либо товарам, услугам или лицам. Ключевое слово является, таким образом, внутренним элементом системы и не показывается в тексте рекламного объявления, целью его использования является не маркировка товаров и услуг для введения в оборот, а определение целевой аудитории. Применение соответствующих обозначений в качестве ключевых не является, таким образом, использованием фирменного наименования или товарного знака и не нарушает исключительных прав правообладателей указанных объектов <1>.

<1> См.: Постановления Суда по интеллектуальным правам от 3 июня 2014 г. по делу [N A51-11605/2013](#) и от 26 ноября 2013 г. по делу [N A40-164436/2012](#); Девятого арбитражного

апелляционного суда от 5 августа 2013 г. [N 09АП-22393/2013-ГК](#) по делу N А40-159412/12 и от 24 июля 2013 г. [N 09АП-19422/2013-ГК](#) по делу N А40-164436/12; Двенадцатого арбитражного апелляционного суда от 20 июня 2012 г. по делу [N А12-1125/2012](#) и др.

Представляется, что описанный подход российской судебной практики не лишен определенной логики. 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 <1>.

<1> **Постановление** Девятого арбитражного апелляционного суда от 24 июля 2013 г. N 09АП-19422/2013-ГК по делу N А40-164436/12.

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 большой 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...

Что отличает подход отечественных судов к проблематике использования ключевых слов с точки зрения положений о товарных знаках, так это категоричность и чрезмерный акцент на технических аспектах функционирования данных сервисов в ущерб экономическим. Подход американских и европейских судов является более взвешенным и учитывающим возможную недобросовестность рекламодателей. 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. Тем более что некоторые формальные основания для этого все же есть. Необходимо упомянуть, что в весьма схожей ситуации (использование товарного знака третьего лица в HTML-коде интернет-страницы для целей оптимизации ее поиска и выдачи поисковыми системами) суд признал факт нарушения исключительного права на товарный знак, указав, что "нарушение прав владельца товарного знака может иметь место не только при использовании сходного до степени смешения обозначения в доменном имени и

других способах адресации, но и иным способом в сети Интернет, если в результате такого использования у потребителей возникнет вероятность смешения производителей этих товаров и услуг. Использование в доменном имени и при других способах адресации не является единственно возможным способом использования товарного знака в сети Интернет, о чем говорит употребленное законодателем словосочетание "в частности" <1>. Таким образом, при желании признать использование ключевого слова нарушением товарного знака суд имеет возможность сослаться на [подп. 5 п. 2 ст. 1484 ГК РФ](#), отметив, что исключительное право на товарный знак охватывает различные способы его использования в Интернете (не только в системах адресации), причислив к ним и использование для целей контекстной рекламы. Пойдет ли практика таким путем и при каких условиях, покажет время, а пока необходимо рассмотреть, может ли использование чужих средств индивидуализации в качестве ключевых слов для рекламы собственных товаров (услуг) выступать как акт недобросовестной конкуренции.

<1> [Постановление](#) ФАС Северо-Западного округа от 22 марта 2010 г. по делу N А56-1580/2008.

2. Размещение контекстной рекламы как акт недобросовестной конкуренции. В соответствии с [п. 9 ст. 4](#) Закона о защите конкуренции под недобросовестной конкуренцией понимаются любые действия хозяйствующих субъектов (группы лиц), которые отвечают следующим признакам в совокупности: 1) направлены на получение преимуществ при осуществлении предпринимательской

деятельности; 2) противоречат законодательству Российской Федерации, обычаям делового оборота, требованиям добропорядочности, разумности и справедливости и 3) причинили или могут причинить убытки другим хозяйствующим субъектам-конкурентам либо нанесли или могут нанести вред их деловой репутации. Данная дефиниция основана на [ст. 10-bis](#) Парижской конвенции по охране промышленной собственности 1883 г. (в редакции Стокгольмского акта 1967 г.), которая гласит: "Актом недобросовестной конкуренции считается всякий акт конкуренции, противоречащий частным обычаям в промышленных и торговых делах". В рамках четвертого антимонопольного пакета положения о недобросовестной конкуренции были существенным образом детализированы: вместо одной статьи появилась целая [глава](#) с выделением в отдельные статьи положений о наиболее типичных видах недобросовестной конкуренции. В контексте проблематики использования ключевых слов в рекламе особый интерес представляют следующие статьи Закона о защите конкуренции: [ст. 14.1](#) "Запрет на недобросовестную конкуренцию путем дискредитации", [ст. 14.2](#) "Запрет на недобросовестную конкуренцию путем введения в заблуждение" и [ст. 14.6](#) "Запрет на недобросовестную конкуренцию, связанную с созданием смешения".

В соответствии со [ст. 14.1](#) Закона о защите конкуренции не допускается недобросовестная конкуренция путем дискредитации, т.е. распространения ложных, неточных или искаженных сведений, которые могут причинить убытки хозяйствующему субъекту и (или) нанести ущерб его деловой репутации. В практике российских судов уже встречались дела, где контекстная реклама была признана ненадлежащей по причине того, что она порочит деловую репутацию

конкурента. Иллюстрацией служит дело, в котором суд пришел к выводу о том, что реклама "Долги группы "РеноваСтройГруп" Экспертиза, взыскание и продажа долгов "РеноваСтройГруп" 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 "РеноваСтройГруп" перед другими хозяйствующими субъектами и формирует негативное отношение к данной компании" <1>. В данном случае было установлено, что правопредшественник истца действительно имел долги, которые были взысканы с использованием услуг ответчика, но на момент размещения рекламы задолженность 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. Однако подобного рода случаи все же носят исключительный характер, в связи с чем особый интерес представляют собой следующие два состава недобросовестной конкуренции.

<1> [Постановление](#) Девятого арбитражного апелляционного суда от 17 ноября 2011 г. N 09АП-27661/2011-АК по делу N А40-51810/11-145-421.

В литературе отмечается, что при недобросовестном использовании ключевых слов может наблюдаться недобросовестная конкуренция посредством введения в заблуждение потребителей. Так, по мнению В. Перевалова и О. Блинова, "недобросовестная конкуренция может иметь место,

например, в том случае, когда текст рекламного объявления, отображаемого при поиске определенного производителя или товаров определенной марки, не позволяет пользователю должным образом определить, что на рекламируемом сайте вместо искомой продукции будет представлена продукция конкурента" <1>. Важно подчеркнуть, что в отличие от ранее действовавшей редакции [ст. 14](#) Закона о защите конкуренции новая [ст. 14.2](#) данного Закона не содержит исчерпывающего перечня условий и характеристик, в отношении которых возможно введение в заблуждение потребителей, что должно облегчить ее применение в рассматриваемом случае. Главное, чтобы действия соответствовали общим признакам недобросовестной конкуренции, указанным выше. Как показывает зарубежная практика, "паразитирование" на репутации известного товарного знака, сопровождающееся введением в заблуждение относительно происхождения рекламируемого товара или характера хозяйственных связей между правообладателем товарного знака и конкурирующим с ним рекламодателем, рассматривается в качестве недобросовестного поведения, в связи с чем установить его противоречие требованиям добросовестности, разумности и справедливости не так сложно. Особенно это будет справедливо в случаях, когда вследствие таких действий клиенты правообладателя направлены по ложному пути, приводящему к конкуренту. Что же касается двух других критериев недобросовестной конкуренции (направленность действий рекламодателя на получение преимуществ при осуществлении предпринимательской деятельности и возможность причинения убытков конкурентам), то с доказыванием их наличия в таких случаях также не должно возникать особых проблем.

<1> Перевалов В., Блинов О. [Поисковая реклама с точки зрения прав](#) на товарные знаки и законодательства о защите конкуренции в России и за рубежом // Закон. 2014. N 9. С. 109.

Примечательно, что уже появляется практика ФАС по квалификации как акта недобросовестной конкуренции действий по использованию в качестве ключевых слов в поисковой рекламе известного товарного знака конкурента с целью привлечения потребителей, желавших воспользоваться схожими услугами по доставке пиццы <1>.

<1> Постановление УФАС по г. Москве от 17 февраля 2014 г. по делу N 4-14.33-114/7714. ТОЕ <http://solutions.fas.gov.ru/to/moskovskoe-ufas-rossii/4-14-33-114-77-14>.

Что же касается возможности применения положений [ст. 14.6](#) Закона о защите конкуренции, то здесь могут возникнуть проблемы, обусловленные существующим судебным толкованием понятия "использование товарного знака" применительно к спорам о нарушении исключительного права на товарный знак. Дело в том, что диспозиция указанной [статьи](#) практически воспроизводит соответствующие положения [ст. 1484](#) ГК РФ, которая гласит: "Не допускается недобросовестная конкуренция путем совершения хозяйствующим субъектом действий (бездействия), способных вызвать смешение с деятельностью хозяйствующего субъекта-конкурента либо с товарами или услугами, вводимыми хозяйствующим субъектом-конкурентом в гражданский оборот на территории Российской Федерации, в том

числе: 1) незаконное использование обозначения, тождественного товарному знаку, фирменному наименованию... путем его использования в информационно-телекоммуникационной сети Интернет, включая размещение в доменном имени и при других способах адресации".

Поскольку **Закон** о защите конкуренции не содержит собственной дефиниции понятия "незаконное использование средства индивидуализации", приходится руководствоваться положениями **ГК РФ** <1>, а вместе с ними и судебной практикой, интерпретирующей данные положения. Как было показано ранее, суды в большинстве своем не усматривают в использовании ключевых слов, тождественных или схожих до степени смешения с зарегистрированным товарным знаком, нарушения исключительного права на последний. Отсутствие факта незаконного использования означает и отсутствие факта совершения акта недобросовестной конкуренции по **п. 1 ст. 14.6** Закона о защите конкуренции <2>. Конечно, теоретически сохраняется возможность представить случаи с использованием ключевых слов как ситуацию **sui generis** - непоименованный в **ст. 14.6** акт недобросовестной конкуренции, но, принимая во внимание наличие специальной **статьи** с определенным перечнем условий, перспективы данного аргумента представляются туманными.

<1> В этом ключе толкуют положения **Закона** о защите конкуренции, в частности, авторы комментария к данному **Закону**, подготовленного под редакцией руководителя ФАС И.Ю. Артемьева. См.: Научно-практический **комментарий** к Федеральному

закону "О защите конкуренции" / Отв. ред. И.Ю. Артемьев; МГИМО, МИД России, ФАС России. М.: Статут, 2015. С. 246.

<2> См., например: [Постановление](#) Суда по интеллектуальным правам от 3 июня 2014 г. по делу N А51-11605/2013, в котором говорится, что "суд кассационной инстанции не может согласиться с доводом заявителя о том, что действия ответчиков по использованию товарного знака истца в контекстной рекламе являются актом недобросовестной конкуренции, поскольку судами установлено, что действия ответчиков не могут быть квалифицированы как использование товарного знака истца в смысле [статьи 1484 ГК РФ](#)".

Думается, что несколько больше шансов на успех может быть в случае квалификации действий рекламодателя по использованию ключевых слов, тождественных или схожих до степени смешения со средствами индивидуализации конкурентов, в качестве акта недобросовестной конкуренции по [ст. 14.8](#) Закона о защите конкуренции как иной формы недобросовестной конкуренции, не предусмотренной [ст. ст. 14.1 - 14.7](#) данного Закона. В тех случаях, когда нет достаточных оснований для вывода о причинении такими действиями ущерба деловой репутации конкурента ([ст. 14.1](#)), введении в заблуждение потребителей ([ст. 14.2](#)) или создании смешения ([ст. 14.6](#)), но тем не менее очевидно стремление рекламодателя повысить свои продажи, привлекая на свой интернет-сайт потребителей, интересующихся товарами (услугами) конкурента, можно говорить о недобросовестной конкуренции, выражающейся в недолжном присвоении преимуществ от заслуженной правообладателем деловой репутации, в создание которой им были произведены значительные

вложения. В таком случае можно утверждать, что рекламодатель пытается "пожинать там, где не сеял". Разумеется, такого рода недобросовестная конкуренция предполагает наличие "сильного" товарного знака, в противном случае говорить о присвоении рекламодателем контекстной рекламы заслуженной деловой репутации, ассоциирующейся с товарным знаком, вряд ли возможно. О "силе" товарного знака могут свидетельствовать следующие факторы: степень различительной способности товарного знака; продолжительность и географический охват его использования; продолжительность и интенсивность маркетинговых компаний правообладателя, проведенных в целях продвижения товарного знака; степень узнаваемости товарного знака и др. Насколько такая квалификация будет востребована практикой в условиях технократического подхода арбитражных судов к решению споров по поводу контекстной рекламы, покажет время.

Признание действий рекламодателя актом недобросовестной конкуренции является основанием для привлечения к административной ответственности по [ст. 14.33 КоАП РФ](#), а также для предъявления правообладателем гражданско-правового иска о прекращении нарушения прав, возмещении убытков, включая упущенную выгоду ([ч. 3 ст. 37 Закона о защите конкуренции](#)). Принимая во внимание положения [п. 2 ст. 15 ГК РФ](#), согласно которым потерпевшее лицо вправе требовать возмещения наряду с другими убытками упущенной выгоды в размере не меньшем, чем доходы, которые нарушитель получил вследствие нарушения права, возможность предъявления гражданско-правового иска может представлять особый интерес для правообладателя даже в тех случаях, если по каким-либо причинам он не получил компенсацию за нарушение исключительного права на принадлежащее

ему средство индивидуализации.

3. Размещение контекстной рекламы как ненадлежащая реклама. Как отмечалось ранее, разновидностью ненадлежащей рекламы является реклама, представляющая собой акт недобросовестной конкуренции (п. 4 ч. 2 ст. 5 Закона о рекламе). Поскольку данный состав недобросовестной рекламы носит отсылочный характер, все то, что было сказано ранее применительно к возможности квалификации в качестве недобросовестной конкуренции действий по использованию в контекстной рекламе ключевых слов, тождественных или схожих до степени смешения со средствами индивидуализации конкурентов, применимо и к квалификации подобных действий в качестве ненадлежащей рекламы. Однако здесь возникает другой весьма важный вопрос: возможно ли одновременное привлечение лица к ответственности за одно и то же деяние при нарушении антимонопольного законодательства и при нарушении законодательства о рекламе?

С одной стороны, существует известный принцип **"non bis in idem"** (от лат. "не дважды за одно и то же"), согласно которому одно и то же действие не должно дважды выступать предметом какого-либо правового разбирательства. Данный принцип нашел свое отражение в КоАП РФ: согласно ч. 5 ст. 4.1 никто не может нести административную ответственность дважды за одно и то же административное правонарушение.

Согласно позиции Пленума ВАС при разграничении сферы применения Закона о рекламе и Закона о защите конкуренции судам следует исходить из того, что если ложные, неточные или искаженные

сведения, которые могут причинить убытки хозяйствующему субъекту либо нанести ущерб его деловой репутации, некорректное сравнение хозяйствующим субъектом производимых или реализуемых им товаров с товарами, производимыми или реализуемыми другими хозяйствующими субъектами, находящимися в состоянии конкуренции с указанным лицом, а также иная информация, распространение которой отвечает признакам недобросовестной конкуренции, содержатся в рекламе, то применяется административная ответственность, установленная [ст. 14.3](#), а не [ст. 14.33](#) КоАП РФ (недобросовестная конкуренция) <1>. Эта позиция получила развитие в письме ФАС России, где указывается, что если информация содержит не соответствующие действительности сведения, некорректное сравнение, вводит потребителей в заблуждение, распространяется исключительно в рекламе, то она подлежит оценке на предмет соответствия законодательству о рекламе; если же она распространяется как в рекламе, так и иными способами при введении товара в оборот, то подлежит оценке на предмет соответствия антимонопольному законодательству (в части недобросовестной конкуренции) <2>. Иными словами, если акт недобросовестной конкуренции имеет место в рекламе, то его пресечение осуществляется в соответствии с [Законом](#) о рекламе, а не в соответствии с [Законом](#) о защите конкуренции <3>.

<1> См. [п. 7](#) Постановления Пленума ВАС РФ от 8 октября 2012 г. N 58 "О некоторых вопросах практики применения арбитражными судами Федерального закона "О рекламе".

<2> См.: [письмо](#) ФАС России от 25 июня 2014 г. N АК/25319/14.

<3> Научно-практический [комментарий](#) к Федеральному закону "О защите конкуренции" / Отв. ред. И.Ю. Артемьев. С. 237.

Таким образом, в случае квалификации в качестве акта недобросовестной конкуренции действий рекламодателя по размещению рекламы с использованием ключевых слов, тождественных или схожих до степени смешения со средствами индивидуализации конкурента, административная ответственность за данное действие должна определяться по [ст. 14.3](#) КоАП РФ, а не по [ст. 14.33](#) КоАП РФ, даже несмотря на то, что диспозиция указанного правонарушения содержится в [Законе](#) о защите конкуренции.

