УДК 004.738.5
ББК 67.401.114
П 68

П 68 **Право в сфере Интернета**: Сборник статей / Рук. авт. кол. и отв. ред. д.ю.н. М.А. Рожкова. – М.: Статут, 2018. – 528 с. – (Анализ современного права).

ISBN 978-5-8354-1417-8 (в обл.)

Четырнадцатый сборник из серии «Анализ современного права» объединяет статьи, посвященные правовому регулированию отношений в Интернете. В него вошли работы, касающиеся вопросов ответственности за киберпреступления, соблюдения антимонопольного законодательства, регулирования отношений по поводу персональных данных, в том числе с участием информационных брокеров, нарушений в социальных сетях, особенностей рекламы и торговли в сети Интернет, признания информации, запрещенной к распространению, перспектив использования технологии блокчейн, регистрации и использования доменных имен и др. Также в сборнике рассматривается проблематика изменения частного права под влиянием развития сети Интернет и, в частности, анализируются договоры присоединения к многопользовательской игре, особенности электронной формы различных договоров, защита авторских прав в цифровой среде (гиперссылки, мемы, лицензии *Creative Commons*, ключевые слова), аспекты частноправовых процедур рассмотрения споров.

Для судей, адвокатов, практикующих юристов, научных работников, преподавателей, аспирантов и студентов юридических факультетов, а также всех тех, кого интересуют проблемы развития российского права и вопросы применения действующего законодательства.

Сборники серии «Анализ современного права» – это издания, в которых публикуются работы на актуальные темы как представителей университетской среды, так и юристов-практиков. В сборник могут быть включены работы различных авторов, в том числе не имеющих ученых степеней. Приглашение к участию в готовящихся сборниках настоящей серии, а также информация о них – на странице *www.asp.rozhkova.com*.

УДК 004.738.5
ББК 67.401.114

ISBN 978-5-8354-1417-8

ПРЕДИСЛОВИЕ

На протяжении длительного времени юристы спорят о том, нужно ли для отношений, возникающих в Интернете, новое, самостоятельное правовое регулирование либо вполне допустимо несколько скорректировать существующее законодательство с тем, чтобы его можно было применить к Интернету. Причем приверженцы идеи разработки специального законодательства для регламентации интернет-отношений не останавливаются на предложениях о новых специальных законах в обозначенной сфере, а говорят о необходимости выделения в отдельную отрасль норм, регулирующих правоотношения в Интернете.

Не вдаваясь в эту дискуссию, хотелось бы поддержать правоведов, не усматривающих проблемы в распространении действующего законодательства на интернет-отношения (хотя, бесспорно, это потребует внесения соответствующих корректив в существующие НПА). Объяснение этому весьма простое и оно всецело подтверждается содержанием настоящего сборника: Интернет проникает во все сферы нашей жизни, «позволяя» возникать отношениям, которые подпадают под регулирование норм различных отраслей законодательства – административного, уголовного, гражданского, конкурентного и т.д.

В таких условиях принятие самостоятельных законов, регламентирующих только отношения, возникающие в Интернете, будет дублировать нормы уголовного, административного, гражданского и иного законодательства, что повлечет за собой известные сопутствующие проблемы. Это и несогласованность законодательных текстов, и вопросы разграничения сфер регулирования, и необоснованные различия в регулировании схожих случаев, а также иные коллизии. Поэтому более верным и, что немаловажно, более простым решением будет дополнение существующих законов нормами, потребность в которых демонстрирует практика.

Настоящий сборник, конечно, не претендует на постановку и освещение всех проблем, возникающих в интернет-среде. Его основная задача состоит скорее в том, чтобы обозначить актуальные направления в рассматриваемой сфере.

Эта задача сборника неожиданно совпала с одной из целей Всероссийского молодежного конкурса работ по праву информационных технологий и интеллектуальной собственности (*IP&IT LAW*) – выявле-

ние перспективных направлений в области правовой охраны и защиты прав в цифровой среде, в частности, прав на персональные данные, доменные имена, интеллектуальную собственность, виртуальную собственность и др. Это и объясняет то, что в настоящем сборнике публикуются в том числе работы победителей и некоторых участников 2 Всероссийского молодежного конкурса работ по праву информационных технологий и интеллектуальной собственности (*IP&IT LAW – 2017*).

В развитие сказанного надо отметить, что темы конкурсных работ 3 Всероссийского молодежного конкурса работ по праву информационных технологий и интеллектуальной собственности (*IP&IT LAW – 2018*) также пересекаются с тематикой готовящегося пятнадцатого сборника серии «Анализ современного права» (его рабочее название – «E-commerce, торговля онлайн и оффлайн (правовые аспекты)»; см. *www.asp.rozhkova.com*). Поэтому предполагается, что наиболее интересные конкурсные работы также будут опубликованы в следующем сборнике данной серии.

В связи со сказанным приглашаем молодых исследователей (аспирантов, студентов) принять участие в конкурсе *IP&IT LAW – 2018* (см. *www.2018.ipclub.in*). Этот конкурс проводится *IP CLUB* совместно с Координационным центром национального домена сети Интернет при поддержке Комитета Государственной Думы по информационной политике, информационным технологиям и связи.

В завершение хотелось бы напомнить потенциальным авторам, что срок принятия статей в следующий сборник настоящей серии, который, как указывалось, носит рабочее название «E-commerce, торговля онлайн и оффлайн (правовые аспекты)», – до 1 апреля 2018 г. Ознакомиться с условиями публикации можно на странице *www.asp.rozhkova.com*

М.А. Рожкова, д.ю.н.,
эксперт Российской Академии Наук,
член Экспертного Совета Комитета
Государственной Думы по информационной
политике, информационным технологиям
и связи, президент IP CLUB

УКАЗАТЕЛЬ СОКРАЩЕНИЙ

АПК РФ	Арбитражный процессуальный кодекс Российской Федерации
АС	Арбитражный суд
ААС	апелляционный арбитражный суд
ВАС РФ	Высший Арбитражный Суд Российской Федерации (в настоящее время упразднен)
ВС РФ	Верховный Суд Российской Федерации
ГГУ	Германское гражданское уложение
ГК	Гражданский кодекс
ГК РФ	Гражданский кодекс Российской Федерации
ГПК РФ	Гражданский процессуальный кодекс Российской Федерации
Закон о персональных данных	Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»
Закон об информации	Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»
ЕСПЧ	Европейский суд по правам человека
КАС РФ	Кодекс административного судопроизводства Российской Федерации
КоАП РФ	Кодекс Российской Федерации об административных правонарушениях
КС РФ	Конституционный Суд Российской Федерации
Конвенция по правам человека	Конвенция о защите прав человека и основных свобод

Концепция развития гражданского законодательства	Концепция развития гражданского законодательства Российской Федерации (Вестник ВАС РФ. 2009. № 11. С. 6–99)
ООО	общество с ограниченной ответственностью
ТК РФ	Трудовой кодекс Российской Федерации
УК РФ	Уголовный кодекс Российской Федерации
ФАС	Федеральный арбитражный суд
ФГК	Французский гражданский кодекс
ФЗ	Федеральный закон

К.А. Шафеев

ПРАВОВОЕ РЕГУЛИРОВАНИЕ ОТВЕТСТВЕННОСТИ ЗА КИБЕРПРЕСТУПЛЕНИЯ В ПРАВЕ ЕВРОПЕЙСКОГО СОЮЗА

Аннотация. *В статье анализируется существующее правовое регулирование противодействия киберпреступности в праве Европейского союза, совершаемой онлайн с использованием преимуществ сети Интернет, а также выявляются тенденции и перспективы соответствующей стратегии кибербезопасности.*

Ключевые слова: *киберпреступления, сеть Интернет, право Европейского союза, уголовное право.*

Развитие информационных технологий влечет их внедрение во все сферы общественных правоотношений. Тем не менее упрощение повседневных операций, вызванное подобным научно-техническим прогрессом, неизменно приводит ко все более широкому использованию информационных технологий в преступных целях. В настоящее время практика показывает, что преступные действия могут совершаться как с использованием современной компьютерной техники и других электронных девайсов, так и посредством использования преимуществ сети Интернет. Соответственно, деятельность законодателей должна учитывать подобные тенденции.

Противодействие подобным преступлениям и привлечение лиц, совершивших подобные преступные деяния, к ответственности затруднены даже в рамках отдельных государств, поскольку зачастую преступников сложно идентифицировать из-за использования ими компьютерной техники и несовпадения места преступления с фактическим нахождением преступника в момент совершения. Тем более уголовное преследование преступлений такого рода будет затруднено в Европейском союзе, где киберпреступления чаще всего имеют трансграничный характер и могут воздействовать на интересы ЕС в целом.

Европейский союз обладает уникальной (в той мере, в какой это может относиться к международной организации) формой политико-правового устройства, которая в некоторых аспектах усложняет регу-

лирование различного рода правоотношений, а в некоторых аспектах их, наоборот, упрощает. Наиболее близкой аналогией здесь может выступать федеративное государство, где субъекты федерации сохраняют достаточно широкую компетенцию, а главные институции ЕС выступают в роли органов федеральной власти. При это достаточно легко усмотреть и соответствующий федеративный правовой конституционализм Европейского союза, при котором учредительные договоры и Хартия о фундаментальных правах исполняют роль конституционных актов, вторичное законодательство (регламенты, директивы, решения, рекомендации) выполняют функцию федеральных законов, а национально-правовые системы являются законодательными системами субъектов федерации, которые действуют до тех пор, пока не будут «вытеснены» вторичным законодательством вследствие гармонизационных процессов.

При этом нельзя сказать, что существуют все классические для национально-правовых систем отрасли права в «федеральном» восприятии права Европейского союза, поскольку ЕС является достаточно молодой международной организацией для того, чтобы полностью гармонизировать свою автономную правовую систему и привести все право государств-членов к единому «знаменателю».

Тем не менее в гармонизации и унификации уголовного права государств-членов и в создании единого уголовного права Европейского союза как наднациональной отрасли права европейские институции достигли заметных успехов. И все это, несмотря на довольно небольшой процент наднациональных нормативно-правовых актов, посвященных вопросам уголовного права, от общего числа законодательных актов ЕС.

1. Развитие уголовного права Европейского союза

Изначально гармонизация уголовного права Европейского союза началась на политическом уровне почти за 20 лет до того, как сам термин «Европейский союз» окончательно пришел на смену термину «Европейские сообщества». В 1975 г. на министерском уровне в рамках Европейского совета была организована группа TREVI[1], которая заложила основу европейского сотрудничества в сфере противодействия особо тяжким преступлениям, имеющим зачастую трансграничный

[1] (*англ.*) **T**errorism, **R**adicalism, **E**xtremism and **V**iolence **I**nternationally.