Однако на практике все не так однозначно. По одному из недавних дел УФАС привлекло сеть супермаркетов к ответственности в связи с нарушением [Закона](#) о защите конкуренции за ненадлежащую рекламу шоколада в СМИ. Как указал суд, "нарушение законодательства о рекламе не исключает возможности привлечения к ответственности, в том числе за нарушение законодательства о конкуренции, так как в соответствии с [частью 1 статьи 4.4](#) КоАП РФ при совершении лицом двух и более административных правонарушений административное наказание назначается за каждое совершенное административное правонарушение. В данном случае факт нарушения заявителем законодательства о конкуренции установлен решением антимонопольного органа" <1>. В другом деле УФАС привлекло хозяйствующего субъекта к ответственности за использование товарного

знака конкурента в качестве ключевых слов по [ст. 14.33](#) КоАП РФ как за недобросовестную конкуренцию <2>. Так что, к сожалению, разъяснения Пленума ВАС РФ и последовавшие за ним разъяснения ФАС России не способствовали обеспечению единства взглядов на рассматриваемую проблему в правоприменительной практике. В некоторых случаях по-прежнему допускается кумулятивное применение [ст. ст. 14.3](#) и [14.33](#) КоАП РФ, в других отдается приоритет [ст. 14.33](#) КоАП РФ несмотря на то, что акт недобросовестной конкуренции имел место в отношении рекламного характера.

<1> [Постановление](#) ФАС Московского округа от 30 июля 2014 г. по делу N А40-181396/13.

<2> Постановление УФАС по г. Москве от 17 февраля 2014 г. по делу N 4-14.33-114/77-14.

Приведенные 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 средства индивидуализации конкурентов, а также содержащих потенциально недостоверные или порочащие их деловую репутацию сведения.

Кроме того, как показывает судебная практика, суды иногда поддерживают квалификацию в качестве ненадлежащей рекламы действий по "заманиванию" потребителей посредством использования в контекстной рекламе обозначений, с которыми

ассоциируется конкурент рекламодателя. Так, в одном из дел застройщик (ЖК "Премьер") был привлечен к ответственности за ненадлежащую контекстную рекламу в системе **Google Adwords**: "Ищете квартиры в ЖК "Оазис"? - gorod-v-gorode.ru. Реклама www.gorod-v-eorode.ru и 8(383) 355-77-44 ЖК "Премьер"...". С обозначением "ЖК "Оазис" у жителей г. Новосибирска ассоциировался микрорайон, возводимый другим застройщиком. Клик по объявлению приводил на сайт с информацией о ЖК "Премьер". По мнению антимонопольного органа, такая реклама намеренно вводила потенциальных приобретателей в заблуждение и нарушала запрет на недостоверную рекламу <1>. Поскольку в данном случае фигурировал не товарный знак, а фирменное наименование, данный случай вряд ли способен изменить доминирующий подход отечественных судов к правовой квалификации использования охраняемых средств индивидуализации в контекстной рекламе.

<1> Решение Арбитражного суда Новосибирской области от 25 сентября 2015 г. по делу N А45-12842/2015.

В общем и целом, как представляется, следует согласиться с мнением В. Перевалова и О. Блинова, что российская практика по делам об использовании товарных знаков в поисковой рекламе в настоящее время не позволяет правообладателям эффективно бороться с использованием принадлежащих им товарных знаков в качестве ключевых слов для поисковой рекламы <1>. У правообладателя товарного знака больше перспектив защиты своих прав при использовании арсенала антимонопольного

законодательства, который в идеале должен дополнять частноправовые средства защиты, предоставляемые законодательством об интеллектуальной собственности. В российских реалиях, учитывая, что за нарушение антимонопольного законодательства, помимо наступления административной ответственности, имеется возможность предъявления гражданско-правовых требований, антимонопольное законодательство может превратиться из комплементарного механизма защиты прав на товарный знак в основной.

<1> Перевалов В., Блинов О. [Указ. соч.](#) С. 110.

В завершение рассмотрения вопроса о возможных рисках использования контекстной рекламы отметим, что необходимо учитывать следующее: в соответствии с недавней судебной практикой использование автоматизированных средств анализа сообщений электронной почты пользователя для последующего отправления ему контекстной рекламы является незаконным. Так, в одном из известных деле Мосгорсуд признал, что роботы компании **Google** "читают" переписку истца, а следовательно, нарушают его право на тайну переписки, закрепленное в [Конституции](#) РФ и Европейской [конвенции](#) по правам человека. Как следствие, локальное подразделение компании **Google** было привлечено к гражданско-правовой ответственности за нарушение личного неимущественного права на тайну переписки в виде возмещения морального ущерба <1>. Это может являться основанием для вывода о том, что контекстная реклама, основанная на автоматизированном анализе контента, защищенного тайной переписки, может быть признана ненадлежащей. Однако на момент написания

второго издания настоящей книги соответствующей практики ФАС не появилось, а само решение Мосгорсуда может быть обжаловано в Верховном Суде РФ. Но в любом случае, несмотря на возможный политический подтекст решения Мосгорсуда, использование автоматизированных алгоритмов анализа пользовательского контента, относящегося к информации ограниченного доступа, сопряжено с рядом рисков, особенно если в качестве провайдера выступает иностранное лицо.

<1> Апелляционное [определение](#) Мосгорсуда от 16 сентября 2016 г. по делу N 33-30344.

§ 3. 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 Интернете является компания **IAB (Interactive Advertising Bureau)**.

<1> Филатова О.А. Гражданско-правовые особенности рекламы в Интернете: Дис. ... канд. юрид. наук. М., 2003. С. 3.

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 <1>);

<1> 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.

2) обращение к услугам специализированного рекламного агентства, которое размещает баннеры на определенных сайтах;

3) баннерообменные сети.

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 ("комиссии системы"), оговоренной заранее, которую баннерообменная сеть получает от каждого участника и может использовать для размещения баннеров коммерческих клиентов (обычно 10 - 15%). 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.

<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.

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 <1>, они принимают условия этой сети, сформулированные ее администратором, вступая тем самым в отношения с администратором сети <2>. 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 <3>. 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 безвозмездно. 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.

<1> Участник обычно даже не знает заранее, на каком именно веб-сайте будет размещен его баннер.

<2> 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>.

<3> 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.

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 <1>. Формула вычисления CTR: (количество кликов: количество показов) x 100. Например, если баннер был показан 100 раз, и только четыре человека кликнуло на него, то CTR будет $(4 : 100) \times 100 = 4\%$. Чем выше CTR, тем по общему правилу успешнее маркетинговая кампания.

<1> По мере того как баннеры стали обычным делом в Интернете 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.

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 уполномоченного лица на веб-сайтах участников такой сети.

Расценки на баннерные показы могут существенно варьироваться и зависят от размера баннера, баннерообменной сети, стоимости клика, определенной рекламодателем, и иных факторов. Цена клика формируется на основе аукциона. В первую очередь показываются наиболее доходные баннеры. Как следствие, участник - владелец сайта продает рекламные места по максимальной цене, а рекламодатели заинтересованы в повышении цены клика.

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 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.

<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.

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 <1>.

<1> См., например: Постановления Девятого арбитражного апелляционного суда от 21 января 2013 г. [N 09АП-38518/2012-АК](#) по делу [N A40-106328/12-148-1018](#); от 2 февраля 2012 г. [N 09АП-35027/2011](#) по делу [N A40-81118/11-17-698](#); Одиннадцатого арбитражного апелляционного суда от 14 марта 2013 г. по делу [N A65-25522/2012](#); ФАС Северо-Кавказского округа от 20 сентября 2012 г. по делу [N A53-8701/2012](#); Семнадцатого арбитражного апелляционного суда от 14 ноября 2012 г. [N 17АП-11567/2012-АК](#) по делу [N A71-9177/2012](#).

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 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".

<1> **Постановление** Девятого арбитражного апелляционного суда от 2 августа 2011 г. N 09АП-17064/2011-АК по делу N А40-21456/11-72-121. **Определением** ВАС РФ от 2 декабря 2011 г. N ВАС-15405/11 отказано в передаче дела N А40-21456/11-72-121 в Президиум ВАС РФ для пересмотра в порядке надзора данного постановления.

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)" <1>.

<1> **Постановление** Одиннадцатого арбитражного апелляционного суда от 22 января 2013 г. по делу N А65-15781/2012.

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, 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>.

<1> **Постановление** Девятого арбитражного апелляционного суда от 23 января 2013 г. N 09АП-39458/2012 по делу N А40-51588/12-153-548.

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.

§ 4. Адресные уведомления как средство рекламы. Спам

Еще одним распространенным способом рекламы в сфере электронной коммерции является использование различного рода адресных уведомлений: рассылка электронных писем на **e-mail**, **sms**-сообщений, **push**-уведомлений <1>.

<1> Под push-уведомлениями обычно понимают краткие "всплывающие" уведомления, которые появляются на экране устройства (как правило,

мобильного телефона) и несут определенную информацию. Такая информация может представлять собой транзакционные сообщения (баланс счета, подтверждение заказа и пр.), новости, сообщения маркетингового характера. В отличие от sms-сообщений, push-уведомления приходят только тем пользователям, которые установили соответствующее приложение на свое устройство, что в большей степени обеспечивает адресный характер таких сообщений и учет волеизъявления пользователя, минимизируя риски нарушения законодательства при распространении таких сообщений. Кроме того, такие сообщения появляются сразу на экране устройства, в то время как sms-сообщения обычно помещаются в специальную папку для sms-сообщений, что обеспечивает более высокую степень восприятия информации пользователем.

Закон о рекламе содержит специальные положения, посвященные регулированию распространения рекламы по сетям электросвязи, к которым относятся сети телефонной, подвижной радиотелефонной (сотовой) связи, а также 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>.

<1> Постановление Пленума ВАС РФ от 8 октября 2012 г. N 58 "О некоторых вопросах практики применения арбитражными судами Федерального

закона "О рекламе" (п. 15).

Реклама признается распространенной без предварительного согласия абонента или адресата, если рекламодатель 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 рекламодателя. 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 возможной, но достаточно рискованной, поскольку впоследствии практически нельзя доказать не только факт его предоставления, но и предоставление его конкретным лицом - получателем рассылки <1>. При этом следует учитывать разъяснение Пленума ВАС РФ, в соответствии с которым согласие абонента на получение от конкретного лица информации справочного характера, например, о прогнозе погоды, курсах обмена валют, не может быть истолковано как согласие на получение от такого лица рекламы <2>.

<1> См., например: решение Арбитражного суда г. Москвы от 14 сентября 2011 г. N А40-1998/2011. По данному делу компания ООО "СК Софтлайн" была привлечена к ответственности за нарушение законодательства о рекламе за отправку 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.

<2> Постановление Пленума ВАС РФ от 8 октября 2012 г. N 58 "О некоторых вопросах практики применения арбитражными судами Федерального закона "О рекламе" (п. 15).

Согласно ст. 18 Закона о рекламе рекламодатель 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 отказа от рассылки, либо такая возможность должна быть обеспечена при обращении адресата по контактным данным интернет-магазина, размещенным на его веб-сайте.

Ответственность за несоблюдение положений ст. 18 Закона о рекламе несет рекламодатель. В случае применения автоматизированных сервисов рассылки это может быть как лицо, непосредственно использующее комплекс технических средств для информационной рассылки, вводя список номеров абонентов, текст сообщения, время рассылки и пр. <1>, так и лицо, являющееся оператором связи, особенно sms-сообщений широкому кругу лиц <2>. Провайдер соответствующего сервиса не является рекламодателем. При этом местом и временем совершения правонарушения является место и время получения каждым конкретным абонентом соответствующей рекламы, даже если она носит идентичный характер. В связи с этим соответствующее правонарушение всегда подведомственно одному

конкретному территориальному органу ФАС РФ <3>.

<1> См.: решение Арбитражного суда Новосибирской области от 24 августа 2012 г. по делу N А45-21343/2012.

<2> [Разъяснения](#) ФАС РФ от 14 июня 2012 г. "О порядке применения статьи 18 Федерального закона "О рекламе".

<3> [Письмо](#) ФАС РФ от 4 июня 2013 г. N АК/21587/13 "О порядке применения части 1 статьи 18 Федерального закона "О рекламе".

Одной из основных проблем, связанных с применением положений [ст. 18](#) Закона о рекламе, является необходимость их системного толкования с понятием "реклама", которая, как отмечалось ранее, представляет собой информацию, адресованную неопределенному кругу лиц. Формальное толкование понятия "реклама" приводит к тому, что наличие в сообщении обращения к конкретному лицу не позволяет квалифицировать его как рекламу и выводит его из-под действия требований [Закона](#) о рекламе, в том числе о распространении рекламы по сетям электросвязи. Существует практика УФАС РФ, разделяющая данный подход <1>. Не добавляют ясности и разъяснения ФАС РФ по данному вопросу, согласно которым "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. Таким образом, под рекламой понимается определенная

неперсонифицированная информация, направленная на продвижение определенного объекта рекламирования, даже если она направляется по определенному адресному списку" <2>. Соответственно, как только информация, направленная на продвижение определенного объекта рекламирования, становится персонифицированной, т.е. отправляется конкретному лицу, она не может быть квалифицирована в качестве рекламы. Как следствие, на нее не должны распространяться требования ст. 18 Закона о рекламе и ответственность за их несоблюдение. Вряд ли с таким подходом можно согласиться, учитывая, что в условиях современных информационных технологий обеспечить "адресный подход" к распространению рекламы, сопроводив ее упоминанием имени адресата, не составляет особого труда. Например, набирающие в последнее время все большую популярность push-уведомления рекламного характера в силу архитектуры лежащей в их основе инфраструктуры (необходимость наличия приложения, устанавливаемого на устройство, которое, как правило, закреплено за конкретным пользователем; регистрация такого приложения и т.п.) зачастую имеют персонализированный характер.

<1> См., например: Постановление УФАС РФ по г. Санкт-Петербургу от 9 ноября 2012 г. N 09/13527э. URL: www.geektimes.ru/post/159473.

<2> [Разъяснения](#) ФАС РФ от 14 июня 2012 г. "О порядке применения статьи 18 Федерального закона "О рекламе".

Примечательно, что в последнее время подразделения ФАС РФ нередко исходят из принципа

substance over form (превалирование существа над формой) и при возможной коллизии двух признаков рекламы (адресованность неопределенному кругу лиц и направленность на привлечение внимания к объекту рекламирования) отдают предпочтение второму как наиболее важному. В качестве иллюстрации данного подхода приведем следующее дело. Банк осуществлял рассылку sms-сообщений бывшему клиенту банка с целью привлечения внимания к своим продуктам. Предварительного согласия на такую рассылку от адресата получено не было. УФАС РФ привлекло банк к ответственности за нарушение положений [ст. 18](#) Закона о рекламе. Суд первой инстанции удовлетворил жалобу банка, сославшись на то, что направленное sms-сообщение не являлось рекламой, так как носило адресный характер. Однако суды последующих инстанций встали на сторону ФАС, указав, что "СМС-сообщения с предложением получить кредит на специальных условиях направлялись бывшему клиенту банка прямой адресной рассылкой по сети электросвязи в форме личного представления, имеют цель привлечь внимание и сформировать интерес к услугам банка. Лицо, которому направлялись сообщения по сети электросвязи, входит в неопределенный круг лиц возможного правоотношения, о которых заранее неизвестно, вступят ли они в конкретные правоотношения с банком по поводу предлагаемых услуг. Следовательно, информация о возможности получения кредита, содержащаяся в СМС-сообщении, отвечает признакам рекламы и является рекламой финансовых услуг банка. Клиент не давал согласие на получение рекламной информации" <1>. Данный подход представляется разумным, однако он порождает вопрос о необходимости уточнения формулировки понятия рекламы с учетом существующих информационных технологий и их возможностей, в частности, по обеспечению персонализированного и

адресного обращения к адресату сообщения.

<1> [Постановление](#) ФАС Северо-Кавказского округа от 25 ноября 2015 г. по делу N А53-9616/2015.

Спам

Несмотря на все имеющиеся в законодательстве правовые нормы, направленные на необходимость учета волеизъявления потребителя на получение сообщений рекламного характера, на практике ситуация зачастую 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. С ростом числа пользователей мобильных телефонов и смартфонов, sms-спам стал еще одной распространенной формой спама. При этом эффективность такого рода спама гораздо выше, чем в случае с **e-mail**. По некоторым данным, процент прочитанных sms-сообщений достигает 95% всех отправленных, а среднее время прочтения сообщения составляет пять минут с момента его получения <2>.

<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 г. В Интернет спам принесли юристы: первая рассылка такого рода была сделана 5 марта 1994 г. двумя юристами, рекламировавшими услуги их юридической фирмы.

<2> Леднев А. Как использовать SMS-сервисы для эффективной работы интернет-магазина // Лайфхакер. 2012. 12 января.

В целях противодействия СМС-спаму в Федеральный закон от 7 июля 2003 г. N 126-ФЗ (далее - Закон о связи) в 2014 г. <1> было введено понятие рассылки по сети подвижной радиотелефонной связи, под которой понимается автоматическая передача абонентам коротких текстовых сообщений (сообщений, состоящих из букв и (или) символов, набранных в определенной последовательности) по сети подвижной радиотелефонной связи или передача абонентам коротких текстовых сообщений с использованием нумерации, не соответствующей российской системе и плану нумерации, а также сообщений, передача которых не предусмотрена договором о межсетевом взаимодействии с иностранными операторами связи. Данное понятие включает в себя в том числе рассылку сообщений рекламного характера.

<1> Федеральный закон от 21 июля 2014 г. N 272-ФЗ "О внесении изменений в Федеральный закон "О связи".

Как видно из приведенной дефиниции понятие рассылки включает в себя (а) автоматические сообщения и (б) сообщения, направляемые с использованием "коротких" или "буквенных" номеров. Сообщения, рассылаемые с "обычных" номеров (т.е. входящих в российскую систему и план нумерации или предусмотренные договором о межсетевом взаимодействии с иностранными операторами связи), не охватываются вышеприведенным понятием рассылки.

Новая [ст. 44.1](#) Закона о связи устанавливает порядок осуществления такой рассылки. Главное условие - получение предварительного согласия абонента, выраженного посредством совершения им действий, однозначно идентифицирующих этого абонента и позволяющих достоверно установить его волеизъявление на получение рассылки. При этом презюмируется отсутствие такого согласия: рассылка признается осуществленной без предварительного согласия абонента, если заказчик рассылки или оператор связи (в зависимости от того, по чьей инициативе она была осуществлена) не докажет, что такое согласие было получено. Как отметил ФАС РФ, простое заполнение бланка/формы, не позволяющее однозначно установить и подтвердить, кто именно заполнил такую форму, не является соблюдением указанного требования ^{<1>}.

^{<1>} [Письмо](#) ФАС России от 5 декабря 2014 г. N АК/49919/14 "О применении новых положений Закона о связи для оценки правомерности рекламных рассылок".

Поскольку в соответствии с [ч. 2 ст. 44.1](#) Закона о

связи рассылка по сети сотовой связи по инициативе заказчика осуществляется на основании договора, заключенного с оператором связи, абоненту которого предназначена рассылка, такой оператор имеет правовую и техническую возможность оценить содержание сообщения, в том числе наличие у сообщения рекламного характера, и проверить у заказчика рассылки наличие согласия абонента на получение такой рассылки. В связи с этим такой оператор может призываться рекламораспространителем и быть привлеченным к ответственности за осуществление рассылок рекламного характера без согласия абонента.

Достаточно важным для пресечения sms-спама является право абонента обратиться на основании [п. 6 ст. 45](#) Закона о связи к оператору сотовой связи с требованием о прекращении передачи на его устройство коротких текстовых сообщений с указанием абонентского номера или уникального кода идентификации, которые содержатся в таких сообщениях и от получения которых абонент отказывается, за исключением сообщений, передача которых осуществляется оператором подвижной радиотелефонной связи в соответствии с законодательством РФ. По получении такого обращения оператор сотовой связи обязан прекратить рассылку по сети подвижной радиотелефонной связи на устройство абонента с абонентского номера или уникального кода идентификации, указанных в обращении абонента, без взимания какой-либо платы с абонента.

В целом данные нормы показали достаточную эффективность в борьбе с sms-спамом, не в последнюю очередь благодаря ограниченному количеству операторов сотовой связи и постоянному нахождению их "под прицелом" регуляторов. Что же касается

классического интернет-спама, которым забиваются почтовые ящики пользователей, здесь ситуация не такая радужная. Как известно, спам является одной из "болезней" Интернета, для которой пока не найдено эффективного "лекарства". Основными причинами, обуславливающими его вредоносный характер, являются:

- ухудшение пропускной способности каналов связи. По данным ЗАО "Лаборатория Касперского", по состоянию на третий квартал 2015 г. общая доля спама в почтовом трафике составила 54,2% <1>;

<1>

<http://www.securelist.com/anaysis/quarterly-spam-reports/72724/Spam-and-phishing-in-q3-2015/>

- 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 неограниченных 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

<1>;

<1> 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. N 45. 2008. P. 165 - 166.

- ущерб окружающей среде. Согласно исследованиям **McAfee** на распространение спама затрачивается порядка 33 млрд. кВт/ч, что эквивалентно количеству электричества, потребляемому 2,4 млн. американских домов <1>;

<1> The Carbon Footprint of Email Spam Report (2009) // http://www.twosides.info:8080/content/rsPDF_130.pdf.

- зачастую спам содержит недостоверную информацию, мошеннические схемы, информацию порнографического характера, непристойные высказывания или иные виды информации вредоносного характера <1>.

<1> См.: Наумов В.Б. Право и Интернет: очерки теории и практики. С. 97 - 98.

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 указанной статье также 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 <1>.

<1> См.: Наумов В.Б. [Противодействие спаму](#): российское законодательство через призму опыта США // Информационное право. 2007. N 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 почтовых отправлений и электронных сообщений лицо, распространяющее информацию, обязано обеспечить получателю такой информации возможность отказа от нее, 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).

<1> Наумов В.Б. Противодействие спаму: российское законодательство через призму опыта США.

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 <1>. Некоторые специалисты утверждают, что такой подход в большей степени соответствует ценностям свободного общества, предполагающим отсутствие необходимости получения разрешения на то, чтобы одному члену общества инициировать коммуникации с другим <2>. 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.

<1> Khong D. An Economic Analysis of Spam Law // Erasmus Law and Economics Review. N 1. 2004. P. 33.

<2> Templeton B. Problems with opt-out lists for E-mail // <http://www.templetons.com/brad-/spam/globout.html>.

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 <1>. 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.

<1> [Постановление](#) ФАС Уральского округа от 15 февраля 2011 г. N 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. N 17АП-5887/2008-АК по делу N 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, в том числе и на электронный адрес ИП Кошина без предварительного его согласия на получение рекламы".

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>.

<1> Обзор иностранного законодательства в указанной области см. в [первом издании](#) данной книги. С. 477 - 480.

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.

§ 5. Рекомендации и отзывы

Помимо классической рекламы на решения потребителей в значительной степени влияют рекомендации и отзывы других потребителей, и в особенности людей, которым они доверяют <1>. Основатель сети **Facebook** Марк Цукерберг утверждает, что "ничто так не влияет на людей, как рекомендации их друзей. Рекомендация, которой доверяют, влияет на людей в гораздо большей степени, чем самые искусно подготовленные сообщения, распространяемые в СМИ. Надежная рекомендация - Святой Грааль маркетинга" <2>. Данные исследований подтверждают, что рекомендации друзей и знакомых рассматриваются в качестве наиболее влиятельного источника информации <3>. Например, в соответствии с одним из исследований в качестве такового их воспринимают более 84% потребителей, а на 68% потребителей сильно влияют отзывы других потребителей, доступные в Интернете <4>. Особенно значительному влиянию отзывов и рекомендаций подвержен развлекательный контент (фильмы, книги, игры), причем наиболее восприимчивы к рекомендациям потребители в возрасте до 24 лет, которые являются активными пользователями Интернета и социальных сетей <5>.

<1> В англоязычной литературе такого рода сообщения нередко именуется **word of mouth**

communications, а использующие их технологии маркетинга - **buzz marketing**.

<2> <http://www.azquotes.com/quote/678720>

<3> Sprague R., Wells E. Regulating Online Buzz Marketing: Untangling a Web of Deceit // American Business Law Journal. Vol 47. N 3. 2010. URL: <http://ssrn.com/abstract=1411692>.

<4> Global Trust in Advertising and Brand Messages. The Nielsen Company. Report. 17 September 2013. URL: <http://goo.gl/Cr6ovi>.

<5> Phillips M., Rasberry S. Marketing without Advertising. N.Y.: Nolo. 2008. P. 36 - 37.

В этой связи неудивительно, что многие сайты интернет-магазинов допускают возможность оставления отзывов о реализуемых ими товарах (услугах). Например, система отзывов и рекомендаций является одним из ключевых элементов бизнес-модели интернет-магазина **Amazon.com**. За более чем 20 лет его существования на сайте накоплено несколько сотен миллионов как положительных, так и критических отзывов о товарах <1>. В таком случае потребитель становится **de facto** маркетологом в отношении товаров, реализуемых интернет-магазином.

<1> Amazon.com, Inc. v. John Does 1-1114. Complaint for damages and injunctive relief. 16.10.2015, N 15-2-25395-6 SEA. URL: <http://www.scribd.com/doc/285422882/Amazon-Complaint>.

При этом сфера распространения отзывов и рекомендаций о товарах не ограничивается только специализированными разделами интернет-магазинов. Пользователи Интернета активно делятся впечатлениями о продуктах и услугах на страницах своих блогов; рассказывают о своем опыте, ставят "лайки" и делают перепосты в социальных сетях; подробно разбирают достоинства и недостатки товаров, качество обслуживания в интернет-магазинах на тематических форумах.

Однако роль и значение рекомендаций выходят далеко за пределы отношений, связанных с дистанционной продажей товаров (услуг) посредством Интернета. В основе новых бизнес-моделей экономики "совместного использования" лежат репутационные механизмы: одни пользователи дают другим пользователям рекомендации, на основе которых коммерчески значимые решения принимают иные лица. Причем такого рода решения могут порой иметь непосредственное влияние на жизнь и здоровье людей. Например, как это имеет место в случае с рекомендациями и основанными на них рейтингами водителя такси в сервисах типа **Uber**, владельца жилого помещения в сервисах типа **Airbnb** и т.п. Вот почему вопросы, связанные с достоверностью таких рекомендаций и отсутствием манипуляций с ними, приобретают важное значение не только для поддержания доверия в электронной коммерции сети Интернет, но и для защиты жизни, здоровья и имущества потребителей.

Возможные злоупотребления, связанные с рекомендациями и отзывами на товары в Интернете, можно разделить на две большие группы: 1) наличие информации, не соответствующей действительности; 2) подготовка отзывов и рекомендаций по заказу

производителей или продавцов товара, что может влечь их необъективность.

Для того чтобы определить, каким образом можно противодействовать такого рода недобросовестным практикам, нужно разграничить ситуации, когда рекомендации и отзывы являются составной частью классической рекламы, и случаи, где рекомендации и отзывы выражены вовне как частное мнение лица и не сопровождаются какими-либо сообщениями рекламного характера, исходящими от производителя или продавца товара (услуги).

В первом случае правовая оценка вышеуказанных практик должна осуществляться в рамках [Закона](#) о рекламе, а сама реклама, сопровождающаяся недостоверными или иным образом вводящими в заблуждение рекомендациями или отзывами потребителей, может рассматриваться в качестве ненадлежащей, например, на основании [ч. 3 ст. 5](#) Закона о рекламе, когда такие рекомендации или отзывы содержат не соответствующие действительности сведения о характеристиках, потребительских свойствах товара (услуги) или других характеристиках, связанных с ним. Представляется, что в качестве недостоверной может признаваться и реклама, которая хотя и не содержит не соответствующих действительности сведений о самом товаре (услугах), но включает в себя рекомендации физических или юридических лиц относительно объекта рекламирования либо его одобрения физическими или юридическими лицами, которого на самом деле такие лица не давали. Поскольку информация, являющаяся составной частью рекламного сообщения и представляющая собой рекомендации или отзывы других лиц, оказывает влияние на выбор потребителя,

манипулирование такого рода сведениями может рассматриваться в качестве ненадлежащей рекламы.

Ситуации второго типа являются более сложными для правового анализа. С одной стороны, в том случае, когда соответствующая рекомендация или отзыв представляют собой **мнение частного лица**, говорить о том, что они сами по себе носят рекламный характер, и распространять на них положения законодательства о рекламе вряд ли возможно. В современных условиях, когда каждый пользователь сети Интернет может выступать в качестве потребителя и производителя информации, распространение на публикуемую им информацию положений законодательства о рекламе исключительно по причине относимости такой информации к определенному товару или продавцу означает чрезмерное ограничение конституционного права на свободный поиск, производство и распространение информации (**ч. 4 ст. 29 Конституции РФ**). Если размещение частным лицом в Интернете информации, связанной с товаром, опытом его приобретения или эксплуатации, будет для него сопряжено с возможной ответственностью за несоблюдение законодательства о рекламе, это существенным образом скажется на количестве и качестве комментариев и отзывов в Интернете, поскольку многие пользователи предпочтут либо не писать ничего, либо же под воздействием эмоций будут писать только негативные отзывы. Как следствие, может получиться так, что большая часть информации о товаре будет сводиться к ее "классической" рекламе, а также "стерильным" или негативным отзывам потребителей. Все это в конечном счете окажет "сковывающее" (**chilling**) влияние на информационное пространство в сети Интернет, существенно снизит уровень информированности потребителей и еще более

усилит информационную асимметрию между потребителями и предпринимателями.

С другой стороны, нельзя не учитывать того значения, которое отзывы и рекомендации имеют в современном коммерческом обороте. Игнорирование недобросовестных практик при их использовании создает большой пробел в законодательстве о рекламе, предоставляя неограниченные возможности для использования стелс-маркетинга, при котором маркетологи организуют диалог с потенциальными потребителями таким образом, что источник и бенефициар такой коммуникации скрыты от них <1>. Как известно, множество источников, рекомендующих один и тот же продукт, выглядят для потребителя гораздо убедительнее, чем информация из одного источника, даже будучи повторенной множество раз <2>. Поэтому манипулирование мнением потребителей посредством использования ряда блогеров и известных интернет-сайтов с отзывами является весьма привлекательной маркетинговой стратегией. Возможный вред для потребителей от нее является вполне очевидным, поскольку вследствие нее они получают экономический ущерб от приобретения товаров, которые не отвечают их нуждам или интересам. Даже в США, где проблематика обеспечения свободы слова носит явно конституционный характер, распространение информации, носящей ложный или вводящий в заблуждение характер, не пользуется охраной [Первой поправки](#) к Конституции США <3>.

<1> Sprague R., Wells E. Regulating Online Buzz Marketing: Untangling a Web of Deceit // American Business Law Journal. Vol 47. N 3. 2010. URL:

<http://ssrn.com/abstract=1411692>.

<2> Roggeveen A., Johar G., Perceived Source Variability Versus Familiarity: Testing Competing Explanations for the Truth Effect // Journal of Consumer Psychology. N 12. 2002. P. 87.

<3> Верховный суд США прямо указал, что "информация, составляющая ложные или вводящие в заблуждение сведения, не пользуется какой-либо охраной в рамках [Первой поправки](#) к Конституции США". См.: Central Hudson Gas & Electric Corp. v. Public Service Comm'n, 447 U.S. 557, 593 (1980).

Американское право требует обязательного указания на то, что лицо, предоставляющее рекомендации или отзыв, имеет определенные связи с производителем (распространителем) товара, которые могут повлиять на их объективность <1>. В частности, если между блогером и рекламодателем есть отношения, имеющие существенный экономический подтекст (например, дорогостоящий товар, выступающий предметом обзора в персональном блоге, был предоставлен продавцом-рекламодателем бесплатно), такой блогер должен сообщить в своем материале об их существовании. При этом на рекламодателя может быть возложена ответственность, если он не проинструктировал автора отзыва или рекомендации о необходимости раскрытия соответствующих отношений, а при обнаружении факта невыполнения им данной обязанности не предпринял разумных усилий по устранению этого нарушения. В данном случае, как отмечается в литературе, должны применяться те же подходы, что и в случаях, когда на рекламодателя возлагается ответственность за рекламу, создание которой было делегировано

третьему лицу с предоставлением широкого усмотрения в процессе творческой реализации <2>. В США уже имеется успешный опыт преследования недобросовестных практик, связанных с использованием проплаченных отзывов и рекомендаций. Так, по иску прокуратуры штата Нью-Йорк 19 компаний, воспользовавшихся так называемыми услугами по управлению репутацией, были привлечены к ответственности за недобросовестную и мошенническую практику (**deceptive act practice**), общая сумма наложенных на них штрафов составила 350 тыс. долл. <3>.

<1> См. § 255.5 of FTC Guides Concerning Use of Endorsements and Testimonials in Advertising. Electronic Code of Federal Regulations. Part 255. URL: <http://goo.gl/XeVC3a>.

<2> Tushnet R. Attention Must be Paid: Commercial Speech, User-Generated Ads, and the Challenge of Regulation // Buffalo Law Review N 58. 2010. P. 760.

<3> A.G. Schneiderman Announces Agreement with 19 Companies to Stop Writing Fake Online Reviews and Pay more than \$350,000 in Fines. Website of New-York Attorney General. 23 September 2013. URL: <http://goo.gl/oq59I3>.