характер (терроризм, экстремизм и т.п.)[1]. При этом за время своей деятельности группа TREVI обозначила необходимость совершенно разных механизмов уголовного права, а также смежных областей. В частности, различные рабочие группы прорабатывали план гармонизации мер противодействия широкому кругу преступных действий, а также необходимых мер для подобной гармонизации: от футбольного хулиганства и безопасности ядерных установок до терроризма и полицейского и судебного сотрудничества по уголовным делам. После введения политики «трех опор» (см. далее) и взятия курса на усиленную политико-правовую интеграцию в начале 1990-х функционирование группы прекратилось ввиду распределения ее разнообразных задач между Европолом и другими *ad hoc* рабочими группами, деятельность которых касалась противодействия терроризму и другим опасным трансграничным преступлениям.

Следующим важным этапом на пути формирования единой отрасли уголовного права Европейского союза является принятие Маастрихтского договора в 1992 г., на основании которого ЕС получил три «опоры» – три главных направления и основания для продолжения европейской политико-правовой интеграции[2].

Первой опорой являлись Европейские сообщества, в рамках которых проводилась интеграция по направлениям создания единого экономического рынка, европейских конкурентных правил, единой политики охраны окружающей среды, а также валютного союза.

Второй опорой стала Общая внешняя политика и политика безопасности, которая обозначала роль Европейского союза в миротворчестве, правах человека, соответствующей помощи третьим государствам и т.п., т.е. очерчивала роль ЕС на мировой арене, несмотря на пока отсутствующую правосубъектность.

Третья опора изначально была обозначена как «Правосудие и внутренние дела» (англ. *Justice and Home Affairs*). Позже, после вступления в силу Амстердамского договора, в 1999 г. она была переименована в «Полицейское и судебной сотрудничество по уголовным делам» (англ. *Police and Judicial Co-operationin Criminal Matters*), что точнее отражает направление гармонизации в данной области. Соответственно в рамках данной опоры государства-члены обеспечивали сотрудниче-

[1] *Tony Bunyan*. Trevi, Europol and the European state (http://www.statewatch.org/news/handbook-trevi.pdf, свободный (загл. с экрана)).

[2] Treaty of Maastricht on European Union // Document information (http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=uriserv:xy0026, свободный (загл. с экрана)).

ство судебных органов по вопросам уголовных дел, а также сотрудничество полицейских органов для противодействия трансграничным преступлениям (терроризм, торговля наркотиками, организованная преступность и т.п.).

Также в этот период принимались пятилетние программы действия для развития кооперации государств-членов в области правосудия и внутренних дел: Тамперская программа (1999 г.)[1] обозначила направления по созданию единой миграционной политики ЕС, европейского пространства правосудия, борьбы с трансграничной преступностью и внешней политики в данной области; Гаагская (2005 г.) и Стокгольмская (2010 г.) программы конкретизировали интеграцию государств-членов в вышеназванных направлениях.

После вступления в силу Лиссабонского договора в декабре 2009 г. система опор была упразднена, однако Европейский союз в силу своей появившейся правосубъектности получил некоторые компетенции в сфере уголовного права.

Статья 67 Договора о функционировании Европейского союза[2] (далее – ДФЕС) устанавливает пространство свободы, безопасности и правосудия, учитывая фундаментальные права человека и различия в правовых системах и традициях государств – членов. При этом безопасность и правосудие должны обеспечиваться посредством мер по предупреждению преступности и взаимного признания и исполнения судебных решений по уголовным делам, путем кооперации полицейских органов и иных компетентных органов, а также при необходимости гармонизацией уголовных законов государств-членов.

На основании ст. 4 ДФЕС в рамках пространства свободы, безопасности и правосудия ЕС имеет совместную с государствами-членами компетенцию, это означает, что и ЕС как наднациональная структура, и государства-члены могут принимать нормативно-правовые акты в данной области. Но (если проводить параллель с европейским федерализмом) в области совместной компетенции действует правило «вытеснения», которое означает, что, если какие-либо правоотношения были гармонизированы институциями ЕС на общесоюзном уровне, государства-члены теряют свое право нормотворческой деятельности

[1] Tampere. Kick-start to the EU's policy for justice and home affairs (http://ec.europa.eu/councils/bx20040617/tampere_09_2002_en.pdf, свободный (загл. с экрана)).

[2] Consolidated version of the Treaty on the Functioning of the European Union. OJ C 326, 26.10.2012. P. 47–390.

в данной области. Это значимо для сферы уголовного права, поскольку благодаря этому ЕС обладает компетенцией определить необходимый минимум уголовного законодательства государств-членов. Такая практика устоялась в отношении конкретного перечня преступных деяний, напрямую указанных в учредительных договорах.

2. Европреступления

Статья 83 ДФЕС подтверждает компетенцию ЕС по установлению минимума состава и санкций в отношении определенных особо тяжких преступлений, часто носящих трансграничный характер, – так называемых европреступлений.

К подобного рода преступным деяниям относятся терроризм, торговля людьми, сексуальная эксплуатация женщин и детей, торговля оружием, торговля наркотиками, отмывание денег, коррупция, подделка платежных средств, компьютерные преступления и организованная преступность. Данный список носит исчерпывающий характер, однако может быть расширен Советом ЕС, действующим единогласно после получения согласия Европейского парламента. При этом на данный момент минимум состава и санкций гармонизирован для всех перечисленных преступлений (за исключением торговли оружием), это означает, что государства-члены не могут сделать свое уголовное законодательство мягче установленных стандартов в рамках противодействия подобным преступлениям и применения мер ответственности к лицам, их совершившим.

Также стоит отметить, что к подобного рода преступным деяниям на основании указанных критериев (особая опасность, трансграничный характер) можно отнести преступления против финансовых интересов Европейского союза (к примеру, подделка евро, ст. 325 ДФЕС); преступлений, затрудняющих единообразное применение политики ЕС в государствах-членах (ст. 83(2) ДФЕС). В этих областях ЕС также имеет компетенцию устанавливать обязательное уголовное преследование подобных преступлений в государствах-членах и минимум состава и санкций.

Подобные компетенции, закрепленные в учредительных договорах, воплощаются путем принятия секторального вторичного законодательства (в основном Директив и Рамочных решений), которое государства – члены обязаны имплементировать в свои национально-правовые системы в течение определенного времени.

3. *Status-quo* противодействия киберпреступлениям

Развитие информационных технологий сделало все аспекты человеческих жизней практически зависимыми от различных электронных девайсов и наличия доступа в сеть Интернет. В настоящий момент сложно представить, к примеру, ведение бизнеса без сайта в сети Интернет, без общения онлайн с контрагентом по договору или без электронного перевода платежей.

Киберпреступность имеет гораздо более значительные масштабы: на сегодняшний день объектом подобных преступных кибердеяний могут стать не только экономические интересы человека, но и, например, его личная информация. Европейский союз, где ввиду отсутствия внутренних границ преследование подобных преступлений осложнено их постоянным трансграничным характером, осознал соответствующие вызовы, стоящие перед ним с законодательной точки зрения, и ответил на угрозу роста киберпреступности своевременной стратегией по кибезащите интересов Союза и его граждан.

Киберпреступления вне зависимости от объекта преступных деяний объединяют два признака: во-первых, все они совершаются онлайн, т.е. с использованием доступа в сеть Интернет; во-вторых, все они совершаются с использованием электронных коммуникационных сетей и информационных систем.

По объектному составу все совершаемые киберпреступления можно разделить на три большие группы: 1) преступления, связанные с информационными возможностями сети Интернет (хакерские атаки на информационные сети, фишинг (кража паролей) и т.п.); 2) онлайн-мошенничество; 3) онлайн-хранение неправомерной информации (детская порнография, информация, подстрекающая к расовой ненависти, терроризму и ксенофобии и т.п.).

3.1. Преступления, связанные с информационными возможностями сети Интернет

Что касается первой группы преступлений, связанной прежде всего с использованием информационных преимуществ сети Интернет, то в данных случаях преступники осуществляют кражу информации, которая обычно находится в закрытом доступе, путем хакерских атак на информационные сети или фишинга, т.е. кражи паролей при помощи фальшивых фишинговых сайтов или программ, где потерпевшие,

заблуждаясь, вводят свою личную информацию (обычно пароли или реквизиты банковских карт).

Противодействие подобным киберпреступлениям было урегулировано одним из первых на общеевропейском уровне.

Еще в 2002 г. была принята первая редакция Директивы 58/ЕС, касающаяся обработки персональных данных и защиты неприкосновенности частной жизни в сфере электронных коммуникаций[1] (Директива о неприкосновенности частной жизни и электронных коммуникациях). Эта Директива в первую очередь ориентирована на защиту прав пользователей, под которыми понимаются любые физические лица, которые используют общедоступные средства электронной коммуникации в личных или коммерческих целях.

Защита пользователей осуществляется путем установления позитивного обязательства поставщиков общедоступных средств электронной коммуникации (провайдеров) по принятию надлежащих технических и организационных мер для обеспечения безопасности предоставляемых ими услуг. Подобные меры должны отвечать соответствующему уровню риска стать жертвой релевантных киберпреступлений и должны как минимум включать обеспечение доступа к личной информации только путем авторизации; защиту личных данных от случайного или неправомерного удаления, изменения, обработки, доступа или раскрытия; и обеспечение реализации соответствующей политики безопасности в отношении обработки персональных данных. Также провайдеры обязаны своевременно сообщать пользователям о любом повышении рисков и случаях взломов и кражи их личной информации.

Государства-члены, в свою очередь, обязаны не допускать случайного или неправомерного нарушения конфиденциальности электронных коммуникаций. Любая запись или хранение электронных коммуникаций возможны лишь при даче ясного согласия на это субъектами коммуникации или на основании закона. Вместе с тем у государств-членов также появляется обязанность по обеспечению соответствия национальных систем электронной коммуникации стандартам Европейского союза.

Еще одним важным нормативно-правовым актом ЕС в сфере противодействия преступлениям, связанным с информационными воз-

[1] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications). OJ L 201, 31.7.2002. P. 37–47.

можностями сети Интернет, стала Директива 2013/40/EU об атаках на информационные системы[1]. Директива устанавливает минимальные определения и санкции для преступлений, связанных с атаками на информационные системы в государствах-членах, а также создает условия для сотрудничества судебных и полицейских органов в преследовании подобных преступных деяний.

На основании данной Директивы государства-члены должны криминализировать следующие уголовные составы: незаконный доступ к информационным системам, незаконное вмешательство в функционирование информационных систем, незаконная обработка данных (например, удаление, копирование, изменение и т.п.) и незаконный перехват передачи данных. Также государства-члены обязаны обеспечить уголовное преследование лиц, производящих, продающих, покупающих, импортирующих и распространяющих орудия для подобных преступлений: компьютерные программы, пароли, коды доступа к информационным системам и любая соответствующая информация. Уголовно преследоваться должны соучастники, а также лица, которые покушались на совершение незаконного вмешательства в функционирование информационных систем и незаконную обработку данных.