Рекомендации ОЭСР по защите прав потребителей в сфере электронной коммерции во многом инкорпировали подход США и содержат специальные положения, устанавливающие необходимость обеспечения достоверности одобрительных комментариев других лиц, содержащихся в рекламе. При этом наличие любой

существенной связи между блогером или иным пользователем сети Интернет, оставившим соответствующий отзыв, которая может повлиять на объективность и восприятие отзыва, должно быть в явной форме раскрыто <1>.

<1> См. § 17 Consumer Protection in E-commerce: OECD Recommendation. 2016. Paris.

Схожая обязанность, хотя и не столь подробно описанная, существует и в европейском праве, запрещающем недобросовестные коммерческие практики, в том числе скрытого характера, даже если сама информация является фактически корректной <1>.

<1> European Commission Guidance on the Implementation/Application of Directive 2005/29/ EC on Unfair Commercial Practices. 2009. P. 8, 31. URL: http://ec.europa.eu/justice/consumer-marketing/files/ucp_guidance_en.pdf.

Считается, что такое указание позволяет обозначить возможную предвзятость рекомендации или отзыва и снизить их убеждающий ("активирующий") потенциал, ведь согласно исследованиям, люди более склонны верить источникам информации, которые не имеют видимой связи с производителем или продавцом товара <1>. Представим себе ситуацию, когда потребитель выбирает отель для проведения отпуска, изучает различные варианты и склоняется к одному из них вследствие отзывов, размещенных на интернет-сайте. Его решение могло бы быть иным, если бы он знал, что владелец отеля заплатил за написание

данных отзывов или предоставлял привилегии их авторам, например, бесплатное проживание.

<1> Goldman E. Peer Promotions and False Advertising Law // South Carolina Law Review. N 58. 2007. P. 705.

Регулирование вопросов, связанных с достоверностью отзывов на веб-сайтах, осуществляется и на уровне судебной практики. Так, в одном из решений Верховный суд Германии указал на наличие обязанности владельца медицинского портала осуществлять мониторинг отзывов, оставляемых посетителями. Особенно это касается оставляемых анонимно отзывов, в отношении которых поступили жалобы от врачей или из клиник относительно их недостоверности <1>. По сути такого рода требования фактически вынуждают владельцев интернет-портала внедрять специальные политики модерирования отзывов и управления поступающими жалобами, в некоторой степени схожие с теми, которые обеспечивают претензионный порядок в отношениях, связанных с защитой исключительных прав.

<1> BGH, Urteil N VI ZR 34/15, 1 March 2016.

Большие проблемы создают некоторые онлайн-платформы (типа **Fiverr**, **Kwork**), позволяющие нанять фрилансеров для проставления "лайков", составления отзывов или распространения от своего имени заранее подготовленных отзывов и совершения иных действий под видом рядовых пользователей. В итоге распространяются отзывы и рекомендации,

содержащие недостоверную информацию либо же создающие впечатление наличия положительного мнения большинства пользователей о соответствующем товаре (продавце), на основании которого принимают коммерчески - значимые решения множество пользователей Интернета.

Борьба с такого рода недобросовестными практиками может вестись различными методами и их сочетаниями: техническими, договорно-правовыми, а также методами правового преследования недобросовестных авторов отзывов и их заказчиков.

Так, многие правила использования интернет-сайтов, допускающих размещение отзывов потребителей, содержат запрет на оставление платных отзывов. Например, правила интернет-магазина **Amazon.com** устанавливают запрет на размещение отзывов и оценок товара, сделанных в обмен на компенсацию любого рода, включая предоставление подарочных сертификатов, бонусного контента, допуска к различного рода мероприятиям, скидки на будущие покупки и пр. При этом допускается написание отзыва в обмен на предоставление бесплатного экземпляра товара или со скидкой, при условии, что автор отзыва прямо укажет о данном факте в своем отзыве <1>. Поскольку соответствующее соглашение является гражданско-правовым договором, его нарушение является основанием для применения мер гражданско-правовой ответственности, включая возмещение убытков, как минимум, в виде выгоды, которую нарушитель получил (см. [абз. 2 п. 2 ст. 15 ГК РФ](#)). Кроме того, возможно расторжение соответствующего соглашения, что на практике означает удаление соответствующего аккаунта пользователя.

<1> Amazon Customer Review Creation Guidelines.
URL: <https://goo.gl/zmYQzv>.

С технической точки зрения противодействие размещению массовых заказных отзывов и рекомендаций могут оказать различного рода **антифрод-системы**, идентифицирующие подозрительные модели поведения пользователей (например, появление множества отзывов с одного IP-адреса или с одного недавно зарегистрированного аккаунта), а также внедрение специальных указаний на то, что автор отзыва является действительным покупателем рецензируемого товара (**verified purchase**)

.

Возможности преследования авторов заказных отзывов и рекомендаций за нарушение законодательства о рекламе весьма ограничены в условиях отсутствия в российском законодательстве нормы о прямой обязанности автора раскрывать наличие существенной экономической связи между ним и производителем (распространителем) товара, подобной той, которая есть в европейском и американском законодательстве. Вместе с тем потенциально возможно привлечение к ответственности заказчика такого рода отзывов и рекомендаций за недобросовестную конкуренцию, за введение в заблуждение по [ст. 14.2](#) Закона о защите конкуренции. Представляется, что все основные признаки недобросовестной конкуренции, перечисленные в [п. 9 ст. 4](#) указанного Закона и уже рассмотренные ранее, в данном случае присутствуют.

В перспективе все же целесообразно

рассмотреть вопрос о "введении" отношений по использованию заказных рекомендаций и отзывов в сети Интернет в правовое поле. Как вариант, размещение оплаченных отзывов и рекомендаций объекта рекламирования под видом мнения нейтрального и незаинтересованного специалиста или потребителя может рассматриваться в качестве разновидности недобросовестной рекламы. К ответственности за нее могут привлекаться как заказчик (рекламодатель), в интересах которого соответствующие отзывы и рекомендации распространяются, так и организация, которая обеспечивает практическое выполнение данного заказа. Можно также рассмотреть возможность возложения ответственности за опубликование "оплаченных" отзывов и рекомендаций без раскрытия факта наличия отношений с заказчиком на известных блогеров, поскольку вследствие наличия у них большой аудитории подписчиков и определенной репутации их оценки обладают особым влиянием и занимают высокие строчки в поисковой выдаче различных поисковых систем Интернета. При этом в качестве отправной точки можно использовать положения [ст. 10.2](#) Федерального закона "Об информации, информационных технологиях и защите информации", дополнив их положением об обязанности блогеров сообщать о наличии экономических взаимоотношений с производителями или продавцами товаров, которые могут повлиять на восприятие объективности их оценок и мнений третьими лицами. Безусловно, само по себе это не решит всех проблем, вызванных распространением заказных отзывов и рекомендаций в сети Интернет, но, по крайней мере, это может стать первым шагом для обозначения факта наличия таких проблем и необходимости их решения. В целом же вопрос о выработке адекватного правового ответа на проблему

заказных отзывов и рекомендаций требует дальнейшего тщательного анализа и проработки, которые будут предприняты автором в последующих изданиях настоящей книги.

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 дефицита внимания со стороны пользователей, обусловленных беспрецедентным многообразием информации, размещенной в ней, можно сказать, что любой клиент 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) <1>. 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 для традиционных офлайновых компаний, которыми они до этого не обладали) 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 свести к минимуму. 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> Нередко пользовательские данные сравнивают с новой "нефтью". Еще в 1995 г. бывший глава компании **Intelsat** Ирвин Голдштейн (**Irving Goldstein**) предсказывал, что информация будет для

экономики XXI в. выполнять ту же роль, что нефть и газ - для экономики начала XX в. (см.: U.S. Foreign Affairs in the New Information Age: Charting a Course for the 21st Century. Washington, D.C.: Annenberg Washington Program in Communications Policy Studies of Northwestern University, 1994, URL: www.annenberg.northwestern.edu/pubs/usfa). В 2009 г. европейский комиссар по защите прав потребителей Меглена Кунева (**Meglana Kuneva**) развила данную мысль, заявив, что "персональная информация является новой нефтью Интернета и валютой в цифровом мире" (Meglana Kuneva. Keynote Speech.Roundtable on Online Data Collection, Targeting and Profiling, Brussels, 31 March 2009. URL: www.europa.eu/rapid/press-release_SPEECH-09-156_en.pdf). А после доклада Мирового экономического форума 2011 г. отождествление персональных данных с "новой нефтью" популяризировалось окончательно. См.: Personal Data: The Emergence of a New Asset Class. World Economic Forum, January 2011. URL: <http://www.weforum.org/reports/personal-data-emergence-new-asset-class>.

§ 1. История появления законодательства 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.

<1> Войниканис Е. [Указ. соч.](#) С. 199.

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 <1>.

<1> Greenleaf G. Global Data Privacy Laws: 89 Countries, and Accelerating // Privacy Laws & Business International Report. N 115. February 2012; Queen Mary School of Law Legal Studies Research Paper N 98/2012. <http://ssrn.com/abstract=2000034>.

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 приняли отдельные законы, посвященные регулированию персональных данных. Впоследствии национальное законодательство было гармонизировано

рядом директив ЕС, в числе которых следует упомянуть [Директиву](#) N 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](#) N 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 N 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> и в конечном счете была признана недействительной Европейским судом справедливости как нарушающая вследствие своих неопределенных и чрезмерно широких формулировок фундаментальное право на частную жизнь <5>.

<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> Digital Rights Ireland and Seitlinger and Others, ECJ, Joined Cases C-293/12 and C-594/12, 8 April 2014. Несмотря на это, национальное законодательство большинства стран ЕС продолжает сохранять большую часть положений, имплементированных из данной Директивы, хотя и с некоторыми уточнениями, принятыми после вынесения вышеуказанного решения Европейского суда справедливости.

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 <1>. В настоящее время завершена 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 распространение социальных сетей, облачных вычислений и т.п.). Наиболее важные новеллы

указанного регламента будут рассмотрены далее.

<1> Подробный компаративный анализ см.: Data Protection Laws in the EU. European Commission Working Paper. N 2. 20 January 2010. URL: <http://goo.gl/Y76pSc>.

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 <1>, проката видеофильмов <2>, финансовых услуг <3>, защиты данных автовладельцев <4>, защиты персональных данных малолетних лиц в сети Интернет <5> и ряда иных тематических законов, принятых как на федеральном уровне, так и на уровне отдельных штатов <6>. Немалую роль играют и акты рекомендательного характера <7>.

<1> The US Health Insurance Portability and Accountability Act of 1996.

<2> The US Video Privacy Protection Act of 1988.

<3> The US Financial Services Modernization Act of 1999.

<4> The US Drivers Privacy Protection Act of 1994.

<5> The Children's Online Privacy Protection Act of 1998.

<6> См., например: the California Online Privacy Protection Act of 2003 (OPPA); the Massachusetts General Law Chapter 93H & 201 CMR 17.00 Regulations of 2010.

<7> NIST Guide to Protecting the Confidentiality of Personally Identifiable Information (PII) NIST Special Publication 800-122. April 2010 // <http://csrc.nist.gov/publications/nist-pubs/800-122/sp800-122.pdf>.

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 <1>. Не последнюю роль в отсутствии 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 Principles**) для обеспечения информированности пользователя о судьбе его персональных данных <2>. Наконец, еще одной причиной нежелания США комплексно подходить к проблеме защиты персональных данных в сети Интернет является позиция американских корпораций, активно лоббирующих свои интересы в американском правительстве. Для компаний вроде **Google** открытый Интернет, максимально свободный от различного рода

обременений в виде локального регулирования информационных процессов, является ключевой основой всей бизнес-модели и условием дальнейшего развития <3>.

<1> Metille S. Swiss Information Privacy Law and the Transborder Flow of Personal Data // Journal of International Commercial Law and Technology. N 8. 2013. P. 71.

<2> 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. N 39. 2004. P. 183 - 184.

<3> Jablonsky M., Powers S. The Real Cyber War: The Political Economy of Internet Freedom. University of Illinois Press. 2015. Неудивительно, что Google не жалеет средств на лоббирование своей позиции, являясь одним из лидеров по затратам в данной области. Ch.: Sankin A. Google Spends more on Lobbying than any other Company // The daily dot. 22 April 2015. URL: <http://goo.gl/lddFPX>.

Неудивительно, что в условиях столь "лоскутного" законодательства существует большой разноречивой 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 <1>. Как следствие, США еще до разоблачений Эдварда Сноудена не рассматривались в качестве страны, обеспечивающей надлежащий уровень защиты персональных данных с точки зрения европейского законодательства что потребовало выработки специальных принципов (**safe**

harbor), присоединение к которым до недавнего времени обеспечивало соответствующей американской компании статус поддерживающей должный уровень защиты для целей европейского законодательства о защите персональных данных. Эти принципы были утверждены Европейской комиссией в 2000 г., однако в конце 2015 г. они были признаны недействительными Европейским судом справедливости, поскольку в свете разоблачений Эдварда Сноудена - рассекречивания им сведений о программах массовой слежки американских спецслужб - принципы **Safe Harbor** более нельзя рассматривать, по мнению Суда, в качестве надежного основания для обеспечения защиты персональных данных европейских граждан при их трансграничной передаче в США <2>. Правда, вопреки представлениям некоторых отечественных специалистов и чиновников, вынесение данного решения отнюдь не означает, что трансграничная передача персональных данных из стран ЕС в США стала невозможной. Просто исчезло одно из специальных оснований для осуществления такой передачи в отсутствие согласия самого субъекта персональных данных, но остались другие основания, в частности, такая передача возможна при наличии специальных, одобренных уполномоченным органом условий в договоре между экспортером и получателем данных договоров либо при наличии корпоративных общеобязательных норм.

<1> 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.

<2> Maximillian Schrems v. Data Protection Commissioner, ECJ, C-362/14, 6 October 2015.

Как видно, в части законодательства о защите персональных данных США не являются 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. <1>, 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. N 152-ФЗ "О персональных данных" (далее - Закон о персональных данных).

<1> Федеральный [закон](#) от 19 декабря 2005 г. N 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.

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 <1> ([ст. 1](#)).

<1> 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 данная сфера не представляет собой интереса в контексте проблематики электронной коммерции, поэтому не будет рассматриваться далее.

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 <1>; 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. Конечно, это справедливо с учетом положений о сфере действия данного [Закона](#) в пространстве и по кругу лиц (см. подробнее § 4.2 гл. 2 настоящей книги).

<1> Под обработкой персональных данных для личных и семейных нужд в рамках указанного исключения подразумеваются действия физического лица по формированию массива данных, предоставленных им третьими лицами, в том числе с использованием личных электронных устройств, личной электронной почты. Это могут быть списки контактов в мобильных телефонах, визитки, список пользователей в коммуникационных сервисах. См.: Федеральный закон "О персональных данных": Научно-практический [комментарий](#) / Под ред. зам. руководителя Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций А.А. Приезжевой. М., 2015. С. 10.

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. Например, загрузка персональных данных на страницу сайта в Интернете также может признаваться обработкой персональных данных <1>.

<1> Европейский суд справедливости уже дважды высказал данную позицию. См.: **Lindqvist**, C101/01; **Google Spain and Google**, C131/12. В силу схожести

определений понятия "обработка персональных данных" в европейском и российском праве данный подход вполне может быть применим и в России.

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 определенному или определяемому физическому лицу (субъекту персональных данных)" (п. 1 ст. 3 Закона о персональных данных). В связи с данной дефиницией необходимо отметить следующее.

1. 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 многом это связано с тем, что основной вид персональных данных юридического лица - фирменное наименование - обладает защитой в рамках специального правового режима, а данные о представителях юридического лица - физических лицах охватываются общим правовым режимом законодательства о персональных данных. Кроме того, отнесение юридических лиц к числу субъектов персональных данных могло бы повлечь негативные последствия для коммерческого оборота как посредством создания дополнительных условий для недобросовестной конкуренции, так и вследствие дополнительных ограничений на трансграничный обмен информацией.

2. Для того чтобы признаваться персональными

данными, соответствующие сведения должны обладать определенным идентифицирующим потенциалом. В связи с этим возникает главный вопрос всего законодательства о персональных данных: **при каких условиях** информация, имеющая отношение к физическому лицу, приобретает статус персональных данных?

Можно выделить два основных подхода к решению данного вопроса: 1) "узкий", исходя из которого только информация, позволяющая однозначно идентифицировать конкретное физическое лицо, может быть квалифицирована в качестве персональных данных; и 2) "широкий", исходя из которого любая информация, имеющая отношение к физическому лицу и позволяющая как-то выделить его из общей массы людей, может быть квалифицирована в качестве персональных данных.