Наказания должны назначаться, учитывая принципы эффективности, пропорциональности и превентивности. При этом санкции назначаются по правилу «максимума-минимума», при котором Европейский союз устанавливает необходимый минимум максимальных санкций. Соответственно, все вышеперечисленные составы, будучи криминализированными в государствах-членах, должны предусматривать максимальные санкции в виде лишения свободы на срок не менее двух лет. Если незаконное вмешательство в функционирование информационных систем или незаконная обработка данных были совершены умышленно и с нарушением функционирования большого количества информационных систем или больших объемов данных, то максимальные санкции должны предусматривать лишение свободы на срок не менее трех лет. Эти же преступные составы наказываются максимальными санкциями в виде лишения свободы на срок не менее пяти лет при наличии следующих квалифицирующих признаков: если они были совершены преступной организацией; если они повлекли серьезный ущерб; если преступление было совершено в отношении

[1] Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA. OJ L 218, 14.08.2013. P. 8–14.

важной инфраструктурной информационной системы. Кроме того, государства – члены должны установить свою юрисдикцию в отношении подобных преступлений, если преступление или его часть были совершены на территории государства-члена; если преступление было совершено гражданином государства-члена; если преступник находится на территории государства-члена; и если информационная система, против которой было совершено преступление, находится на территории государства-члена. Также после соответствующего уведомления Европейской комиссии государство-член имеет право расширить свою юрисдикцию и на те случаи, когда преступник имеет свое обычное местожительство на территории государства-члена и когда преступление было совершено в пользу юридического лица, которое зарегистрировано в данном государстве-члене.

3.2. Онлайн-мошенничество

Основным нормативно-правовым актом Европейского союза в рамках противодействия онлайн-мошенничеству и смежных с ним преступных деяний является Рамочное решение Совета ЕС 2001/413/ JHA о противодействии мошенничеству и подделке безналичных платежных средств[1].

Это решение обязывает государства-члены криминализировать практически все основные уголовные составы, так или иначе связанные с безналичными расчетами: кража банковских карт, фальсификация платежных инструментов, умышленное использование заведомо краденых платежных средств и т.п. Государства обязаны криминализировать ряд преступлений, относящихся к сфере киберпреступлений, совершаемых онлайн посредством сети Интернет: получение выгоды за счет трансфера денежных средств другого лица без соответствующих прав на обработку (введение, изменение, удаление, копирование) персональных данных и соответствующих прав на вмешательство в функционирование компьютерной системы или программы. Также уголовно преследоваться должны изготовление, продажа, покупка и передача компьютерных программ, предназначенных для совершения вышеназванных киберпреступлений. Соответственно должны преследоваться соучастие и покушения на эти преступления.

[1] 2001/413/JHA: Council Framework Decision of 28 May 2001 combating fraud and counterfeiting of non-cash means of payment. OJ L 149, 02.06.2001. P. 1–4.

Что касается гармонизации санкций в отношении данной категории киберпреступлений, то нельзя с уверенностью сказать, что эта область достаточно гармонизирована. Это связано с тем, что, помимо необходимости соответствия наказания принципам эффективности, пропорциональности и превентивности, в Рамочном решении указано лишь на возможность применения санкций в виде лишения свободы (с допустимостью экстрадиции) «в серьезных случаях», без указания какого-либо минимума такого лишения. Вследствие этого определение санкций практически полностью передано на усмотрение государств-членов.

При этом государства-члены обязаны установить свою обязательную юрисдикцию в отношении уголовного преследования киберпреступлений подобного рода, если: преступление или его часть были совершены на территории государства-члена; преступление было совершено гражданином государства-члена; преступление было совершено в пользу юридического лица, чей административный центр находится на территории данного государства-члена.

3.3. Онлайн-хранение неправомерной информации

Сеть Интернет помимо общеизвестной полезности является самым большим хранилищем информации. Но не всегда хранимая информация является правомерной. И, к сожалению, широко распространены ситуации, при которых хранение неправомерной информации нарушает права особо уязвимой категории граждан – детей.

Именно поэтому в рамках вторичного законодательства Европейским союзом была разработана и принята Директива 2011/92/EU о противодействии сексуальному надругательству и сексуальной эксплуатации детей и детской порнографии[1].

Помимо необходимости криминализировать ряд основных преступлений, связанных с детской порнографией и детской сексуальной эксплуатацией, у государств-членов появляется обязательство по криминализации нескольких киберпреступлений в данной сфере, которые появились совсем недавно ввиду развития информационных технологий и сети Интернет. Так, криминализации подлежат

[1] Directive 2011/92/EU of the European Parliament and of the Council of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA. OJ L 335, 17.12.2011. P. 1–14.

любые попытки встретиться с ребенком, совершенные при помощи средств информационных и коммуникационных технологий, с намерением совершить любое преступление из группы преступлений, связанных с сексуальной эксплуатацией детей. Подобные преступления должны наказываться в государствах-членах лишением свободы на максимальный срок не менее одного года. Также уголовно преследоваться должно и покушение на подобное преступление, совершенное при помощи средств информационных и коммуникационных технологий. Все электронные девайсы, с помощью которых были совершены подобные преступные деяния, подлежат конфискации.

Также государства-члены обязаны принять все необходимые меры для оперативного удаления веб-страниц, содержащих или распространяющих детскую порнографию, если серверы данного веб-сайта находятся на их территории; и все попытки, необходимые для удаления данных веб-сайтов, если их серверы находятся за пределами территории государств-членов. Также могут устанавливаться соответствующие внутренние меры по блокировке сайтов, содержащих или распространяющих детскую порнографию, при условии соблюдения принципов эффективности, пропорциональности и прозрачности.

Что касается установления юрисдикции, то государства-члены обязаны установить юрисдикцию в отношении всех киберпреступлений, сопряженных с онлайн-хранением неправомерной информации, если все преступление или его часть были совершены на его территории и если преступление было совершено гражданином данного государства-члена.

Также с условием уведомления Европейской комиссии государства-члены могут расширить свою юрисдикцию на ситуации, когда киберпреступления были совершены против гражданина данного государства-члена или лица, имеющего свое постоянное местожительство на территории данного государства-члена; когда киберпреступление было совершено в пользу юридического лица, зарегистрированного в установленном законом порядке на территории данного государства-члена; когда субъект киберпреступления имеет свое обычное местожительство на территории данного государства-члена. При этом киберпреступление считается совершенным на территории государства-члена, даже если на его территории всего лишь находятся информационные и коммуникационные технологии, при помощи которых киберпреступление было совершено.

3.4. Иные инициативы ЕС в области противодействия киберпреступлениям

В мае 2015 г. Европейская комиссия под председательством Жан-Клода Юнкера инициировала создание европейского Цифрового единого рынка (англ. *Digital Single Market*) – сегмента европейского Единого рынка, в рамках которого свободное передвижение товаров, услуг, лиц и капитала могло бы осуществляться с постоянным доступом онлайн в условиях честной конкуренции и защиты личных данных вне зависимости от гражданства или местонахождения[1]. Однако необходимые основы для формирования безопасного цифрового рынка были заложены еще в 2013 г., когда Европейский парламент, Совет Европейского союза, Европейский экономический и социальный комитет и Комитет регионов совместно предложили Стратегию кибербезопасности ЕС[2].

Помимо необходимых основ по защите личных данных для формирования Цифрового единого рынка, поводом для формирования Стратегии кибербезопасности ЕС стала серьезная обеспокоенность институций ЕС соблюдением фундаментальных прав человека, в том числе и онлайн. Киберпреступления – весьма специфический и труднорегулируемый вид преступных деяний, где объектом преступления помимо экономических интересов граждан является их право на защиту частной и семейной жизни. Киберпространство должно соответствовать таким стандартам, при которых права граждан онлайн не только бы защищались, но и могли бы свободно реализовываться самими гражданами. Свобода слова является одной из главнейших демократических ценностей, а поскольку сеть Интернет является ключевым информационным источником на сегодняшний день, невозможно представить современное демократическое общество без возможности свободного при условии правомерности выражения мнения онлайн.

Кибербезопаность Европейского союза предполагает реализацию на основе ряда принципов, каждый из которых учитывает как позитивные, так и негативные аспекты современного роста информационных технологий.

---

[1] Digital Single Market // official site of European Commission (https://ec.europa.eu/digital-single-market/en/digital-single-market (загл. с экрана)).

[2] Cyber Security Strategy of the European Union: An open, safe and secure cyberspace. Joint communication to the European Parliament, The Council, The European Economic and Social Committee and The Committee of the Regions /* JOIN/2013/01 final */

Первостепенным является защита фундаментальных прав человека: свободы слова, неприкосновенности личной жизни и персональных данных. При этом реализация и защита прав человека онлайн должна происходить с учетом стандартов Хартии о фундаментальных правах ЕС[1] – основополагающего нормативно-правового акта по правам человека в Европейском союзе, имеющего юридическую силу учредительных договоров.

Не менее важным является соблюдение принципа равенства, а именно установление свободного доступа в сеть Интернет для всех граждан Союза и осуществления в отношении всех граждан единых стандартов кибербезопаности.

Также стратегия кибербезопасности должна реализовываться с соблюдением принципа «антимонопольности» управления, что подразумевает возможность оказания услуг по предоставлению доступа в сеть Интернет не только государственными организациями, но и частными компаниями. Подобный публично-частный дуализм управления должен реализовываться на основании принципа разделения ответственности, на основании которого как публичные, так и частные провайдеры должны нести ответственность перед законом и соответствовать общепринятым стандартам кибербезопасности.

Стратегия ЕС в области кибербезопасности осуществляется по пяти основным направлениям, отражающим как внутрисоюзные потребности киберпространства, так и международные тенденции в этой области.

Первое направление включает достижение устойчивого уровня защиты от киберугроз. Под этим понимается установление минимальных стандартов Сетевой и информационной безопасности, которые были бы обязательными как для частных, так и для публичных акторов, координация и сотрудничество национальных компетентных органов, отвечающих за кибербезопасность, увеличение технического уровня частного сектора в данной области, а также развитие общеевропейских инициатив в сфере кибербезопасности.

Вторым направлением является непосредственное снижение количества совершаемых киберпреступлений путем принятия эффективного и строгого законодательства в сфере противодействия киберпреступлениям, расширения числа оперативных мероприятий и сотрудничества полицейских и судебных органов государств-членов.

[1] Charter of Fundamental Rights of the European Union. OJ C 326, 26.10.2012. P. 391–407.