Очевидным преимуществом первого подхода является его практичный характер, обеспечивающий определенную степень предсказуемости и определенности законодательства в указанной сфере. Это облегчает жизнь операторам и правоприменительным органам, в связи с чем не должна вызывать удивления его апология отдельными чиновниками Роскомнадзора <1> и практикующими юристами <2>. Если рассматривать вопрос с практической точки зрения, то из первого подхода следует, например, что персональными данными являются сведения, фактически представляющие собой "анкетные данные": Ф.И.О. + место регистрации; Ф.И.О. + номер мобильного телефона; Ф.И.О. + дата рождения; Ф.И.О. + государственный идентификатор (типа ИНН, СНИЛС, номер паспорта). Кроме того, в качестве персональных данных может быть

квалифицирована информация, которая прямо названа в качестве таковой в нормативных актах, например, геномная информация <3>, дактилоскопическая информация <4>. И наоборот, как отмечается в комментарии представителей Роскомнадзора, "к числу данных, которые не могут рассматриваться, по крайней мере, по отдельности друг от друга в качестве персональных, могут быть отнесены: фамилия, имя, отчество <5>, адрес проживания, электронный адрес, номер телефона, дата рождения. Другие идентификаторы сами по себе не определяют однозначно конкретное физическое лицо. Такие данные должны быть отнесены к персональным данным только в том случае, если они хранятся и обрабатываются совместно с идентификаторами, которые сами по себе определяют физическое лицо" <6>.

<1> Данная позиция отражена в ряде выступлений и ответов на вопросы отдельных чиновников Роскомнадзора на различного рода конференциях и в иных публичных выступлениях, а также из комментария, опубликованном под редакцией А.А. Приезжевой. См.: Федеральный закон "О персональных данных": Научно-практический комментарий / Под ред. зам. руководителя Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций А.А. Приезжевой. С. 15 - 17.

<2> См., например: Архипов В.В. Понятие персональных данных: динамика определения и его интерпретации в условиях развития информационно-телекоммуникационных технологий: Материалы международной конференции "Защита

персональных данных" 11 ноября 2015 г. URL: <http://zpd-forum.com/programm.html>.

<3> Геномная информация - персональные данные, включающие кодированную информацию об определенных фрагментах дезоксирибонуклеиновой кислоты физического лица (ч. 3 ст. 1 Федерального закона от 3 декабря 2008 г. N 242-ФЗ "О государственной геномной регистрации в Российской Федерации"). Данный вид информации в будущем будет иметь достаточно важное значение для целей развития электронной медицины и трансграничных научных исследований. Уже существуют организации, которые на началах саморегулирования вырабатывают политики в указанной области. См., например: Концепция ответственного обмена геномными данными и данными, связанными со здоровьем человека. 10 сентября 2014 г. Глобальный альянс в сфере геномной информации и здоровья. URL: <https://goo.gl/gbaFfj>.

<4> Дактилоскопическая информация - биометрические персональные данные об особенностях строения папиллярных узоров пальцев и (или) ладоней рук человека, позволяющие установить его личность (ст. 1 Федерального закона от 25 июня 1998 г. N 128-ФЗ "О государственной дактилоскопической регистрации в Российской Федерации").

<5> Данный вывод встречается и в других источниках. См., например: Обзор обращений граждан за II квартал 2012 года в Управление Роскомнадзора по Республике Карелия, где указано: "Ф.И.О. (фамилия, имя, отчество) наряду со многими другими способами используются для идентификации отдельного человека среди других. По своей природе это составной ключ, идентификатор, основанный на комбинациях трех

параметров фамилии, имени и отчества, на самом деле не идентифицирующий человека однозначно, а лишь сильно сокращающий выборку из тех, кому они могут принадлежать" URL: http://10.rkn.gov.ru/queries/lookup/people_2kv_2012/p1/.

<6> См.: Федеральный закон "О персональных данных": Научно-практический [комментарий](#) / Под ред. зам. руководителя Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций А.А. Приезжевой. С. 17.

Иным, даже более важным следствием применения узкого подхода к рассматриваемому вопросу является необходимость признания любых данных, не идентифицирующих конкретное лицо, в качестве обезличенных данных, на обработку которых не распространяется законодательство о персональных данных <1>.

<1> Собственно, именно такой вывод напрашивается по результатам анализа Методических [рекомендаций](#) по применению Приказа Роскомнадзора от 5 сентября 2013 г. N 996 "Об утверждении требований и методов по обезличиванию персональных данных", утвержденных руководителем Роскомнадзора 13 декабря 2013 г. В частности, это особенно явно следует из приведенного в указанном документе понятия "деобезличивание", определенного как "действия, в результате которых обезличенные данные принимают вид, позволяющий определить их принадлежность конкретному субъекту персональных данных, то есть становятся персональными данными" (выделено мной. - **А.С.**).

Признавая наличие логики и политико-правовой целесообразности такого подхода, следует заметить, что он весьма не бесспорен с точки зрения его нормативного обоснования. По сути, он ограничивает понятие персональных данных лишь той информацией, которая прямо относится к определенному физическому лицу (в англоязычной терминологии - **identified person**), и игнорирует наличие в дефиниции прямого указания на то, что персональными данными в равной степени признается и информация, которая косвенно относится к определяемому лицу (**identifiable person**). Таким образом, "узкий" подход к понятию персональных данных не имеет прочных оснований в действующем законодательстве, а те акты, в которых он находил свое отражение, либо утратили силу, либо имеют подзаконный статус <1>.

<1> Да и фамилия, имя, отчество вопреки комментариям представителей Роскомнадзора вполне могут признаваться персональными данными непосредственно в силу указания самого [Закона о персональных данных](#). Так, в соответствии с [п. 5 ч. 2 ст. 22](#) данного Закона оператор вправе осуществлять без уведомления Роскомнадзора "обработку персональных данных... **включающих только фамилии, имена и отчества субъектов персональных данных**" (выделено мной. - **А.С.**). Из данного положения вполне можно сделать вывод о том, что только фамилия, имя и отчество лица, безотносительно к степени их распространенности, признаются персональными данными. Некоторые суды также полагают, что Ф.И.О. являются персональными данными. См., например: Апелляционное [определение](#) Московского городского суда от 6 сентября 2012 г. по делу N 11-17136, в

котором указано, что "ссылка ответчика на то обстоятельство, что фамилия, имя и отчество не являются персональными данными, не может быть принята во внимание как противоречащая действующему законодательству, так как, исходя из положений п. 1 ст. 3 ФЗ от 27 июля 2006 г. N 152-ФЗ "О персональных данных", персональные данные - любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных)".

Так, в одном из первых определений персональных данных содержался данный признак. В соответствии со ст. 2 Федерального закона от 20 февраля 1995 г. N 24-ФЗ "Об информации, информатизации и защите информации" под персональными данными понимались "сведения о фактах, событиях и обстоятельствах жизни гражданина, позволяющие идентифицировать его личность". Этот Закон утратил силу с 8 августа 2006 г., с момента вступления в силу нового Закона об информации. Трудовой кодекс РФ также в течение некоторого времени содержал дефиницию персональных данных работника, в которой был отражен признак идентифицируемости - "информация, необходимая работодателю в связи с трудовыми отношениями и касающаяся конкретного работника" (ст. 85 ТК РФ). Однако и это положение утратило силу в 2013 г. <1>.

<1> Федеральный закон от 7 мая 2013 г. N 99-ФЗ "О внесении изменений в отдельные законодательные акты Российской Федерации в связи с принятием Федерального закона "О ратификации Конвенции Совета Европы о защите физических лиц при

автоматизированной обработке персональных данных" и Федерального закона "О персональных данных".

Но наиболее показательны изменения, произошедшие в формулировке дефиниции персональных данных, содержащейся в самом [Законе](#) о персональных данных. Ранее, до 27 июля 2011 г., она выглядела следующим образом: "...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 (выделено мной. - **А.С.**)". Действующая формулировка такова: "...любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных)". Как видно, основным отличием новой дефиниции является исключение из нее слов "на основании такой информации", а также отсутствие перечня возможных видов персональных данных, что было компенсировано включением оговорки о том, что информация может относиться к субъекту прямо или косвенно. Эти изменения свидетельствуют о трансформации отношения законодателя к понятию "персональные данные": оно стало гораздо более широким, а также контекстно-ориентированным. Вопрос о квалификации информации в качестве персональных данных стал зависеть от конкретных обстоятельств и возможных взаимосвязей между различного рода фрагментами информации.

Единственным актом, в котором остались признаки идентифицируемости субъекта персональных данных, является Указ Президента РФ от 6 марта 1997

г. N 188 "Об утверждении перечня сведений конфиденциального характера", который к числу таких сведений относит, в частности, "сведения о фактах, событиях и обстоятельствах частной жизни гражданина, позволяющие идентифицировать его личность (персональные данные)" (п. 1). По мнению В.В. Архипова, данный [Указ](#) при системном толковании с дефиницией персональных данных, содержащейся в настоящее время в [Законе](#) о персональных данных, позволяет сделать вывод о сохранении в российском законодательстве признака идентифицируемости субъекта как необходимого условия квалификации данных в качестве персональных <1>. Это мнение представляется спорным в силу как минимум двух причин. Во-первых, с учетом иерархии нормативных актов указ Президента РФ по своему статусу ниже федерального закона, поэтому дефиниция [Закона](#) о персональных данных уже в силу этого имеет приоритет в случае возможной конкуренции с дефиницией, содержащейся в этом [Указе](#). Во-вторых, [Закон](#) о персональных данных, будучи всецело посвященным одному конкретному виду конфиденциальной информации, имеет статус **lex specialis** по отношению к рассматриваемому [Указу](#), который регламентирует виды конфиденциальной информации в общем.

<1> Архипов В.В. Понятие персональных данных: динамика определения и его интерпретации в условиях развития информационно-телекоммуникационных технологий: Материалы международной конференции "Защита персональных данных" 11 ноября 2015 г.

Тем не менее анализ судебной практики позволяет сделать вывод о том, что большая часть

судов разделяет именно "узкий" подход. Так, суды не признают конфиденциальной информацией ИНН <1>, СНИЛС <2>, номер паспорта <3>, поскольку, по их мнению, по такой информации нельзя идентифицировать конкретное лицо. В одном деле, например, суд и вовсе пришел к выводу об отсутствии нарушений [Закона](#) о персональных данных, "поскольку запрашиваемая сотрудниками банка информация в отношении В., высказывания работников ответчиков не содержат персонифицированных и детализированных данных, работниками ответчиков не назывались ни адрес места проживания лица, ни год, месяц, дата и место рождения, семейное, социальное, имущественное положение, образование, профессия, доходы, а также другая информация, по которой возможно идентифицировать конкретное лицо" <4>.

<1> Апелляционное [определение](#)
Санкт-Петербургского городского суда от 3 февраля
2015 г. по делу N 2-3097/2014.

<2> Решение Белоглинского районного суда
Краснодарского края от 22 июня 2014 г. по делу N
2-300/2014 N 2-300/2014.

<3> [Определение](#) Московского городского суда от
29 февраля 2012 N 33-6709; [Постановление](#)
Тринадцатого арбитражного апелляционного суда от 21
июня 2010 г. по делу N А56-4788/2010.

<4> Апелляционное [определение](#) Московского
городского суда от 28 января 2014 г. по делу N 33-5461.

Напротив, информация, включающая Ф.И.О.
субъекта, обычно признается судами в качестве

персональных данных, например, информация о задолженности по коммунальным платежам (Ф.И.О. + адрес проживания + размер задолженности по оплате коммунальных платежей) <1>, данные в заявке на выдачу кредита (Ф.И.О. + паспортные данные + место жительства + дата рождения и т.п.) <2>, информация, содержащаяся в техническом паспорте на дом (Ф.И.О. + паспортные данные + документ о праве собственности) <3> и т.д.

<1> [Постановление](#) Нижегородского областного суда от 12 мая 2015 г. по делу N 4а-288/2015; Кассационное [определение](#) Пермского краевого суда от 1 августа 2011 г. по делу N 33-7668.

<2> Апелляционное [определение](#) Тульского областного суда от 28 апреля 2015 г. по делу N 33-850.

<3> [Определение](#) Приморского краевого суда от 28 апреля 2014 по делу N 33-3718.

Суть второго ("широкого") подхода сводится к тому, что к персональным данным можно отнести в том числе и информацию, которая сама по себе хотя и не указывает однозначно на имя конкретного лица, но содержит описание каких-либо его индивидуальных характеристик, позволяющих отграничить его от других субъектов, выделить его из круга лиц, к которому он принадлежит, или по крайней мере сузить такой круг лиц <1>. Этот подход, имеющий в своей основе возможность "косвенной" идентификации, вполне следует из существующей в России законодательной дефиниции персональных данных, которая в свою очередь основана на положениях [Конвенции](#) N 108 <2> и [Директивы](#) ЕС 95/46/ЕС "О защите персональных

данных" <3>.

<1> В некоторых странах, например в Финляндии и Норвегии, законодательство о персональных данных допускает признание информации персональными данными, даже если она относится не к конкретному индивиду, а к семье или домовладению. См.: Bygrave A. Data Privacy Law: An International Perspective. Oxford: University Press. 2014. P. 135.

<2> Персональные данные означают любую информацию об определенном или поддающемся определению физическом лице (субъект данных). См. [ст. 2 \(а\)](#) Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных СДСЕ N 108.

<3> Согласно [ст. 2 \(а\)](#) Директивы ЕС персональные данные означают любую информацию, связанную с идентифицированным или идентифицируемым физическим лицом (субъектом данных); идентифицируемым лицом является лицо, которое может быть идентифицировано прямо или косвенно, в частности, посредством ссылки на идентификационный номер или на один или несколько факторов, специфичных для его физической, психологической, ментальной, экономической, культурной или социальной идентичности.

В [п. 26 преамбулы](#) указанной Директивы даже указано, что "для определения того, является ли лицо идентифицируемым, следует принимать в расчет все средства, в равной мере могущие быть вероятно (**likely**) и разумно (**reasonably**) использованными либо оператором, либо любым иным лицом для

идентификации указанного лица". Исходя из анализа этого положения можно сделать два основных вывода: 1) в качестве идентифицирующего лица может выступать любое лицо, а не только оператор, что расширяет понятие "персональные данные", поскольку не требуется концентрироваться исключительно на анализе возможностей отдельно взятого оператора; 2) в качестве критериев, которыми надо руководствоваться при анализе вероятности отнесения данных к личности субъекта таким "любым лицом", фигурируют (а) вероятность и (б) разумность их использования. Вероятность использования должна оцениваться с учетом всех обстоятельств: к примеру, она гораздо выше у компаний, использующих продвинутые технологии анализа данных в своих бизнес-процессах (финансовые организации, организации связи, социальные сети, крупные онлайн-магазины и т.п.), чем у небольших организаций, которые не могут позволить себе использование таких технологий. Разумность по общему правилу должна предполагать возможность идентификации лица с привлечением правомерных средств, т.е., например, без взлома компьютерных систем или незаконного доступа к базам данных третьих лиц, в том числе государственных органов.

Преимуществом рассматриваемого "широкого" подхода является его гибкость, позволяющая учитывать современные технологические возможности по обработке 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 нередко называется профайлингом (**profiling**). 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 Интернете (в социальных сетях, на форумах, такими способами, как "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 расположении 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).

Таким образом, технологии **Big Data** позволяют без особых проблем идентифицировать личность конкретного лица посредством установления корреляций между несколькими фрагментами данных <1>. Любая информация об относительно уникальном качестве лица (например, о его музыкальных предпочтениях или посещенных местах) может служить основанием для "опознания" такого лица в иных базах данных. Вероятность деанонимизации в значительной степени увеличилась в связи с появлением социальных

сетей и иных веб-сайтов, где люди оставляют значительное количество информации о себе. Впрочем, практически любое действие пользователя в Интернете может служить средством приближения к идентификации его личности, поскольку оно оставляет так называемый цифровой след.

<1> Narayanan A., Shmatikov V. Robust De-Anonymization of Large Sparse Datasets // The University of Texas. 2008 IEEE Symposium on Security and Privacy. URL: https://www.cs.utexas.edu/~shmat/shmat_oak08netflix.pdf (дата обращения - 14 февраля 2015 г.); Dwork C., "Differential Privacy". ICALP'06 Proceedings of the 33rd International Conference on Automata, Languages and Programming, Berlin: Springer, 2006.