Третье направление вводит кибербезопасность в рамки Общей внешней политики и политики безопасности. В рамках данного направления планируется открытие диалога между частным и военным секторами в области кибербезопасности, более стандартизированное обучение соответствующего персонала, сотрудничество с международными партнерами (к примеру, НАТО).

Четвертое направление включает в себя развитие индустриальных и технологических ресурсов для обеспечения средств кибербезопасности.

И, наконец, пятое направление заключается в создании согласованной международной политики в области кибербезопасности, которая бы продвигала основные ценности Европейского союза в данной области (фундаментальные права человека, свобода Интернета, защита частной и семейной жизни и т.п.). В рамках данного направления ожидается сотрудничество с НАТО, ОБСЕ, ООН, АСЕАН и другими ключевыми международными межправительственными организациями.

Также в рамках поддержки положений Стратегии кибербезопасности ЕС в январе 2013 г. Европол создал Европейский центр по борьбе с киберпреступностью[1] (далее – ЕС3).

ЕС3 является специальным отделом Европола, в компетенцию и задачи которого входит усиление правоохранительных органов в ответ на угрозу киберпреступности в Европейском союзе и, таким образом, защита прав граждан, предприятий и государств – членов от онлайн-преступности. Для этого ЕС3 разрабатывает методики экспертиз в случаях совершения киберпреступлений, собирает и классифицирует информацию о новых способах совершения киберпреступлений, разрабатывает стратегии для осуществления сотрудничества национальных полицейских органов, а также рекомендует порядок проведения и виды оперативных мероприятий в случае совершения киберпреступлений.

ЕС3 тесно сотрудничает с Агентством ЕС по сетевой и информационной безопасности, которое учреждено после вступления в юридическую силу Регламента No 460/2004[2]. Главной целью данного Агентства является разработка и помощь институциями государствам-членам и представителям экономического сектора в имплементации стан-

[1] About // EuropeanCybercrimeCentre (https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3 (загл. с экрана)).

[2] Regulation (EC) No 460/2004 of the European Parliament and of the Council of 10 March 2004 establishing the European Network and Information Security Agency (Text with EEA relevance). Official Journal L 077, 13.03.2004. P. 0001–0011.

дартов сетевой и информационной безопасности для надлежащего функционирования внутреннего рынка ЕС.

Отдельно стоит упомянуть нормативно-правовые акты, которые станут частью системы права Европейского союза и вступят в свою законную силу в скором будущем.

В 2016 г. был принят новый Регламент 2016/679 об общей защите данных[1]. Регламент представляет собой масштабный и объемный нормативно-правовой акт, призванный установить стандарты обработки данных в Европейском союзе, при которых гарантировались бы все фундаментальные права граждан ЕС, а также принцип законности. В документе содержатся такие новеллы права прав человека и кибербезопаности, как право «быть забытым», право на изменение информации, право на переносимость данных и т.п. Но, несмотря на то что регламенты обладают прямым действием и не нуждаются в имплементации в национально-правовые системы, в законную силу Регламент 2016/679 вступит только 25.05.2018.

4. Ответственность юридических лиц

На данный момент существует очевидная тенденция по включению в национальные уголовные кодексы института уголовной ответственности юридических лиц. Страны Европейского союза не стали исключением: институт уголовной ответственности юридических лиц существует, к примеру, в Литве (ст. 20 Уголовного кодекса Литовской Республики[2]), Франция (ст. 121-2 Уголовного кодекса Французской Республики[3]) и т.д.

Однако на данный момент не представляется возможным гармонизировать институт уголовной ответственности юридических лиц на общесоюзном уровне ввиду слишком больших различий в правовом регулировании данного вопроса в государствах-членах. Соответственно в наднациональном праве Европейского союза нет института

[1] 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) (Text with EEA relevance). OJ L 119, 04.05.2016. P. 1–88.

[2] Lietuvos Respublikosbaudžiamojokodekso (https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.111555, свободный (загл. с экрана)).

[3] Codepénal (https://www.legifrance.gouv.fr/affichCode.do;jsessionid=F06BB691FF16DDFE9DF58E6822AEA8B9.tpdila11v_1?idSectionTA=LEGISCTA000006149817& cidTexte=LEGITEXT000006070719&dateTexte=20170331, свободный (загл. с экрана)).

уголовной ответственности юридических лиц, но предусматривается ответственность юридических лиц за преступления. При этом государства-члены обязаны преследовать юридические лица за совершение киберпреступлений, однако вид преследования (административное или уголовное), а также виды санкций остаются на усмотрение государств-членов.

При этом, указывая на возможность ответственности юридических лиц за преступления, европейские институты всегда оставляют рекомендательную норму, содержащую возможные административные и уголовные виды санкций, применимые к юридическим лицам. Норма ответственности юридических лиц за преступления содержится в неизменном виде практически в каждом нормативно-правовом акте, который относится к уголовному праву ЕС, и преследование киберпреступлений, совершаемых в и при помощи сети Интернет, не является исключением.

Ответственность юридических лиц за преступления наступает при наличии определенных критериев и при этом не исключает возможности уголовного преследования физического лица, непосредственно совершившего преступные деяния. Основания ответственности юридических лиц за киберпреступления можно условно разделить на обязательные и дискреционные. При наличии всех обязательных оснований государства-члены обязаны привлечь юридическое лицо к ответственности; если установлены все дискреционные основания, то государство-член должно решить вопрос о необходимости привлечения юридического лица к ответственности.

Под обязательными основаниями понимаются: совершение преступления физическим лицом; совершение преступления в пользу и в интересах юридического лица, наличие у физического лица руководящей позиции. Руководящая роль выражается в наличии полномочий по представлению юридического лица, по совершению юридических действий от имени юридического лица, а также наличии контролирующих полномочий в целом. При этом не имеет значения, в каком качестве выступает физическое лицо в момент совершения преступления.

Дискреционные основания включают в себя: совершение преступления физическим лицом (а именно любым, кто представляет интересы юридического лица), совершение преступления в пользу юридического лица, отсутствие достаточного контроля со стороны руководящего лица.

Стандартным положением для данного института уголовного права является государственный иммунитет и иммунитет международных публичных организаций: меры ответственности юридических лиц не могут быть применены к государству, государственным предприятиям, институциям государства и местной власти, а также к международным публичным организациям.

Также предусматриваются следующие рекомендательные санкции: штраф, временное лишение права деятельности, ликвидация, запрет на предоставление государственной помощи, временный запрет на участие в государственных закупках (в том числе там, где покупателем выступает ЕС или его институция).

Заключение

Таким образом, правовое регулирование противодействия киберпреступности в Европейском союзе является достаточно широким и в первую очередь направленным на защиту потерпевших, их прав на неприкосновенность частной и семейной жизни, а также на защиту личной информации. Стоит отметить, что европейское законодательство в данной области учитывает все опасные тенденции развития информационных и коммуникационных технологий, а также совершение уже ранее известных уголовному законодательству государств-членов преступных деяний, получивших принципиально новую форму ввиду использования для их совершения информационных удобств сети Интернет.

Несмотря на тот факт, что киберпреступность – явление весьма молодое, европейские институции значительно преуспели в вопросе правового регулирования противодействия, которое не ограничивается нормативно-правовыми актами уголовного права. В частности, благодаря процессам гармонизации на данный момент уже можно говорить о сложившихся стандартах обработки информации в ЕС, а также о достаточном соблюдении прав человека в этой области, что на практике дополняет действие Хартии о фундаментальных правах, которая устанавливает общие положения о неприкосновенности частной, семейной жизни и личной информации.

Что касается уголовного права Европейского союза в сфере противодействия киберпреступлениям в сети Интернет, то на сегодняшний день можно наблюдать достаточно эффективную гармонизацию законодательства государств-членов посредством имплементации

вторичного законодательства ЕС. Это законодательство устанавливает минимум определений и санкций (преимущественно в виде лишения свободы и конфискации электронных девайсов, с помощью которых были совершены релевантные киберпреступления) для наиболее распространенных категорий преступных деяний, сопряженных с информационными возможностями сети Интернет, онлайн-мошенничеством и онлайн-хранением неправомерной информации.

Стоит отметить, что применительно к онлайн-хранению неправомерной информации на общеевропейском уровне эффективно урегулировано лишь противодействие хранению информации, касающейся сексуальной эксплуатации детей. Это, безусловно, является значительным для системы уголовного права ЕС, поскольку в данном случае защищаются права наиболее уязвимых граждан.

Вместе с тем в перспективе необходимо развивать регулирование противодействия онлайн-хранения информации экстремистского характера. На данный момент противодействие разжиганию ненависти по любым мотивам регулируется Рамочным решением Совета 2008/913/JHA[1], однако данный нормативно-правовой акт включает в преступные составы лишь те преступные деяния, которые были совершены публично, оставляя за сферой своего действия преступления такого рода, совершенные при помощи средств онлайн-коммуникации и сети Интернет.

Противодействие онлайн-мошенничеству также весьма эффективно. Несмотря на то что правовое регулирование на общеевропейском уровне основывается лишь на одном нормативно-правовом акте, все самые последние тенденции киберпреступности в данной сфере отслеживаются ЕСЗ, который осуществляет сотрудничество с полицейскими органами всех государств-членов, что позволяет оперативно осуществлять мероприятия для предотвращения онлайн-мошенничества.

Самым проблемным полем остается группа киберпреступлений, связанных с информационными возможностями сети Интернет, поскольку передвижение информации онлайн связано, во-первых, с огромными объемами, а во-вторых, с каждодневным появлением новых возможностей для преступников возобновить и изменить свою преступную деятельность, выходящую за пределы существующего уголовного законодательства. В отличие от основных видов преступлений, таких как фи-

[1] Council Framework Decision 2008/913/JHA of 28 November 2008 on combating certain forms and expressions of racism and xenophobia by means of criminal law. OJ L 328, 06.12.2008. P. 55–58.

шинг или хакерские атаки (которые урегулированы достаточно новыми Директивами), вопрос свободного движения информации в ЕС в целом остается открытым – эта сфера на данный момент не урегулирована, но, возможно, ситуация улучшится с вступлением в силу Регламента об общей защите данных.

Таким образом, правовое регулирование противодействия киберпреступлениям в Европейском союзе характеризуется разносторонним и многоуровневым подходом, сочетающим как нормативно-правовые акты «мягкого» права, так и регламенты, директивы и рамочные решения, обязательные для государств-членов. В целом уже на данном этапе развития этого сегмента уголовного права ЕС существующая практика и модель правового регулирования, а также существующие стандарты в этой области могут быть переняты государствами, не входящими в ЕС, в качестве образца для реформирования собственных систем уголовной юстиции в сфере противодействия киберпреступлениям.