Например, в свое время компания **AOL** сделала общедоступной совокупность старых поисковых запросов с намерением дать возможность их использования в исследовательской деятельности. Набор данных из 20 млн. поисковых запросов 650 тыс. пользователей за период с 1 марта по 31 мая 2006 г. был тщательно анонимизирован: личные данные пользователей в виде имен и IP-адресов были удалены и замещены уникальными цифровыми идентификаторами. Однако на основании сопоставления различных запросов удалось установить личности ряда пользователей. Можно привести и иной пример. Известный интернет-сервис проката фильмов **Netflix** выпустил 100 млн. записей о прокате от 500 тыс. пользователей, личные идентификаторы которых были удалены, с целью проведения конкурса на улучшение системы рекомендаций фильмов. Однако, сравнив

данные от **Netflix** с иными общедоступными источниками (в частности, с данными об оценках пользователями фильмов на известном веб-сайте **IMDb**), исследователи пришли к выводу, что на основе всего шести оценок фильмов можно установить личность пользователя в 84% случаев, а зная дату оценки - с точностью 99% <1>. Особенно подвержены деанонимизации люди, пользующиеся социальными сетями за счет возможности проследить так называемый социальный граф - дружеские связи между пользователями таких сетей: исследования доказали возможность идентификации анонимных пользователей социальных сетей исключительно на основании анализа "социального графа" <2>. Возможность определения конкретной личности посредством соединения различных фрагментов информации и установления взаимосвязей между ними лежит в основе деятельности спецслужб ("принцип мозаики") <3>. Национальный институт США по стандартизации и технологиям (**NIST**) был вынужден недавно признать обоснованность высказанных опасений по поводу возможностей идентификации граждан на основании формально обезличенных фрагментов информации, а также отсутствия теоретической базы под современными методологиями обезличивания персональных данных <4>. Эти опасения приобрели еще больше оснований под собой после того, как Стэнфордский университет опубликовал исследование, согласно которому метаданные телефонных переговоров (номера телефонов абонентов, время и продолжительность звонка либо время и количество символов sms-сообщений) позволяют без особых проблем реидентифицировать личность абонента, устанавливать его связи с другими лицами, а также выводить "чувствительные" персональные данные: политические, религиозные, сексуальные взгляды и предпочтения субъекта, состояние его здоровья и ряд

других) <5>.

<1> Майер-Шенбергер В., Кукьер К. Большие данные. Революция, которая изменит то, как мы живем, работаем и мыслим. М., 2014. С. 162.

<2> Narayanan A., Shmatikov V. De-Anonymizing Social Networks. 2009. URL: <http://userweb.cs.utexas.edu/~shmat/shmat-oak09.pdf> (дата обращения - 14 февраля 2016 г.).

<3> Pozen D. Deep Secrecy // Stanford Law Review. Vol. 62/2. 2010. P. 257, 284.

<4> Garfinkel S. De-Identification of Personal Information. NIST IR 8053. October 2015. URL: <http://nvlpubs.nist.gov/nistpubs/ir/2015/NIST.IR.8053.pdf>.

<5> Mayer J. et al. Evaluating the Privacy Properties of Telephone Metadata. Stanford University. 1 March 2016. URL: http://www.pnas.org/content/113/20/5536_.

Однако реальная проблема еще глубже: в большинстве случаев интернет-компаниям или иным лицам, заинтересованным в получении сведений, отражающих определенные признаки лица, не требуется знать его имя. Как отмечается, "если компания имеет порядка 100 единиц информации обо мне, которые оказывают влияние на то, как она строит свои отношения со мною в цифровой среде, какая разница, знают они мое имя или нет?" <1>. В современных технических реалиях компании не обязательно знать имя лица для того, чтобы персонализировать свое отношение к нему и предлагать соответствующие товары (услуги). Реальная

"оффлайн" личность лица не имеет особого значения в сети Интернет, имеют значение те характеристики личности, в которых проявляется поведение и предпочтения лица в Сети. "Большие данные" позволяют создавать достаточно детальные портреты людей без необходимости раскрывать при этом их реальные личности. В той мере, в какой эти данные учитываются при принятии решений в отношении такой личности (например, принятие решения о заключении или отказе в заключении договора, определение индивидуальной стоимости товара для него, направление персонализированной рекламы или иного контента для него и т.п.), защита персональных данных, обеспечиваемая посредством их обезличивания, мало что значит. В иностранной литературе по этой причине уже высказываются мнения о том, что необходимо переходить от регулирования собственно персональных данных к регулированию оборота информации в целом <2>. Так или иначе в новых технологических реалиях "узкий" подход к понятию персональных данных, "заточенный" под анкетные данные и данные различного рода государственных реестров, уже не способен выполнять функцию эффективного средства защиты частной жизни граждан в сети Интернет.

<1> Nissenbaum H. et al. Privacy, Big Data, and the Public Good: Frameworks for Engagement. Cambridge University Press. 2014. P. 70.

<2> Gutwirth S., Hert P. Regulating Profiling in Democratic Constitutional State in Profiling the European Citizen: Cross-Disciplinary Perspectives / Ed. by Murielle Hildebrandt & Serge Gutwirth. Dordrecht. Springer. 2008. P. 289.

Из широкого понимания понятия "персональные данные" исходит европейское законодательство <1>. При этом недавно принятый Общий регламент о защите персональных данных развивает эти идеи, определяя персональные данные как "любую информацию, относящуюся к физическому лицу" (ст. 4 (1) **GDPR**). Даже законодательство о персональных данных Великобритании, которое нередко приводят в пример как содержащее наиболее четкое определение персональных данных, последнее время исходит из широкого подхода к нему. Попытки некоторых национальных судов истолковать данное понятие ограничительно <2> были впоследствии с неодобрением восприняты Европейской комиссией, и последующая судебная практика Великобритании пошла по пути широкой интерпретации понятия персональных данных <3>. В настоящее время персональными данными в соответствии с законодательством Великобритании могут выступать следующие данные (по отдельности): имя, адрес, дата рождения, номер паспорта, размер обуви, образец ДНК, группа крови, номер кредитной карты, любимый ресторан, последнее время и место использования кредитной карты, геолокационные данные, аэропорт назначения в авиабилете и др. <4>.

<1> См.: Working Party 29 Opinion 4/2007 on the Concept of Personal Data. 20 June 2007. URL: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_en.pdf.

<2> В частности, в деле **Durant v. Financial Services Authority** [2003] EWCA Civ 1746 судьей была предпринята попытка ограничить понятие "персональные данные" лишь информацией, которая

может иметь биографическое значение и "фокусироваться" на субъекте персональных данных. При этом, по мнению судьи, простое упоминание индивидуума в документе не превращает информацию, содержащуюся в таком документе, в персональные данные.

<3> Edem v. IC & Financial Services Authority [2014] EWCA Civ 92.

<4> См.: Carey P. Data Protection: A Practical Guide to UK and EU Law. Oxford University Press. 2016. P. 25.

В пользу широкого подхода к понятию персональных данных высказывались и некоторые российские чиновники. Например, по мнению бывшего министра Минкомсвязи России, помощника Президента РФ Игоря Щеголева, поисковые запросы, геоданные и информация о посещенных сайтах характеризуют "мировоззрение" пользователя, поэтому должны входить в понятие "персональные данные" <1>.

<1> См.: Луганская Д. В Кремле предложили отнести к персональным данным информацию из соцсетей // РБК. 2015. 20 апреля. URL: <http://rkn.gov.ru/press/publications/news31880.htm?print=1>.

Оценивая рассматриваемые подходы к понятию персональных данных, хотелось бы высказать следующее. Представляется, что будущее - за "широким" подходом к определению персональных данных, по крайней мере, пока на смену законодательству о персональных данных не придет принципиально новое регулирование, ориентированное

не столько на защиту "анкетных данных" физических лиц, сколько на защиту данных об их поведении в цифровом мире, на основании которых в перспективе будет приниматься множество юридически значимых решений в отношении таких лиц. Немаловажен и тот факт, что широкий подход к понятию персональных данных находится в фарватере развития европейского законодательства о персональных данных.

Однако здесь есть одно "но". Российская правовая система и правоприменительная практика вряд ли готовы к адекватному применению широкого подхода к рассматриваемому понятию в современных российских реалиях. Свойственная ему неопределенность требует достаточно высокой квалификации и беспристрастности контрольно-надзорных органов и судов. Особенно это актуально в контексте недавно имплементированных положений о локализации отдельных процессов обработки персональных данных: в отсутствие относительно четкого понимания у всех трех основных участников информационных процессов в сфере использования персональных данных - физических лиц, бизнеса и государственных органов - их практическая реализация невозможна без серьезных рисков избирательного и (или) некомпетентного правоприменения. В этой связи при рассмотрении данного вопроса **de lege lata** и применительно к **современным российским реалиям** автор настоящей книги приветствует применение "узкого" подхода к понятию персональных данных как своего рода вынужденную меру ^{<1>} и в этой части всячески поддерживает В.В. Архипова в том, что критерий идентифицируемости может рассматриваться как некая юридическая фикция, которая необходима для того, чтобы существующие нормы законодательства о персональных данных можно было бы применять

предсказуемо и системно, что, в свою очередь, соответствовало бы конституционному принципу формальной определенности нормы права, точности, ясности, недвусмысленности правовых норм <2>. Иной более широкий подход к определению понятия персональных данных приводил бы, по мнению В.В. Архипова, к "размыванию" объекта регулирования в степени, существенно затрудняющей правоприменение <3>.

<1> В этой части позиция автора по сравнению с первым изданием данной книги не изменилась **de lege lata**, можно говорить лишь о ее некоторой корректировке **de lege ferenda**, да и то с существенной оговоркой о необходимости существенной "перестройки" российской правовой действительности для ее позитивной реализации. В противном случае его такая имплементация приведет лишь к усилению репрессивных начал в деятельности Роскомнадзора и иных органов власти, а также к возрастанию уровня "ненависти" со стороны бизнеса и интернет-сообщества к законодательству о персональных данных в целом.

<2> Принцип формальной определенности был высказан Конституционным Судом РФ в ряде постановлений. См., например: Постановления Конституционного Суда РФ от 31 марта 2015 г. [N 6-П](#); от 29 июня 2012 г. [N 16-П](#); от 20 апреля 2009 г. [N 7-П](#) и др.

<3> Данный аргумент был озвучен этим автором на ряде конференций, а также в ходе переписки с автором настоящей книги в сети **Facebook**. Вполне возможно, что на момент публикации настоящей книги он будет формализован и развит В.В. Архиповым в его

публикациях.

3. Для признания данных персональными не имеет значения, соответствуют ли они действительности или нет, являются 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. Кроме того, указанный вывод следует и из недавно принятых положений о "праве быть забытым" ([ст. 10.3 Закона об информации](#)), которые предоставляют гражданину право требовать от поисковой системы прекратить выдачу ссылок, позволяющих получить доступ к информации о заявителе, распространяемой с нарушением законодательства РФ, являющейся **недостоверной**, а также неактуальной, утратившей значение для заявителя в силу последующих событий или его действий <2>.

<1> Opinion 4/2007 Article 29 Data Protection Working Party // <http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/200>

<2> Впервые положения о "праве быть забытым" были имплементированы в европейское законодательство решением Европейского суда справедливости по делу **Google Spain SL, Google Inc. v Agencia Española de Protección de Datos, Mario Costeja González**, C-131/12, 13 May 2014. Данному решению предшествовало обращение гражданина Испании Гонсалеса в Национальное агентство по защите данных (AEPD) с требованием удалить электронную версию статьи 1998 г. в архиве газеты **La Vanguardia** о продаже его дома на аукционе в счет уплаты долга, который был впоследствии им погашен, а также ссылки на эту статью. Жалоба заявителя об **удалении статьи на сайте** газеты была отклонена на основании законности ее публикации, однако жалоба к **Google Spain** по вопросу **удаления из поиска ссылки на газету** была удовлетворена.

В принципе не исключена возможность квалификации в качестве персональных данных различного рода мнений третьих лиц о субъекте персональных данных, в том числе ложного и (или) оскорбительного характера. В таком случае возможно параллельное использование средств защиты, предоставляемых законодательством о персональных данных, - в отношении оператора (например, интернет-сайта, на котором размещена соответствующая информация) и норм ГК РФ о защите чести, достоинства и деловой репутации (ст. 152) - в отношении автора такого мнения. Следует отметить, что новая редакция ст. 152 ГК РФ предусматривает возможность применения гражданско-правовой ответственности за распространение **любых** сведений,

не соответствующих действительности, а не только порочащих (п. 10 ст. 152 ГК РФ в ред. Федерального закона от 2 июля 2013 г. N 142-ФЗ), а также возможность предъявления требования об удалении соответствующей информации из сети Интернет, в том числе к владельцу соответствующего интернет-ресурса (п. 5 ст. 152 ГК РФ) <1>. В связи с вышеизложенным необходимо обозначить ключевые различия между средствами защиты, предоставляемыми ст. 152 ГК РФ, ст. 14 Закона о защите персональных данных и ст. 10.3 Закона об информации.

<1> В данном случае речь идет не о привлечении владельца интернет-ресурса к ответственности за действия третьего лица, разместившего соответствующую информацию, а о средстве защиты прав гражданина. См.: [Постановление Конституционного Суда РФ от 9 июля 2013 г. N 18-П "По делу о проверке конституционности положений пунктов 1, 5 и 6 статьи 152 Гражданского кодекса Российской Федерации в связи с жалобой гражданина Е.В. Крылова"](#).

Во-первых, положения ст. 14 Закона о защите персональных данных предоставляют возможность предъявления соответствующих требований оператору (например, об удалении соответствующих данных) в силу одного лишь наличия у заявителя статуса субъекта персональных данных. Доказывания их недостоверного характера не требуется. Невыполнение оператором данного требования дает возможность защиты нарушенного права не только в судебном порядке, но и в административном, посредством направления субъектом жалобы в Роскомнадзор и возможного последующего привлечения оператора к

административной ответственности. В некоторых случаях также возможна блокировка интернет-ресурса на основании судебного решения, в котором требование субъекта персональных данных было признано обоснованным (ст. 15.5 Закона об информации). Примечательно, что все иные из рассматриваемых способов защиты не предусматривают такого последствия.

Во-вторых, право, предоставленное субъекту персональных данных в силу ст. 10.3 Закона об информации ("право быть забытым"), может быть реализовано лишь в отношении специального субъекта - поискового сервиса. Оно предоставляет субъекту возможность удаления ссылок на интернет-ресурс, где размещена недостоверная или неактуальная информация. Реализация такого права не предполагает удаления самого спорного контента. Невыполнение поисковой системой заявленного требования влечет возможность как предъявления субъектом персональных данных иска в суд с требованием об удалении ссылки, так и последующего инициирования производства по делу об административном правонарушении в случае неисполнения решения суда (ч. 1.1 ст. 17.15 КоАП РФ). При этом ст. 10.3 Закона об информации не предусматривает возможности предъявления к поисковой системе требований о возмещении убытков или морального вреда.

В-третьих, в рамках ст. 152 ГК РФ может быть привлечен к ответственности непосредственно автор, разместивший недостоверные сведения об истце <1>. При этом важно подчеркнуть, что основанием для предъявления требований по указанной статье могут выступать лишь утверждения о фактах, которые можно проверить и опровергнуть. Оценочные суждения об истце, даже если они носят обидный или

провокационный характер, являются выражением субъективного мнения и не могут быть проверены на предмет соответствия их действительности, а следовательно, распространение таких сведений в сети Интернет не может служить основанием для удовлетворения иска о защите чести, достоинства или деловой репутации <2>. В этом заключается основное отличие данного способа защиты от двух предыдущих.

<1> О распределении бремени доказывания по ст. 152 ГК РФ см.: Потапенко С.В. Особенности доказывания по делам о защите чести, достоинства и деловой репутации // Текст выступления на межвузовском круглом столе, посвященном 75-летию со дня рождения Михаила Константиновича Треушникова. 15 ноября 2013 г. URL: <http://goo.gl/tZJZnw>.

<2> См. п. 9 Постановления Пленума Верховного Суда РФ от 24 февраля 2005 г. N 3 "О судебной практике по делам о защите чести и достоинства граждан, а также деловой репутации граждан и юридических лиц".

4. Персональными данными могут признаваться сведения не только о живом, но и об умершем физическом лице. Данный вывод следует из положений ст. 9 Закона о персональных данных, в которой говорится, что "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".

Материалы судебной практики демонстрируют

актуальность вопроса об обеспечении надлежащей защиты персональных данных умерших лиц. В ряде случаев организация вследствие заключения с медицинскими учреждениями договора на безвозмездную перевозку тел умерших получает приоритетный доступ к персональным данным умерших и их родственников, что дает ей возможность в первоочередном порядке предлагать свои услуги родственникам умерших. И хотя судами данная ситуация рассматривается преимущественно через призму законодательства о защите конкуренции, она неплохо иллюстрирует возможную ценность персональных данных умерших лиц <1>. Представляется, что персональные данные об умерших представляют собой ценность и в интернет-среде, поскольку обладание ими дает возможность манипуляций рекламного и прочего характера в отношении родственников умерших, которые пребывают в уязвимом психологическом состоянии. Так что российский подход в части возможности распространения законодательства о персональных данных на персональные данные умерших является более гуманным, нежели, к примеру, английский, согласно которому персональные данные могут относиться только к **living individual**, т.е. к живущему физическому лицу <2>.

<1> См.: Постановления Семнадцатого арбитражного апелляционного суда от 28 августа 2014 г. по делу [N A50-2319/2014](#); ФАС Уральского округа от 26 марта 2013 г. по делу [N A60-25035/2012](#); решения Арбитражного суда Республики Бурятия от 29 декабря 2014 г. по делу [N A10-4767/2014](#); арбитражного суда Свердловской области от 26 декабря 2013 г. по делу [N](#)

[A60-22167/2013](#). Правда, используемый правоприменительными органами канцеляризм "персональные данные трупов умерших" наводит на размышления о существовании персональных данных трупов "неумерших".