Пристатейный библиографический список:

1. Consolidated version of the Treaty on the Functioning of the European Union. OJ C 326, 26.10.2012. P. 47–390.

2. Charter of Fundamental Rights of the European Union. OJ C 326, 26.10.2012. P. 391–407.

3. Regulation (EC) No 460/2004 of the European Parliament and of the Council of 10 March 2004 establishing the European Network and Information Security Agency (Text with EEA relevance). Official Journal L 077, 13.03.2004. P. 0001–0011.

4. 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) (Text with EEA relevance). OJ L 119, 04.05.2016. P. 1–88.

5. Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications). OJ L 201, 31.7.2002. P. 37–47.

6. Directive 2011/92/EU of the European Parliament and of the Council of 13 December 2011 on combating the sexual abuse and sexual exploitation of

children and child pornography, and replacing Council Framework Decision 2004/68/JHA. OJ L 335, 17.12.2011. P. 1–14.

7. Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA. OJ L 218, 14.08.2013. P. 8–14.

8. Council Framework Decision 2001/413/JHA of 28 May 2001 combating fraud and counterfeiting of non-cash means of payment. OJ L 149, 02.06.2001. P. 1–4.

9. Council Framework Decision 2008/913/JHA of 28 November 2008 on combating certain forms and expressions of racism and xenophobia by means of criminal law. OJ L 328, 06.12.2008. P. 55–58.

10. Cyber Security Strategy of the European Union: An open, safe and secure cyberspace. Joint communication to the European Parliament, The Council, The European Economic and Social Committee and The Committee of the Regions, /* JOIN/2013/01 final */.

11. Lietuvos Respublikosbaudžiamojo kodekso (https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.111555, свободный (загл. с экрана)).

12. Codepénal (https://www.legifrance.gouv.fr/affichCode.do; jsessionid=F06BB691FF16DDFE9DF58E6822AEA8B9.tpdila11v_1?idSectionTA=LEGISCTA000006149817&cidTexte=LEGITEXT000006070719&dateTexte=20170331, свободный (загл. с экрана)).

13. *Tony Bunyan*. Trevi. Europoland the Europeanstate (http://www.statewatch.org/news/handbook-trevi.pdf, свободный (загл. с экрана)).

14. Tampere. Kick-start to the EU's policy for justice and home affairs (http://ec.europa.eu/councils/bx20040617/tampere_09_2002_en.pdf, свободный (загл. с экрана)).

15. Treaty of Maastricht on European Union // Document information (http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=uriserv:xy0026, свободный загл. с экрана)).

16. Digital Single Market // official site of European Commission (https://ec.europa.eu/digital-single-market/en/digital-single-market (загл. с экрана)).

17. About // EuropeanCybercrimeCentre (https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3 (загл. с экрана)).

Е.С. Хохлов[1,2]

ДЕЛО ФАС РОССИИ В ОТНОШЕНИИ ПРАКТИК GOOGLE В СФЕРЕ ОПЕРАЦИОННОЙ СИСТЕМЫ ANDROID: ПРАВОВЫЕ ПРОБЛЕМЫ И ЗНАЧЕНИЕ ДЛЯ РОССИЙСКОГО АНТИМОНОПОЛЬНОГО РЕГУЛИРОВАНИЯ

Аннотация. *В настоящей статье рассматриваются правовые и иные аспекты антимонопольного дела в отношении Google, рассмотренного ФАС России. Данное дело касалось различных практик, применявшихся Google в рамках операционной системы Android и магазина Google Play. В статье подробно анализируются фактические обстоятельства, ставшие предметом оценки ФАС России, правовые и иные проблемы, стоявшие перед ФАС России в рамках рассмотрения дела, выводы ФАС России, а также контраргументы, заявлявшиеся Google. Особое внимание уделено проблемам в применении антимонопольного законодательства в отношении интернет-сервисов и отношений по использованию объектов интеллектуальной собственности.*

Ключевые слова: *Федеральная антимонопольная служба, антимонопольное законодательство, злоупотребление доминирующим положением, исключительные права.*

Дело против *Google*[3], рассмотренное Федеральной антимонопольной службой России (далее – ФАС России), является знаковым как для

[1] Автор являлся частью команды консультантов, представлявшей интересы заявителя в данном деле, – компании Яндекс. В то же время автор, будучи также преподавателем конкурентного права, пытался дать научную оценку сделанным ФАС России выводам.

[2] Следует также сделать важную оговорку: в настоящей статье рассмотрены исключительно вопросы, раскрытые в составе публичного решения и предписания ФАС России. Само дело в ФАС России рассматривалось в закрытом режиме для целей сохранения коммерческой тайны сторон, равно как и последующие судебные разбирательства по данному делу, рассматривавшиеся в закрытых судебных заседаниях по ходатайству *Google*. Поэтому многие детали данного дела, которые могли бы сделать изложение более понятным и подробным, не приводятся.

[3] Решение и предписание ФАС России были вынесены в отношении двух компаний корпорации *Google Inc*. и компании *Google Ireland Limited*. Для целей настоящей статьи обе компании будут именоваться «*Google*».

российского антимонопольного регулирования, так и для международного сообщества. ФАС России стала первым антимонопольным органом в мире, давшим негативную оценку практикам *Google* в отношении операционной системы *Android*.

В настоящее время дела в отношении аналогичных фактов рассматриваются Европейской комиссией, Комиссией по справедливой торговле Южной Кореи и с совсем недавнего времени – антимонопольным органом Турции. Европейская комиссия, хронологически уже после принятого ФАС России решения, вынесла свое заключение об обстоятельствах (*statement of objections*)[1] в апреле 2016 г. При этом из пресс-релиза Комиссии, сопровождавшего вынесение заключения об обстоятельствах[2], можно резюмировать, что предварительные выводы Комиссии в целом соответствуют заключениям, к которым пришла ФАС России.

В данном деле перед ФАС России стояли непростые вопросы, связанные с тем, подходят ли классические методы антимонопольного регулирования для новой экономики, основанной на информационных технологиях. Данное дело было вдвойне сложным для ФАС России, поскольку в России аналоги таких знаковых дел, как, например, дела против *Microsoft* в ЕС (дела касательно *Windows Media Player* и *Internet Explorer*), на момент рассмотрения дела против *Google* отсутствовали. ФАС России пришлось фактически с нуля формулировать так называемую теорию перенесения рыночной власти (*leveraging theory of harm*), которая является основой обвинения против *Google* в деле по *Android*.

По мнению автора настоящей статьи, подходы классического антимонопольного регулирования вполне применимы в отношении подобных дел, и эта точка зрения в целом разделяется европейскими специалистами. Очевидно, что это не единственная точка зрения, и находятся те, кто полагает, что рынки в сфере информационных технологий обладают такой спецификой, которая требует выработки принципиально новых подходов к их антимонопольному регулирова-

[1] Заключение об обстоятельствах в конкурентном праве ЕС представляет собой предварительные выводы Комиссии о наличии нарушения антимонопольных норм в действиях хозяйствующего субъекта. Компания, в отношении которой вынесено заключение об обстоятельствах, имеет возможность ответить на него, опровергая выводы Комиссии, и запросить слушания по делу, если посчитает необходимым. Исходя из публичной информации *Google* уже направила Комиссии свой ответ на заключение об обстоятельствах, но не запросила проведение слушаний.

[2] См.: http://europa.eu/rapid/press-release_IP-16-1492_en.htm

нию (а, возможно, и вообще к неприменению мер антимонопольного регулирования к ним).

В частности, сторонники такой точки зрения исходят из того, что многие информационные компании можно слишком легко признать монополистами просто в силу их размера и наличия у них особого положения как владельцев соответствующих информационных платформ (т.е. в силу самого факта обладания такими платформами), что является слишком низким стандартом доказывания. Более того, по мнению данных ученых, на рынках в сфере высоких технологий в принципе невозможно обладание рыночной властью, поскольку «новый лидер рынка может образоваться не только из стартапа, но и путем репозиционирования существующего онлайн-сервиса на смежные рынки»[1], т.е. барьеры доступа на рынок являются низкими.

Представляется, что это упрощенный взгляд на вещи, поскольку сторонники применения традиционного антитраста не отрицают возможности конкуренции между платформами, и в таком случае вывод о наличии доминирующего положения владельца одной из платформ вполне может и не быть сделан. Однако если сама платформа *действительно* является доминирующей (как та же операционная система *Android*), то почему антимонопольные органы не должны пытаться применять антимонопольное законодательство к действиям владельца этой платформы? Применительно к тому, что барьеры доступа на рынки в сфере высоких технологий являются низкими и что конкуренция на них находится «на расстоянии одного клика» (*competition is one click away* – известное выражение основателей *Google*), это опровергается реальной практикой и длительным отсутствием новых конкурентов на многих имеющих значение рынках в сфере информационных технологий, в том числе тех, которые стали предметом рассмотрения ФАС России в деле *Google*.

С развитием новой цифровой экономики перед специалистами в сфере антимонопольного регулирования встал вопрос: что важнее для экономики – инновации или конкуренция? При этом сторонники приоритета инноваций над конкуренцией почему-то противопоставляют эти ценности, т.е. исключают возможность конкуренции при инновациях. Тем не менее конкуренция и инновации вполне

[1] *D. O'Connor.* 'Understanding Online Platform Competition: Common Misunderstandings'. *Internet Competition and Regulation of Online Platforms* (May 2016) // Competition Policy International. P. 9–10.

совместимы, поскольку одним из следствий конкуренции является внедрение инноваций[1].

Очевидно, что инновации важны, но в долгосрочной перспективе конкуренция важнее, поскольку жизненный цикл той или иной инновации рано или поздно проходит и хозяйствующие субъекты могут начать применять ограничительные практики во вред тем конкурентам, которые могут дальше развивать инновации в соответствующей области. В связи с этим, по мнению автора настоящей статьи, не должно быть препятствий для применения мер антимонопольного регулирования, если действия обладателя платформы начинают тормозить инновации посредством вытеснения с нее конкурентов.

Решение ФАС России против *Google* вызвало дискуссии в российской и иностранной прессе и профессиональных изданиях. Решение ФАС России было проанализировано в контексте проводимого в ЕС расследования в статье, написанной известными в мире специалистами в области конкурентного права[2], и в данной работе была дана позитивная оценка принятого ФАС России решения против *Google*.

Автор настоящей статьи ставит задачу проанализировать дело ФАС России против *Google* в контексте тех сложностей, которые возникли перед ФАС России при его рассмотрении, а также его значения для российского и международного антимонопольного сообщества.

Ход рассмотрения дела

Прежде чем переходить непосредственно к анализу рассмотренного ФАС России дела и сделанных в рамках него выводов, следует напомнить то, каким образом происходило собственно рассмотрение дела.

Дело было возбуждено в феврале 2015 г. по жалобе Яндекса – российской поисковой системы и основного конкурента *Google* в России и странах СНГ. Изначально дело было возбуждено по такому составу потенциального нарушения, как недобросовестная конкуренция, которая в наиболее общем виде предполагает обязанность хозяйствующего субъекта конкурировать на рынке, используя честные и добросовестные способы и не используя такие методы, которые заведомо направ-

[1] Подробнее см.: *Сушкевич А.Г.* Институты конкурентного права и новая экономика: как добиться соответствия // Законы России: опыт, анализ, практика. 2016. № 3. С. 21–34.

[2] См.: *B. Edelman and D. Geradin*. 'Android and competition law: exploring and assessing Google's practices in mobile' [2016] // European Competition Journal. P. 1–36.

лены на причинение вреда конкурентам. Через некоторое время после возбуждения дела ФАС России добавила еще одну квалификацию, впоследствии ставшую основой для принятия обвинительного решения, – злоупотребление доминирующим положением.

В такой первоначальной «двойственной» квалификации нет ничего удивительного: ФАС России, очевидно, стремилась по такому сложному делу оставить возможность выбора итоговой квалификации на случай, если проанализированные в рамках дела фактические обстоятельства приведут к выводу о наличии только одного нарушения антимонопольных запретов. С формальной точки зрения также не была исключена и возможность, когда определенные практики могли быть признаны недобросовестной конкуренцией, а остальные – злоупотреблением доминирующим положением. С точки зрения теории конкурентного права недобросовестная конкуренция имеет место там, где отсутствует проявление рыночной власти; если же ограничительная практика является проявлением рыночной власти, ее следует квалифицировать как злоупотребление доминирующим положением. В рамках данного дела ФАС России в итоге пришла к выводу о том, что все действия *Google* явились проявлением рыночной власти, вследствие чего в итоге осталась только квалификация в виде злоупотребления доминирующим положением.

В сентябре 2015 г. ФАС России вынесла обвинительное решение, признав *Google* нарушившей российское антимонопольное законодательство применительно к своим практикам в отношении операционной системы *Android*.

В своем решении ФАС России признала антиконкурентыми следующие практики Google:

1. Предоставление своего доминирующего товара – магазина приложений *Google Play* – исключительно в составе пакета приложений *Google Mobile Services* (далее – *GMS*), который включает в себя более десятка иных приложений от *Google* для ОС *Android*. Тем самым, в соответствии с выводами ФАС России, *Google* переносила свою рыночную силу в отношении *Google Play* на иные приложения для ОС *Android*, получая возможность предустанавливать их на большом количестве устройств без конкурентной борьбы. В то же время конкуренты *Google* в сфере иных мобильных приложений для ОС *Android* не имели возможности предоставить равноценную замену магазину приложений *Google Play*, чтобы предустановить свои приложения на условиях, сопоставимых с условиями предустановки, имевшимися у *Google*.

2. В дополнение к практике связывания *Google* также требовала от производителей мобильных устройств для ОС *Android* соблюдения дополнительных ограничительных требований: (а) настройки поиска *Google* «по умолчанию» во всех точках доступа к поиску на устройствах, (б) приоритетного размещения иконок приложений *Google* на первом экране устройств и (в) запрета на предустановку приложений конкурентов *Google* (включая те, в отношении которых у *Google* отсутствовали конкурирующие приложения), в том числе обусловленного выплатой соответствующего вознаграждения.

В дополнение к решению ФАС России было также вынесено предписание, в соответствии с которым *Google* была обязана:

1) прекратить нарушение и не допускать его в будущем, а именно:

– не обусловливать предоставление *Google Play* требованием об обязательной предустановке иных приложений, сервисов *Google* (*GMS*);

– не обусловливать предоставление *Google Play* требованием о размещении иконок приложений *Google* (*GMS*) на главном экране мобильного устройства;

– не обусловливать предоставление *Google Play* требованием о предустановке поисковой системы *Google* в качестве поиска «по умолчанию»;

– не запрещать производителям мобильных устройств предустановку приложений и сервисов конкурентов *Google* (в том числе путем выплаты вознаграждения за отказ вендоров от предустановки приложений и сервисов конкурентов *Google*);

2) совершить все действия, необходимые для внесения изменений во все действующие соглашения/договоры с производителями мобильных устройств с целью исключения из них вышеуказанных требований;

3) проинформировать пользователей мобильных устройств о возможности деактивации предустановленных приложений *Google*, изменения поисковой машины в браузере *Google Chrome*, о возможности установки иного виджета поиска и установки иных приложений, аналогичных входящим в пакет *GMS*, а также о возможности изменения расположения иконок на экране устройства в форме уведомления, которое должно быть выведено на экран мобильного устройства.

Позднее ФАС России наложила на *Google* штраф в размере около 440 млн руб. за злоупотребление доминирующим положением в соответствии со ст. 14.31 КоАП РФ.

Google оспорила решение и предписание ФАС России, а также административный штраф в судебном порядке. В рамках данного судебного разбирательства были приняты решения судов первой и апелляционной инстанций, подтвердившие законность решения и предписания ФАС России.

В связи с имевшимся, по мнению ФАС России, неисполнением предписания было возбуждено соответствующее дело об административном правонарушении, и в конце 2016 г. было принято решение о наложении на *Google* административного штрафа за неисполнение предписания по ст. 19.5 КоАП РФ. *Google* оспорила и этот штраф, и в настоящее время принято решение суда апелляционной инстанции, подтвердившее законность позиции ФАС России.

Но этими процессами дело в отношении *Google* не исчерпывается. ФАС России, полагая свое предписание неисполненным, подала в Арбитражный суд г. Москвы уже собственный иск о понуждении *Google* к исполнению предписания. В свою очередь, *Google* подала еще одно заявление к ФАС России в отношении слишком короткого, по мнению *Google*, срока исполнения предписания, который ФАС России вновь назначила на основании ч. 7 ст. 51 ФЗ от 26.07.2006 № 135-ФЗ «О защите конкуренции» (далее – Закон о защите конкуренции) после того, как признала, что *Google* не исполнила предписание в первоначальный срок и привлекла *Google* к административной ответственности за это.

Таким образом, решение и предписание ФАС России «обросли» множеством разнообразных судебных процессов.

На момент написания настоящей статьи в суде кассационной инстанции по основному делу (об оспаривании решения и предписания ФАС России) было утверждено мировое соглашение, которым был урегулирован спор в отношении решения и предписания ФАС России. Содержание мирового соглашения недоступно публично в связи с тем, что сам спор рассматривался в режиме закрытых судебных заседаний. Тем не менее с существенными условиями мирового соглашения можно ознакомиться в пресс-релизе ФАС России[1]. Из публикаций в прессе можно сделать вывод о том, что остальные споры между ФАС России и *Google* будут тем или иным образом урегулированы в связи с утверждением мирового соглашения по основному делу и *Google* выплатит наложенные на нее штрафы по ст. 14.31 и ст. 19.5 КоАП РФ.

[1] См.: http://fas.gov.ru/press-center/news/detail.html?id=49773

Ключевые проблемы и развилки, стоявшие перед ФАС России, и выработанные ФАС России решения

(1) *Анализ рынка*

ФАС России определила соответствующий рынок, на котором *Google* была признана занимающей доминирующее положение, как рынок предустанавливаемых магазинов приложений для ОС *Android*, локализованных для России. Локализация отсылает к тому, что для каждой страны фактически существует своя собственная версия магазина приложений, которая должна учитывать национальные особенности (например, язык) и соответствовать требованиям национального законодательства. ФАС России было установлено, что лишь малая часть российских пользователей готова использовать магазин приложений, предназначенный для предустановки на мобильные устройства в другой стране. При этом с точки зрения географических границ рынок был определен как глобальный, поскольку товар, будучи воплощенным в программном обеспечении, может перемещаться от производителя к покупателю в любую точку мира с минимальными затратами.

Было признано, что магазин приложений – самостоятельный товар, который имеет особое функциональное назначение и не может быть заменен другими приложениями. В частности, не является товаром-заменителем мобильный браузер, основная функция которого состоит в предоставлении доступа к веб-страницам и через который лишь незначительное количество пользователей реально скачивает приложения (которые в любом случае могут обновляться только через *Google Play*). При этом ФАС России установила, что *Google Play* с технической точки зрения может функционировать отдельно от других приложений из пакета *GMS*. Важное отличие *Google Play* от других приложений *Google* состоит в том, что иные приложения могут быть скачаны пользователем самостоятельно из *Google Play*, тогда как сам *Google Play* в силу коммерческого решения *Google* невозможно получить иначе, кроме как предустановленным на мобильном устройстве.

При определении границ рынка ФАС России основывалась на Порядке проведения анализа состояния конкуренции на товарном рынке[1].

[1] Утвержден Приказом ФАС России от 28.04.2010 № 220 (с последующими изменениями).

Однако этот акт не устанавливает каких-либо особенностей в отношении анализа рынков в сфере информационных технологий, поэтому ФАС России пришлось вырабатывать подходы самостоятельно.

Одной из проблем, с которой столкнулась ФАС России, было соотношение традиционного понимания рынка и так называемых многосторонних рынков. В случае с *Google* имеется платформа – операционная система *Android*, вокруг которой «вращается» большое количество отдельных продуктов: те же самые магазины приложений, поиск в Интернете, веб-браузеры, приложения для работы с фото и видео и огромное множество других приложений и сервисов, имеющих различную функциональность. В свою очередь, приложения и сервисы связаны с услугами онлайн-рекламы, с помощью которой данные приложения могут монетизироваться. Некоторые приложения, в том числе и сам магазин приложений, предоставляют возможность монетизации от непосредственно самого приложения; например, встроенные покупки или комиссия, взимаемая с разработчиков за размещение приложений в магазине приложений. Наконец, существуют производители мобильных устройств, которые компонуют свои устройства определенными приложениями и сервисами и взаимодействуют с разработчиками приложений, как правило, по модели разделения доходов от предустановленного приложения/сервиса.

Все это многообразие рынков тесно взаимосвязано и характеризуется многосторонними косвенными сетевыми эффектами. Косвенным сетевым эффектом в экономической теории признается ситуация, при которой ценность товара для покупателя на одном рынке повышается, если повышается количество покупателей товара на смежном рынке. Например, ценность рекламы в газете (один рынок) повышается с увеличением количества читателей этой газеты (другой рынок). Многосторонние косвенные сетевые эффекты характерны для платформ, объединяющих несколько элементов воедино. Например, ценность рекламы в приложении «Погода» повышается не только, если увеличивается количество пользователей этого приложения, но и если растет количество пользователей операционной системы, для которой это приложение создано, или количество производителей мобильных устройств, которые используют эту операционную систему[1].