<2> § 2.2.2. Data Protection Act 1998: Legal Guidance. Version 1. 2001 // http://www.ico.org.uk/upload/documents/library/data_protection/detailed_speci alist_guides/data_protection_act_legal_guidance.pdf.

К сожалению, [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. 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.

<1> Кучеренко А.В. Особенности обработки персональных данных лица в случае его смерти // Информационное право. 2011. N 2.

§ 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 цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными". Иными словами, под оператором понимается лицо, которое осуществляет **контроль** над персональным данными,

определяя цели и средства их обработки в собственном интересе. Фактическое "владение" такими данными, а равно осуществление непосредственного процесса обработки данных не требуется <1>.

<1> Bygrave A. Data Privacy Law: An International Perspective. Oxford University Press. 2014. P. 17.

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 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.

<1> В [Постановлении](#) Правительства РФ от 1 ноября 2012 г. N 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), 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](#).

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, включая требование локализации отдельных процессов их обработки;

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 [ч. 1 ст. 6 Закона о персональных данных](#). К ним относятся:

1) наличие согласия субъекта персональных данных на такую обработку;

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>;

<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.

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;

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. Требование конкретного характера согласия предполагает совершение каких-либо действий, свидетельствующих о таком согласии <2>. Например, предоставление самим субъектом персональных данных определенных сведений о себе может в некоторых случаях быть расценено как выражение согласия на их обработку в конклюдентной форме <3>.

<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> Bygrave A. Data Privacy Law: An International Perspective. Oxford University Press. 2014. P. 160.

<3> См., например: решение Сысертского районного суда Свердловской области от 14 мая 2012 г. N 2-526/2012 (в данном случае подача субъектом персональных данных письменного обращения, в котором содержались его персональные данные, была признана судом конклюдентной формой выражения согласия на их последующую обработку адресатом).

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>. По мнению некоторых чиновников Роскомнадзора, "регистрация пользователя Интернета на сайте, подтвержденная логином и паролем, означает согласие субъекта на обработку его персональных данных" <2>. Другое дело, что владельцу интернет-ресурса необходимо быть готовым доказать не только факт дачи такого согласия, но и факт дачи согласия конкретным лицом на обработку его персональных данных в обозначенном объеме. 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 <3>. Факт дачи согласия определенным лицом в отсутствие электронной подписи может быть доказан только косвенными доказательствами, например, фактом использования в качестве средства платежа банковской карты, принадлежащей субъекту персональных данных.

<1> Федеральный закон "О персональных данных": Научно-практический [комментарий](#) / Под ред. зам. руководителя Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций А.А. Приезжевой. С. 48; Зоркольников Р.Д. [Персональные данные, получаемые через Интернет: практические вопросы](#) // СПС "КонсультантПлюс". 2012.

<2> Федеральный закон "О персональных данных": Научно-практический [комментарий](#) / Под ред. зам. руководителя Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций А.А. Приезжевой. С. 52.

<3> 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.

Не следует также забывать и о возможности оспаривания условий, включенных в договор присоединения, особенно заключенный с участием потребителя. 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 <1>. Вряд ли можно говорить о наличии сознательного согласия в случаях, когда предварительное согласие на обработку персональных данных всеми возможными способами является необходимым условием получения какой-либо услуги. Такое требование нарушает принцип обеспечения справедливого характера обработки и в некоторых правопорядках выступает предметом прямого запрета <2>.

<1> См.: [Постановление](#) Семнадцатого арбитражного апелляционного суда от 12 апреля 2013 г. N 17АП-2955/2013-АК по делу N А60-39156/2012, оставленное без изменений [Постановлением](#) ФАС Уральского округа от 29 июля 2013 г. N Ф09-5767/13; а также Постановления Восьмого арбитражного апелляционного суда от 18 марта 2013 г. по делу N [А70-8957/2012](#); Восемнадцатого арбитражного апелляционного суда от 28 мая 2013 г. N

18АП-3864/2013 по делу [N A47-13986/2012](#).

<2> Bygrave A. Data Privacy Law: An International Perspective. Oxford University Press. 2014. P. 146, 147.

Кроме того, 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>.

<1> См., например: [Постановление](#) Второго арбитражного апелляционного суда от 16 июля 2012 г. по делу N A31-3106/2012.

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 вряд ли возможно. 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. Особый подход к таким данным обусловлен тем, что нарушение конфиденциальности подобного рода сведений может серьезно повлиять на частную и семейную жизнь граждан, а также на их социальное положение и трудовую занятость, поскольку делает их объектом поругания и возможных гонений. Кроме того, соблюдение конфиденциальности данных о здоровье имеет ключевое значение не только для защиты частной жизни пациента, но и для сохранения его доверия к медицинским работникам и системе здравоохранения в целом. При отсутствии таких гарантий защиты лица, нуждающиеся в медицинской помощи, могут воздерживаться от обращения за необходимым лечением, подвергая тем самым свое здоровье опасности <1>.

<1> См.: Постановление Европейского суда по правам человека по делу Авилкина и других против Российской Федерации. Жалоба N 1585/09. 6 июня 2013 г.

Для обработки означенных видов "чувствительных" 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;

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

(собственноручная или электронная).

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 безусловно 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 справедливости <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](#) N 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.

<1> ECJ Case C-101/01. 06.11.2003.

Если же пользователь форума сам указал в

своим профилем 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 ^{<1>}. Поскольку стабильность оборота, необходимость защиты публичных интересов и прав третьих лиц требует, чтобы оператор не выступал в роли заложника волеизъявления субъекта персональных данных, законодательство о персональных данных предусматривает закрытый перечень оснований для обработки персональных данных в отсутствие согласия такого субъекта, в том числе и в случае отзыва им такого согласия в порядке, предусмотренном [Законом](#) о персональных данных.

^{<1>} Данное право закрепляется императивной нормой, что обуславливает 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.

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 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>.

<1> См. п. 6 письма ФНП от 23 декабря 2011 г. N 2515/07-17 "О применении ряда положений Федерального закона от 27 июля 2006 г. N 152-ФЗ "О персональных данных".

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 <1>. 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 <2>.

<1> [Постановление](#) ФАС Западно-Сибирского округа от 20 марта 2013 г. по делу N A27-13226/2012; Апелляционное [определение](#) Ярославского областного суда от 5 марта 2012 г. по делу N 33-939/2012; Кассационное [определение](#) Оренбургского областного суда от 8 февраля 2012 г. по делу N 33-805/2012. Противоположный подход см.: [Постановление](#) Тринадцатого арбитражного апелляционного суда от 29 марта 2013 г. по делу N A21-10205/2012.

<2> Анохин Д.А. [Возможность обработки персональных данных](#) субъекта-должника без его согласия // Банковское право. 2012. N 6.

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 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 Интернете, 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 Интернете являются сертификаты ключей проверки электронной подписи, которые в силу своего существа не могут относиться к иной категории персональных данных.

^{<1>} См.: Методические [рекомендации](#) по использованию сети Интернет в целях поиска информации о должниках и их имуществе, утв. ФССП России 30 ноября 2010 г. N 02-7 // СПС "КонсультантПлюс".

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 использование, 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 (принцип спецификации цели).

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 (принцип минимизации данных).

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 (принцип

обеспечения качества 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. Обработываемые 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 N 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>}. Основное значение данных принципов заключается в том, что они не только представляют собой определенные нормативные положения, которые могут быть предметом непосредственного применения, но и выполняют важную ориентирующую функцию для правоприменительной практики контрольно-надзорных органов, а также служат фундаментом для дальнейшего развития законодательства о персональных данных ^{<2>}.

<1> См., например: Schedule 1, UK Data Protection Act 1998.

<2> Bygrave A. Data Privacy Law: An International Perspective. Oxford University Press. 2014. P. 145.

Анализ содержания вышеуказанных принципов позволяет сделать вывод, что они пронизаны идеей **защиты разумных ожиданий** субъекта персональных данных относительно целей, способов и последствий обработки его персональных данных иными лицами.

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 обозначенной цели, что должно обеспечивать определенную степень предсказуемости такой обработки для субъекта персональных данных;

2) отсутствие чрезмерности: объем и содержание обрабатываемых персональных данных должны быть минимально необходимыми для достижения поставленной цели, но не более того <1>, а по достижении такой цели - удалены;

<1> См., например: [Постановление](#) ФАС Северо-Кавказского округа 21 апреля 2014 г. по делу N А53-13327-2013, в котором указано: "Суд... сделал правильный вывод о том, что для идентификации личности при приеме на работу достаточно фамилии,

имени и отчества, при условии предъявления лицом документа, удостоверяющего личность, в котором содержатся все необходимые сведения. Хранение копий паспорта, страниц военного билета, свидетельства о заключении брака, свидетельства о рождении ребенка на рабочем месте превышает объем обрабатываемых персональных данных работника, действующим законодательством не предусмотрено, нарушает права и свободы гражданина, снижает уровень прав и гарантий работника, противоречит федеральному законодательству. При проведении проверки управление сделало правильный вывод о том, что банк производит обработку избыточных персональных данных, по сравнению с теми, которые определены к заявленным целям их обработки, что является нарушением **части 5 статьи 5 Закона N 152-ФЗ**".

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** этого Закона. 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](#).

К сожалению, благой посыл [ст. 14](#) Закона о персональных данных в значительной степени нейтрализуется требованиями [ч. 3 этой статьи](#), согласно которой для реализации права на доступ к обрабатываемым персональным данным субъект должен предоставить оператору запрос, в котором должны быть указаны помимо прочего полные паспортные данные такого субъекта. Получается, что по результатам реализации субъектом права на доступ к своим персональным данным у оператора может появиться еще больше персональных данных, причем верифицированных достаточным образом. В итоге реализация этого права создает значительные риски для субъекта персональных данных в то время, как наделение его таким правом преследует прямо противоположные цели. Гораздо более разумным был бы "зеркальный" подход, исходя из которого для реализации права на доступ к персональным данным субъект должен предоставить ту же идентифицирующую информацию, которая уже содержится в системе и используется для его идентификации (например, по предоставлении такого права после прохождения аутентификации с использованием логина и пароля на сайте либо с использованием электронной почты, предоставленной для регистрации).

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 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.

<1> College van burgemeester en wethouders van Rotterdam v. M.E.E. Rijkeboer. ECJ. Case C553/07. 07.05.2009.

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. Предварительное подписание согласия на обработку персональных данных является безусловным условием заключения договора или

предоставления услуги, в том числе со стороны государственных и муниципальных учреждений.

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 (РКН - в части вопросов соблюдения прав субъектов персональных данных, ФСБ России и ФСТЭК - в части соблюдения требований к обеспечению информационной безопасности в информационных системах обработки персональных данных). 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 <1>;

<1> 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. N 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных". После определения требуемого уровня защищенности в отношении системы персональных данных оператор должен принять организационно-технические меры, предусмотренные для данного уровня защищенности. Перечень указанных мер содержится в [Приказе](#) ФСТЭК России от 18 февраля 2013 г. N 21 "Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных".

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;

7) обеспечение локализации отдельных процессов обработки персональных данных российских граждан ([ч. 5 ст. 18 Закона о защите персональных данных](#)) - с 1 сентября 2015 г.

Рассмотрим подробнее те меры, которые обладают особой актуальностью в сфере электронной коммерции.

1. 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](#).

2. Однако наибольшие сложности в практическом плане представляет реализация меры N 7, а именно обеспечения локализации отдельных процессов обработки персональных данных. В соответствии с недавно введенной [ч. 5 ст. 18](#) Закона о персональных данных при сборе персональных данных, в том числе посредством сети Интернет, оператор "обязан обеспечить запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение персональных данных граждан Российской Федерации с использованием баз данных, находящихся на территории Российской Федерации". Исключения составляют случаи, указанные в [п. п. 2, 3, 4, 8 ч. 1 ст. 6](#) Закона о персональных данных. Это положение, введенное в [Закон](#) о персональных данных Федеральным [законом](#) от 21 июля 2014 г. N 242-ФЗ, вызвало шквал дискуссий и критики с момента начала его обсуждения в Госдуме (которое было, впрочем, весьма недолгим) и до вступления в силу 1 сентября 2015 г. С одной стороны, это было вызвано новизной конструкции локализации в сочетании с отсутствием ограничений на трансграничную передачу персональных данных, с другой стороны - неоднозначностью терминов, использованных в [ч. 5 ст. 18](#) Закона о персональных данных. Как видно из текста

указанного положения, требование локализации "активируется" при наличии совокупности следующих условий: 1) деятельность по сбору информации осуществляется оператором; 2) такая информация представляет собой персональные данные; 3) такие персональные данные принадлежат российским гражданам; 4) отсутствуют предусмотренные законом исключения из требований локализации и 5) Закон о персональных данных распространяется на оператора с точки зрения существующих положений о его сфере деятельности по территории и кругу лиц.

Отсутствие одного из указанных условий, например, факта сбора персональных данных или же ограничения оператором собираемой от пользователей информации таким объемом, которого недостаточно для квалификации собранных данных в качестве персональных (особенно в рамках "узкого" подхода к дефиниции персональных данных), означает отсутствие обязанности по локализации. Условия N 2 и 5 были подробно рассмотрены ранее, в связи с чем необходимо остановиться на оставшихся трех.

В значительной степени многие из возникающих в связи с ними вопросов были сняты с момента опубликования официальных разъяснений Минкомсвязи России по применению положений о локализации персональных данных <1>. Следует рассмотреть их подробнее.

<1> <http://www.minsvyaz.ru/ru/personaldata/>

Во-первых, необходимо отметить, что обязанность по локализации возникает у оператора не

при любой обработке персональных данных, а лишь в связи с осуществлением им сбора таких данных. Закон о персональных данных, неоднократно упоминая термин "сбор", не раскрывает данного понятия. В соответствии с разъяснениями Минкомсвязи России под сбором понимается "целенаправленный процесс получения персональных данных оператором непосредственно от субъекта персональных данных либо через специально привлеченных для этого третьих лиц". Таким образом, интернет-сервисы и интернет-магазины, вступающие в непосредственные отношения с пользователями, предоставляющими свои данные при заполнении различных форм или вследствие пребывания на таких ресурсах, осуществляют сбор персональных данных. В случае если получение персональных данных определенного лица от его работодателя осуществляется по электронной почте, то такие действия сбором не являются (сбор в данном случае осуществил работодатель).

Во-вторых, поскольку обязанность по локализации распространяется не на любые собранные персональные данные, а только те из них, которые принадлежат российским гражданам, необходимо определиться с тем, как будет происходить идентификация гражданства пользователей. По мнению Минкомсвязи России, законодатель предоставил оператору при сборе персональных данных возможность самостоятельно решать данный вопрос исходя из специфики его деятельности. Если же этот вопрос не был решен оператором самостоятельно, то возможно применение ч. 5 ст. 18 Закона о персональных данных ко всем персональным данным, сбор которых был осуществлен на территории Российской Федерации. Таким образом, интернет-сервис может предусмотреть при регистрации дополнительное поле с

указанием гражданства. В случае указания в нем гражданства РФ может происходить переадресация на сервер, расположенный на территории России. Этот метод может сочетаться с технологией геолокации (определение географической принадлежности пользователя по используемому им IP-адресу). Данное разъяснение следует применять в совокупности с разъяснениями о сфере действия **Закона** о персональных данных в пространстве и по кругу лиц (критерий направленной деятельности, см. об этом **§ 4.2 гл. 2** настоящей книги). Также следует отметить, что в соответствии с позицией Роскомнадзора требование локализации не распространяется на случаи сбора персональных данных российских граждан, находящихся за пределами территории Российской Федерации <1>. Таким образом, если иностранный интернет-ресурс осуществил сбор и обработку персональных данных российского гражданина в период нахождения последнего за рубежом, например, в отпуске или в связи с осуществлением им трудовой деятельности, такой сбор не подпадает под действие требований **ч. 5 ст. 18** Закона о персональных данных.

<1> Данная позиция высказывалась представителями Роскомнадзора в ходе ряда публичных мероприятий. См., например: Приезжева А.А. О ходе реализации требований Федерального закона N 242-ФЗ: Материалы международной конференции "Защита персональных данных". 11 ноября 2015 г. URL: <http://zpd-forum.com/programm.html>.