[1] Подробнее о многосторонних сетевых эффектах в контексте дела *Google* см.: *Юсупова Г.Ф.* ФАС против Google: экономический анализ для особых рынков // Экономическая политика. 2016. Т. 11. № 6. С. 82–99.

Возникает вопрос, следует ли в таком случае считать рынком всю платформу целиком или определять рынок по каждой стороне платформы в отдельности?

Проблема для ФАС России состояла в том, что понятия многосторонних рынков в российском законодательстве нет. Если в некоторых странах вопрос анализа границ рынка не является принципиальным, и в отношении него может быть допущена определенная степень погрешности, то в случае с российским законодательством и судебной практикой неправильное определение границ рынка может стать самостоятельным основанием для оспаривания решения ФАС России.

Поскольку с формальной точки зрения иного варианта не было, ФАС России определила границы рынка в отношении каждой стороны платформы в отдельности. В то же время ФАС России приняла во внимание при определении границ рынка и рыночной власти *Google* сетевые эффекты в качестве барьеров доступа и экспансии, тем самым учтя особенности многосторонних рынков. Иными словами, сильные косвенные сетевые эффекты, имеющиеся на платформе *Android*, были признаны ФАС России в качестве факторов, осложняющих доступ на какую-либо из сторон этой платформы. ФАС России также было учтено, что *Google* является разработчиком и владельцем самой операционной системы *Android*.

Таким образом, ФАС России фактически сделала вывод о том, что конкуренция существует не только между платформами, но и внутри одной платформы. Этот вывод представляется справедливым в отношении операционной системы *Android*, учитывая, что в нее с момента запуска было привлечено множество производителей устройств и разработчиков приложений и сервисов и что она изначально пропагандировала свою открытость.

Также перед ФАС России встал вопрос о том, может ли в принципе являться товаром объект, в отношении которого не установлена цена (магазины приложений для операционной системы *Android* предоставляются для предустановки бесплатно). Классическое определение товара и рыночной власти привязаны к цене, в частности, именно на этом основан широко известный *SSNIP*-тест (называемый в России «тестом гипотетического монополиста»), а также многие иные тесты для определения границ рынка и рыночной власти.

Однако в случае с *Google Play*, во-первых, можно говорить о том, что встречное предоставление за товар уплачивается не в денежной, а иной форме (например, путем необходимости соблюдать определен-

ные требования к предустановке и (или) приобретения возможности получения доли доходов от онлайн-рекламы). Во-вторых, в случае нулевой цены товара в расчет можно принимать возможность снижения качества товара (поскольку качество в дополнение к цене является ключевым фактором конкуренции). Кроме того, в соответствии с формальным определением товара по ст. 4 Закона о защите конкуренции товаром может являться благо, вводимое в оборот любым способом (в случае с *Google Play* – путем его бесплатной предустановки). Таким образом, тот факт, что какой-то объект гражданских прав предоставляется условно-бесплатно, не влияет на возможность его квалификации как товара с точки зрения антимонопольного законодательства.

Наконец, ФАС России был проанализирован вопрос о том, могут ли считаться взаимозаменяемыми магазины приложений, разработанные для других операционных систем для мобильных устройств, и был сделан вывод, что не могут. Поскольку операционная система *iOS*, разработанная корпорацией *Apple*, является закрытой системой и не представляется для лицензирования иным производителям мобильных устройств, кроме корпорации *Apple*, производители мобильных устройств в настоящее время имеют выбор между ОС *Android* и ОС *Windows Phone* (доля других операционных систем для мобильных устройств ничтожно мала). При этом переключение на магазин приложений, разработанный под другую операционную систему, невозможно без переключения на другую операционную систему.

ФАС России проанализировала реальную рыночную практику и пришла к выводу, что лишь крайне небольшое количество производителей мобильных устройств фактически производят мобильные устройства для последующей реализации в России на ОС *Windows Phone* или альтернативных операционных системах. Причем наибольшее количество таких устройств производилось компанией *Nokia*, которая контролируется производителем одной из альтернативных операционных систем (ОС *Windows Phone*) – корпорацией *Microsoft*. При этом фактические данные говорят о том, что переключения на другую операционную систему на практике почти не происходят, а те, которые имели место, были коммерчески неуспешны (например, попытка запуска *Samsung* собственной операционной системы *Tizen*).

Помимо сложностей для производителей мобильных устройств, связанных с переключением на другую операционную систему, были учтены и сложности для пользователей. Например, невозможен перенос приобретенных приложений с мобильного устройства, рабо-

тающего на одной операционной системе, на мобильное устройство, работающее на другой операционной системе. Вследствие этого переход производителя мобильных устройств на другую операционную систему будет означать потерю значительного количества лояльных пользователей, фактически теряющих при смене мобильного устройства ранее приобретенные ими приложения (и сделанные в них встроенные покупки).

(2) *Измерение рыночной власти/определение доминирующего положения*

Как отмечалось выше, вопрос измерения рыночной власти в сфере многосторонних рынков в соответствии с традиционными методами антимонопольного регулирования является непростым, особенно в ситуации, когда товар предоставляется (условно) бесплатно. Тем не менее ФАС России выработала подход, позволивший ей сделать вывод о наличии у *Google* рыночной власти и, следовательно, доминирующего положения.

Google Play – самый популярный и наиболее распространенный магазин приложений на ОС *Android*. ФАС России установила, что если на мобильном устройстве под управлением ОС *Android* отсутствует *Google Play*, такое устройство не будет коммерчески успешным у пользователей, поэтому все основные производители мобильных устройств на ОС *Android* вынуждены обращаться к *Google* за получением *Google Play*.

При этом *Google Play* в принципе предоставляется только производителям мобильных устройств[1]. Конечные пользователи мобильных устройств не имеют возможности самостоятельно загрузить магазин приложений *Google Play* из какого бы то ни было источника, т.е. не могут его использовать, если только он не предустановлен производителем на соответствующем мобильном устройстве. Кроме того, с помощью *Google Play* невозможно загрузить магазины приложений иных производителей[2].

ФАС России сделала вывод, что в сфере мобильных приложений и сервисов предустановка – это ключевой способ продвижения то-

[1] См.: http://source.android.com/source/faqs.html#if-i-am-not-a-manufacturer-how-can-i-get-google-play

[2] См. разд. 4.5 Соглашения *Google Play* о распространении программных продуктов (https://play.google.com/about/developer-distribution-agreement.html).

вара, обусловливающий коммерческий успех того или иного приложения. Как показали представленные в дело социологические исследования ВЦИОМ и «Ромир», подавляющее большинство пользователей пользуется тем, что предустановлено на устройстве или настроено по умолчанию. Лишь малая их часть загружает приложения самостоятельно (а в отношении *Google Play*, как отмечалось, это в принципе невозможно).

Поэтому ФАС России посчитала, что рыночную власть в рассматриваемом случае можно определить посредством количества устройств, на которых предустановлены магазины приложений (как некий аналог доли рынка в традиционном понимании).

Помимо этого, как отмечалось, ФАС России учла и наличие на рынке сильных косвенных сетевых эффектов, а также были учтены иные барьеры входа/экспансии, в том числе обусловленные собственными действиями/требованиями *Google*.

(3) *Существо злоупотребления доминирующим положением*

Ключевая практика, признанная ФАС России антиконкурентной, – это связывание доминирующего товара (магазина приложений *Google Play*) с иными товарами, которые могут обращаться на конкурентных рынках (отдельными приложениями и сервисами, входящими в состав *GMS*). ФАС России установила, что требование предустановки множества различных по функционалу приложений совместно с *Google Play* не было обусловлено технологическими причинами. Достаточно сказать, что даже если какое-либо из приложений из пакета *GMS* не предустановлено на устройстве, оно может быть самостоятельно загружено пользователем из магазина приложений *Google Play*.

С точки зрения негативных последствий для конкуренции от практики связывания ФАС России применила так называемую теорию перенесения рыночной власти (*leveraging theory*), признав, что *Google* распространила свою рыночную власть применительно к *Google Play* на иные собственные приложения, получая возможность предустановить их на большом количестве устройств бесплатно и без конкурентной борьбы. Путем связывания *Google* повышала для своих конкурентов стоимость конкуренции, что приводило к необходимости последним тратить существенные ресурсы для предустановки своих приложений либо пытаться предложить аналог *Google Play* и всех иных приложений, входящих в *GMS* (что заведомо невыполнимо).

При этом ФАС России учла, что пакетирование само по себе является допустимым способом продвижения товара. ФАС России указала в решении, что само по себе связывание не является нарушением, однако оно становится таковым, если пакетирование применяется доминирующим субъектом в качестве *единственного* способа продвижения своего доминирующего товара (возможность отдельного приобретения которого у покупателя отсутствует)[1]. То есть *Google* была признана злоупотребившей своим доминирующим положением не в силу самого по себе факта связывания, а поскольку у производителей мобильных устройств отсутствовала иная возможность получения *Google Play*, кроме как в составе пакета *GMS*.

Такой вид злоупотребления доминирующим положением, как пакетирование (связывание)[2], является хорошо разработанным в зарубежной антимонопольной практике и литературе. Как отмечалось выше, в сфере высоких технологий в ЕС уже имелись прецедентные дела в отношении корпорации *Microsoft* (дела в отношении *Windows Media Player* и *Internet Explorer*), не говоря уже о том, что и до дел в отношении *Microsoft* существовала хорошо проработанная правоприменительная практика в других областях (дела *Hilti*, *Tetra Pak* и др.).

В отличие от конкурентного права ЕС антимонопольных дел по связыванию в России практически не было. Фактически единственными прецедентами были дела против естественной монополии – РЖД. В одном показательном деле ОАО «РЖД» по умолчанию включало в стоимость билета на пассажирскую перевозку стоимость страховки

[1] В экономической теории данный вид связывания получил наименование «чистое связывание» (*pure bundling*).

[2] Понятия «пакетирование» (*bundling*) и «связывание» (*tying*), пришедшие из зарубежного права, в целом совпадают; под ними понимается такое явление, как «продажа в нагрузку», т.е. условием приобретения одного (доминирующего) товара является приобретение другого (недоминирующего) товара или нескольких товаров. Различия состоят в том, что связывание представляет собой неценовую практику, т.е. любую ситуацию, при которой совместное приобретение доминирующего и недоминирующего товара делается вынужденным или выгодным с использованием неценовых методов (через соответствующие требования в договорах, отказ в поставке доминирующего товара, технические особенности, делающие затруднительным или невозможным приобретение товаров по отдельности). Пакетирование представляет собой практику, при которой несколько товаров реализуется единовременно по единой цене. Несмотря на различия, антиконкурентный эффект у данных практик является одинаковым, более того, зачастую ценовые и неценовые факторы, способствующие практике пакетирования (связывания), используются доминирующими субъектами в совокупности. Поэтому для целей настоящей статьи данные понятия используются как синонимы.