В-третьих, для интернет-сервиса, осуществляющего деятельность на территории различных стран или использующего "облачные"

сервисы, предоставляемые глобальными компаниями, неизбежно встанет вопрос о необходимости осуществления трансграничной передачи персональных данных, а следовательно, и об обеспечении выполнения при этом требований локализации. Ключевое значение для уяснения соотношения требования о локализации персональных данных и возможности их трансграничной передачи имеет понятие трансграничной передачи данных. В соответствии с п. 11 ст. 3 Закона о персональных данных это не просто передача данных за пределы Российской Федерации, но передача персональных данных на территорию иностранного государства **иностранному лицу** - органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу. Таким образом, персональные данные гражданина Российской Федерации, первоначально внесенные в базу данных на территории Российской Федерации и актуализируемые в ней ("первичная база данных"), могут далее передаваться в базы данных, расположенные за пределами России ("вторичные" базы данных), администрируемые иными лицами, с соблюдением положений о трансграничной передаче данных (см. далее). Такие "вторичные" базы данных могут использоваться, в частности, для целей резервного копирования, обеспечения функционирования глобальных процессов транснациональной компании и пр. При этом при передаче персональных данных за границу иному оператору ответственность за действия, совершаемые в отношении переданных персональных данных, несет такой оператор в соответствии с применимым к его деятельности законодательством. Предоставление удаленного доступа к базам данных, находящихся на территории Российской Федерации, с территории другого государства **Законом** о персональных данных не запрещается.

В-четвертых, необходимо отметить, что перечень исключений из требований локализации, представленный в ч. 5 ст. 18 Закона о защите персональных данных, является закрытым и не предусматривает в таких часто используемых в сфере электронной коммерции оснований для обработки, как согласие субъекта персональных данных с размещением его данных на зарубежном сервере, а равно осуществление обработки собранных данных в связи с заключенным договором, стороной которого является субъект персональных данных. Это лишний раз подчеркивает публично-правовую направленность положений о локализации процессов обработки персональных данных, а не стремление предоставить субъекту персональных данных дополнительную возможность по распоряжению своими данными.

В определенной степени российский Закон о защите персональных данных стимулирует иностранные компании, в частности, интернет-сервисы, осуществляющие направленную деятельность на российский рынок, обеспечивать на территории России свое присутствие в различных формах, например, путем создания российской дочерней компании с собственными или арендованными вычислительными мощностями либо заключения договора на обработку персональных данных с российскими компаниями. Это создает условия для их дальнейшего налогообложения на территории России, а также для получения доступа к таким данным со стороны отечественных правоохранительных органов в отсутствие юрисдикционных сложностей <1>.

<1> Подробнее о возможных мотивах принятия

закона о локализации процессов обработки персональных данных и толковании его положений см.: Savelyev A. Russia's New Personal Data Localization Regulations: A Step Forward or a Self-imposed Sanction? // Computer Law & Security Review. Vol. 32/1. 2016. P. 128 - 145.

2.4. Направление уведомления в уполномоченный орган об обработке персональных данных

Оператор до начала обработки персональных данных должен направить в Роскомнадзор уведомление о намерении осуществлять обработку персональных данных, на основании которого он ведет общедоступный реестр операторов персональных данных <1>.

<1>

<http://pd.rkn.gov.ru/operators-registry/operators-list>

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).

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 добросовестных отношений со своими клиентами (пользователями), целесообразно подать такое уведомление. При этом, правда, следует иметь в виду, что подача такого уведомления означает также "попадание на радар" Роскомнадзора и увеличение вероятности включения пославшего его оператора в список организаций, в отношении которых будут проведены плановые проверки.

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, местонахождении баз данных, в которых осуществляется обработка персональных данных, и др. Также необходимо иметь в виду рекомендации, изданные Роскомнадзором по вопросам заполнения формы уведомления <1>.

<1> [Приказ](#) Роскомнадзора от 19 августа 2011 г. N 706 "Об утверждении Рекомендаций по заполнению образца формы уведомления об обработке (о

намерении осуществлять обработку) персональных данных".

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.

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. ст. 15 - 18) <1>, Конвенции о защите физических лиц при автоматизированной обработке персональных данных (ст. 12 и ст. 2 дополнительного протокола к Конвенции от 2001 г.), Директиве N 95/46/ЕС "О персональных данных" (ст. ст. 25 - 26) и большинстве национальных актов о защите персональных данных <2>.

<1> OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. 1980.

<2> Подробный их перечень и изложение соответствующих положений на английском языке см.: Kuner C. Op. cit. P. 189 ff.

Директива N 95/46/ЕС "О персональных данных" содержит общую презумпцию запрета трансграничной передачи данных. Во многом это связано с особым пониманием целей, для достижения которых приняты

положениями о трансграничной передаче данных, в том числе создание определенного барьера для обхода требований европейского законодательства о персональных данных посредством вывода операций по их обработке в третьи страны <1>. Как следствие, трансграничная передача персональных данных возможна лишь при соблюдении общих условий обработки данных (в частности, при наличии законного основания для такой обработки), а также специальных условий, установленных для трансграничной передачи в [ст. ст. 25 и 26](#) Директивы ЕС. К таким специальным условиям относятся:

<1> Bygrave A. Data Privacy Law: An International Perspective. Oxford University Press. 2014. P. 190.

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".

<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/bmding-corporate-rules/mdex_en.htm. См. также: Working Document on Frequently Asked Questions (FAQs) related to Binding Corporate Rules. Article 29 Working Party. 24 June 2008.

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 <1>.

<1> 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.

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 февраля 2015 г. такими странами признаны Андорра, Аргентина, Австралия, Канада, Швейцария, Израиль, 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 **BCR**.

<1>

http://ec.europa.eu/justice/data-protection/document/international-transfers/adequacy/index_en.htm#h2-11

Учитывая существующие положения об ответственности за нарушение законодательства о персональных данных, состояние отечественной правоприменительной практики по данному вопросу <1>, а также общую обстановку с состоянием защиты прав человека в информационно-телекоммуникационных сетях <2>, такой подход европейских коллег можно рассматривать

как вполне заслуженный и обоснованный.

<1> См. далее.

<2> Так, в недавнем решении Европейского суда по правам человека было признано, что российское законодательство не способно защитить граждан от несанкционированного прослушивания их переговоров и ограничить применение негласных методов наблюдения (СОПМ) только теми случаями, когда это необходимо в демократическом обществе. Процедура выдачи разрешений на прослушивание не гарантирует, что прослушивание проводится только в тех случаях, когда это оправданно и необходимо. Надзор за законностью проведения негласных оперативно-розыскных мероприятий неэффективен; отсутствуют действенные средства обжалования. См.: [решение](#) Европейского суда по правам человека по делу "Захаров против Российской Федерации". Жалоба N 47143/06. 4 декабря 2015 г.

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 <1>. 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. ч. 1, 2 ст. 12). Данный перечень по состоянию на 1 февраля 2015 г. включает следующие

страны: Австралия, Аргентина, Израиль, Канада, Марокко, Малайзия, Мексика, Монголия, Новая Зеландия, Ангола, Бенин, Кабо-Верде, Южная Корея, Перу, Сенегал, Тунис, Чили <2>.

<1> 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.

<2> Приказ Роскомнадзора от 15 марта 2013 г. N 274 (ред. от 29 октября 2014 г.) "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".

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 в целом 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". Но при этом хотелось бы большей прозрачности со стороны Роскомнадзора при принятии им решения об отнесении той или иной страны к странам, обеспечивающим адекватный уровень защиты персональных данных, в частности, обозначение им критериев, исходя из которых такое решение было принято.

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. Как отмечалось ранее, проставление "галочки" на веб-сайте или принятие условий

click-wrap-соглашения, сделанное определенным лицом из личного кабинета, 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 <1>;

<1> Следует обратить внимание, что в отличие от [п. 5 ч. 1 ст. 6](#) Закона о персональных данных, допускающего обработку без согласия субъекта персональных данных также и **на стадии заключения договора** по инициативе субъекта персональных данных или договора, по которому субъект персональных данных будет являться выгодоприобретателем или поручителем, [п. 4 ч. 4 ст. 12](#) этого же Закона не предусматривает возможность трансграничной передачи данных на преддоговорном этапе, необходим именно заключенный договор.

5) защиты жизни, здоровья, иных жизненно важных интересов субъекта персональных данных или других лиц при невозможности получения согласия в письменной форме субъекта персональных данных.

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 не в состоянии "переварить" тот объем оборота информации, который имеет место в Интернете, превратившись в один из наиболее декларативных компонентов всего законодательства о персональных данных.

В свое время данный вопрос встал перед

Европейским судом справедливости, 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.

<1> Bodil Lindquist, ECJ Case C-101/01.
06.11.2003.

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 помимо выполнения требований локализации (ч. 5 ст. 18 Закона о персональных данных) в политику конфиденциальности и договоры с

субъектами персональных данных целесообразно включать условия об их согласии на такую передачу, по возможности как можно более конкретно сформулированные, в частности, с указанием страны - импортера данных, а также целей такой передачи. 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.

§ 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 1 тыс. рублей; на юридических лиц - от 5 тыс. до 10 тыс. рублей. 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>;

<1> См., например: [Постановление](#) ФАС Уральского округа от 13 января 2012 г. N Ф09-9061/11.

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 1 тыс. до 3 тыс. рублей. 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 информации 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 рублей с возможной конфискацией несертифицированных средств защиты; на должностных лиц - от 1 тыс. до 2 тыс. рублей; на юридических лиц - от 10 тыс. до 20 тыс. рублей 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. N 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 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 3 тыс. до 5 тыс. 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>.

<1> См.: [Постановление](#) Двенадцатого арбитражного апелляционного суда от 1 сентября 2011 г. по делу N А06-858/2011.

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 <1>.

<1> См. п. 15 Постановления Пленума Верховного Суда РФ от 24 марта 2005 г. N 5 "О некоторых вопросах, возникающих у судов при применении Кодекса Российской Федерации об административных правонарушениях".

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. О необходимости повышения ответственности за нарушение законодательства о персональных данных говорили уже давно. В настоящее время подготовлен проект нового КоАП РФ, который содержит ст. 22.9, отражающую новый подход к ответственности в указанной сфере <1>. В этой статье проекта, состоящей из восьми частей, устанавливается дифференцированный подход к правонарушениям в сфере оборота персональных данных, в ней также отражены конкретные составы правонарушений. Среди них фигурируют такие составы, как обработка персональных данных без согласия субъекта персональных данных; незаконная обработка специальных категорий персональных данных; неразглашение способов обработки персональных данных; непредоставление оператором субъекту информации, касающейся обработки его персональных данных, и др. Несколько увеличивается размер штрафов, максимальный размер в отношении

юридических лиц может составить 300 тыс. рублей.

<1> См. [проект](#) N 957581-6 Кодекса Российской Федерации об административных правонарушениях.

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 тыс. ф.ст. <1>. Во Франции размер штрафа за единичное нарушение может достигать 150 тыс. евро, за повторное - до 300 тыс. евро или 5% годового дохода <2>. В Германии средний штраф составляет 50 тыс. евро, максимальный штраф - 300 тыс. евро <3>. 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 112350350 евро.

<1> 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.

<2> Art. 47 Loi relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel et modifiant la loi. N 78 -

17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés .

<3> § 43 Bundesdatenschutzgesetz 2009.

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 20 млн. евро, или до 4% годового мирового дохода <1>.

<1> Art. 83 (5) Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) // Official Journal of the European Union L 119/1. URL: http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=C_ELEX:32016R0679&rid=1.

Как видно, предлагаемые в новом КоАП РФ 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 будут прилагать усилия по обеспечению соблюдения требований 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.** Собираение сведений, составляющих коммерческую, налоговую или банковскую тайну, путем похищения документов, подкупа или угроз, а равно иным незаконным способом. При этом соби́рание 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;

<1> **Комментарий** к Уголовному кодексу Российской Федерации (постатейный) / Под ред. А.И. Чучаева. М., 2013. Комментарий к ст. 183.

- **часть 2.** Незаконные разглашение или использование сведений, составляющих коммерческую, налоговую или банковскую тайну, без согласия их владельца лицом, которому она была доверена или стала 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. 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. N 98-ФЗ "О коммерческой тайне" (далее - Закон о коммерческой тайне). Как правило, данные о клиентах организации охватываются режимом коммерческой тайны, введенным в ней <1>.

<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.).

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) <1>;

<1> Приговор первомайского районного суда г. Кирова по уголовному делу от 30 августа 2011 г. N

1-269/2011 (43902).

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 <1>). 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 имени переписку и тем самым знакомились с личной информацией, адресованной таким лицам в письмах от их друзей и знакомых <2>, либо которые из неприязненных отношений размещали на таких фальшивых аккаунтах помимо прочих персональных данных ложные сведения о сексуальных предпочтениях потерпевшей <3>.

<1> См.: [Комментарий](#) к Уголовному кодексу Российской Федерации (постатейный) / Под ред. Г.А. Есакова. М., 2012. Комментарий к ст. 137.

<2> См. приговор Исакогорского районного суда г. Архангельска от 31 января 2011 г., которым была осуждена генеральный директор ООО "Гелиос" по ст. ст. 137 и 272 УК РФ // <http://pravo.ru/news/view/47465>.

<3> См. приговор Октябрьского районного суда г. Белгорода от 18 августа 2010 г.

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 закона 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".

<1> [Пункт 2](#) Постановления Пленума Верховного Суда РФ от 20 декабря 1994 г. N 10 "Некоторые вопросы применения законодательства о компенсации морального вреда".

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 рублей <1>. Такая "щедрость" не вызывает удивления на фоне общей картины взыскания морального вреда российскими судами. Так, сумма, близкая к 100 тыс. рублей, 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 <2>. В связи с этим субъекту персональных данных, чьи права были нарушены незаконной обработкой данных, в большинстве случаев целесообразно обратить внимание на административную или уголовную ответственность, не тратя свое время на длительный гражданский процесс о возмещении морального вреда.

<1> Решение Ленинского районного суда г. Чебоксары Чувашской Республики от 6 июля 2010 г. по делу N 2-2225/2010.

<2> См.: Кузнецова О.В. Возмещение морального

вреда: Практическое [пособие](#). М., 2009.

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.

Гораздо более перспективной является введенная Федеральным [законом](#) N 242-ФЗ процедура блокировки интернет-ресурса, на котором осуществляется обработка персональных данных с нарушением законодательства РФ. Закон об информации пополнился еще одним реестром запрещенных интернет-ресурсов - Реестром нарушителей прав субъектов персональных данных ([ст. 15.5](#)). Основанием для внесения в этот Реестр нарушителей сведений о сайте в сети Интернет является размещение на нем персональных данных, обрабатываемых с нарушением законодательства РФ, подтвержденным вступившим в законную силу судебным решением. При этом [ст. 15.5](#) Закона об информации не содержит перечня конкретных нарушений, которые могут послужить основанием для внесения в Реестр нарушителей. В этой связи любая информация, размещение которой на сайте в сети Интернет нарушает права субъекта персональных данных или является следствием несоблюдения какой-либо обязанности, возложенной на оператора персональных данных, и которая не была устранена в процессе взаимодействия Роскомнадзора с провайдером хостинга и владельцем сайта, может стать причиной блокировки такого информационного ресурса (например, при размещении на спорном веб-сайте персональных данных, согласие на обработку которых не было в установленном порядке получено от субъекта

персональных данных и отсутствует одно из оснований, указанных в [ст. 6](#) Закона о персональных данных для их обработки в отсутствие такого согласия; невыполнение оператором в установленный [ст. 20](#) Закона о персональных данных семидневный срок требования субъекта персональных данных об уточнении персональных данных, их блокировании или уничтожении в случае, если персональные данные являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки).

В связи с тем что изображение гражданина, особенно обладающего известностью, может рассматриваться в качестве персональных данных, появляются дополнительные возможности по защите чести, достоинства и деловой репутации, в случае если они были нарушены с использованием изображения гражданина или иных персональных данных. В дополнение к арсеналу правовых средств, доступных по [ст. ст. 152 и 152.1](#) ГК РФ, добавляется еще и возможность заявления требования об удалении соответствующего изображения (персональных данных) под страхом блокировки интернет-ресурса. Уже существуют прецеденты применения законодательства о персональных данных в подобных случаях, в частности, в известном деле Роскомнадзора, выступавшего в интересах известного исполнителя В. Сюткина против интернет-ресурса **Луркмор**, на котором был размещен демотиватор с использованием изображения этого исполнителя <1>. Насколько часто блокировка интернет-ресурса в качестве меры ответственности будет применяться к случаям нарушения законодательства о персональных данных, покажет время, однако уже очевидно, что данная мера обладает куда большим превентивным потенциалом

для операторов персональных данных, чем административные штрафы, которые в настоящее время предусмотрены [КоАП](#) РФ. Сопутствующие репутационные риски могут быть куда более серьезным последствием для компаний с устоявшейся репутацией, особенно учитывая "самоисполнимый" характер соответствующих решений (отсутствие необходимости обращения за содействием в зарубежные органы власти).

<1> См.: решение Мещанского районного суда г. Москвы от 7 апреля 2015 г. по делу N 2-1869/15, оставленное без изменения Определением Мосгорсуда от 14 октября 2015 г.

Документ предоставлен [КонсультантПлюс](#)