от несчастных случаев, предоставляемой входящей в его группу страховой компанией. В другом деле ОАО «РЖД» включало в стоимость перевозки пассажиров в плацкартном вагоне стоимость дополнительной услуги – использования постельного белья.

Несмотря на то что связывание как вид злоупотребления доминирующим положением напрямую не предусмотрено ст. 10 Закона о защите конкуренции, закрепленное в данной статье общее понятие злоупотребления дало ФАС России возможность применить концепцию связывания в рассматриваемом деле.

Помимо собственно связывания, ФАС России признала антиконкурентными и иные вытекающие из него практики. В частности, то, что предустановка *Google Play* требовала от производителей мобильных устройств соблюдения дополнительных ограничительных требований *Google*: (1) приоритетного размещения иконок приложений *Google* на первом экране мобильного устройства; (2) настройки поиска *Google* «по умолчанию» во всех точках ввода поискового запроса на мобильном устройстве и (3) запрета на предустановку приложений, разработанных конкурентами *Google*. Данные практики *Google* были признаны ФАС России повлекшими ограничение конкуренции и нарушение интересов конкурентов *Google*, являющихся разработчиками мобильных приложений и сервисов, что выразилось в первую очередь в прямых отказах производителей мобильных устройств предустанавливать мобильные приложения конкурентов *Google*.

В частности, условие о приоритетном размещении мобильных приложений на экране мобильного устройства ограничивало возможность конкурентов договариваться с производителями о размещении своих приложений на условиях, аналогичных тем, на которых предустанавливались приложения *Google*. Приоритетное размещение на экране обеспечивает более высокую частоту использования приложений по сравнению с теми приложениями, которые размещены на менее выгодных местах на экране. Условия о настройке поиска *Google* в качестве поиска, по умолчанию, во *всех* точках доступа на устройстве и о запрете предустановки приложений конкурентов имеют непосредственный вытесняющий эффект (представляют собой «прямое исключение» (*naked exclusion*)).

В итоге ФАС Росси пришла к выводу о том, что *Google* получала преимущество перед конкурентами не за счет конкурентной борьбы, а исключительно за счет своей рыночной власти в отношении *Google Play*.

(4) *Исключение для осуществления исключительных прав в отношении объектов интеллектуальной собственности*

В ч. 4 ст. 10 Закона о защите конкуренции содержится исключение для действий доминирующих субъектов, сформулированное следующим образом: «Требования настоящей статьи (запреты для доминирующих субъектов. – *Е.Х.*) не распространяются на действия по осуществлению исключительных прав на результаты интеллектуальной деятельности и приравненные к ним средства индивидуализации юридического лица, средства индивидуализации продукции, работ или услуг».

Очевидно, что в рамках рассмотрения дела *Google* ссылалась на данное исключение в обоснование правомерности своих практик.

В частности, *Google* занимала позицию о том, что все ее действия, признанные злоупотреблением доминирующим положением, были действиями по осуществлению исключительных прав на результаты интеллектуальной деятельности (к которым относится собственно магазин приложений *Google Play* как программа для ЭВМ), а заключаемые с производителями мобильных устройств соглашения являлись лицензионными[1]. Кроме того, поскольку данные соглашения подчинены иностранному, а не российскому праву, то и понятие осуществления исключительных прав должно толковаться в соответствии с иностранным правом.

ФАС России, в том числе с учетом правовых заключений, подготовленных Московским государственным юридическим университетом им. О.Е. Кутафина (МГЮА) (проф. М.А. Рожкова) и Институтом законодательства и сравнительного правоведения (доц. В.О. Калятин), пришла к выводу о том, что спорные действия *Google* выходят за пределы осуществления его исключительных прав, и, следовательно, к ним не подлежит применению исключение, предусмотренное ч. 4 ст. 10 Закона о защите конкуренции. ФАС России также сочла необходимым толковать понятие «осуществление исключительных прав» в соответствии с российским, а не иностранным правом.

[1] Сами положения договоров, заключаемых *Google* с производителями мобильных устройств на *Android*, являются конфиденциальными. Тем не менее публично доступны два договора о продвижении мобильных приложений *Google* (*Mobile Application Distribution Agreements*), заключенные *Google* с *Samsung* и *HTC* в редакции 2011 г., которые были раскрыты в рамках разбирательства по делу *Oracle America v. Google* в США. Дальнейшие отсылки к договору *MADA* сделаны на публично доступные тексты договоров.

Аргументация ФАС России состояла в следующем. Исключение по ч. 4 ст. 10 Закона о защите конкуренции означает, что обладателя исключительного права на определенный результат интеллектуальной деятельности нельзя признать лицом, занимающим доминирующее положение, исключительно в силу наличия такого исключительного права, а действия по распоряжению своим исключительным правом, в том числе путем заключения лицензионного договора, не подпадают под антимонопольные запреты.

Однако это не означает, что вообще любые положения (ограничительные условия), содержащиеся в договоре, в рамках которого осуществляется передача лицензии, являются автоматически относящимися к лицензионным правоотношениям и не подлежат оценке в соответствии с антимонопольным законодательством.

Осуществлением исключительного права является реализация заложенных в соответствующем субъективном праве возможностей в предусмотренных законом пределах. В соответствии с п. 1 ст. 1229 ГК РФ правообладатель наделен правом использовать результат интеллектуальной деятельности по своему усмотрению любым не противоречащим закону способом, распоряжаться исключительных правом (в частности, путем отчуждения в полном объеме или предоставления права использования третьему лицу), а также по своему усмотрению разрешать или запрещать другим лицам использование результата интеллектуальной деятельности. При этом ограничительные требования *Google* при предоставлении магазина приложений *Google Play* подлежат оценке только с точки зрения правомочия распоряжения исключительным правом, поскольку *Google* предоставляла магазин приложений для его использования (предустановки) третьим лицам.

В соответствии с закрепленным в российском праве подходом лицензионное правоотношение представляет собой предоставление одним лицом (правообладателем) другому лицу (лицензиату) права использования объекта исключительных прав на определенный срок, в рамках согласованной территории и в пределах тех способов использования, которые возможны для соответствующего объекта в силу его природы, а также допустимы в соответствии с российским законодательством.

В частности, в отношении программ для ЭВМ (к которым относится *Google Play*) перечень способов использования приведен в п. 2 ст. 1270 ГК РФ (например, воспроизведение, доведение до всеоб-

щего сведения и пр.). Указанный перечень не является закрытым, использование объекта интеллектуальных прав возможно и другими способами, однако все они подразумевают совершение определенных операций либо с программой для ЭВМ (например, создание копий), либо с материальным носителем, содержащим такую программу (например, продажа носителя). Указание на «предусмотренные договором пределы» следует понимать в значении подп. 2 п. 6 ст. 1235 ГК РФ как согласование в договоре конкретных способов использования результата интеллектуальной деятельности, а также территории и срока, в пределах которых такое использование разрешается.

Однако соглашения с *Google* имели более широкий предмет, нежели простое предоставление лицензии на приложения из состава *GMS*; основным элементом соглашений являлись обязательства производителей мобильных устройств по продвижению приложений и сервисов *Google* для мобильных устройств. Иными словами, предмет соглашений *Google* был шире, чем предоставление лицензии. Даже из самого наименования договоров, которые *Google* заключала с производителями мобильных устройств, можно сделать вывод о том, что они носили смешанный характер и не могли квалифицироваться как обычный лицензионный договор. Так, договор *MADA* («Договор дистрибуции мобильных приложений») в своем наименовании содержит указание на обязательство производителей по продвижению мобильных приложений, а вовсе не на предоставление им права использования результатов интеллектуальной деятельности.

Исходя из вышеизложенного ФАС России пришла к выводу о том, что соглашения *Google* являются смешанными, а элемент предоставления лицензии – вспомогательным (необходим для того, чтобы производители мобильных устройств могли осуществить свою основную обязанность по продвижению приложений и сервисов *Google*). При этом ограничительные условия, признанные ФАС России злоупотреблением доминирующим положением (в частности, запрет предустановки приложений и сервисов конкурентов, требование о преимущественном размещении приложений и сервисов *Google*, требование о настройке поиска *Google* в качестве единственного поиска по умолчанию на устройствах), относились именно к основному предмету соглашений – продвижению приложений и сервисов *Google*. ФАС России сделала вывод о том, что запреты и ограничения *Google* являлись самостоятельными обязательствами – требованиями к дистрибуции мобильных приложений, сходными по своему характеру с обязатель-

ствами об оказании услуг. Поскольку данные ограничительные требования не входят в состав лицензионных правоотношений, они были признаны не подпадающими под исключение по ч. 4 ст. 10 Закона о защите конкуренции.

Применительно к самой практике связывания обязанность использовать все программы для ЭВМ исключительно совместно также была признана выходящей за пределы осуществления исключительных прав на каждую из программ для ЭВМ, входящую в пакет. Требование об использовании одного результата интеллектуальной деятельности (РИД 1) только при одновременном использовании другого результата интеллектуальной деятельности (РИД 2) не является элементом осуществления исключительного права на РИД 1, поскольку никак не касается определения способов и пределов использования РИД 1.

ФАС России в этой связи указала: «Самостоятельным объектом исключительных прав является каждая конкретная программа для ЭВМ (приложение), осуществление исключительных прав на которые охватывает только действия по использованию данной программы, но не весь процесс коммерческой деятельности, связанный с ним. Соответственно в предмет договора, оформляющего предоставление права использования программы для ЭВМ, может включаться только описание пределов использования программы. Любые иные вопросы взаимоотношений сторон, которые также может урегулировать лицензионный договор, будут выходить за пределы лицензионных правоотношений».

Правомерность позиции ФАС России подтверждается имеющейся судебной практикой. В частности, по делу *Ангстрем* (дело № А40-3954/10-149-52) Президиум ВАС РФ в Постановлении от 29.11.2011 № 6577/11 поддержал доводы кассационной инстанции о том, что не подпадает под исключение по ч. 4 ст. 10 Закона о защите конкуренции условие об эксклюзивности в лицензионном договоре, не касающееся непосредственно права на использование результата интеллектуальной деятельности. Аналогичная позиция была сформулирована кассационной инстанцией по знаковому делу *Teva* (дело № А40-42997/2014) и впоследствии поддержана ВС РФ.

Применительно к аргументу *Google* о том, что понятие «осуществление исключительных прав» должно толковаться в соответствии с иностранным правом, которому подчинены соглашения *Google* с производителями мобильных устройств, ФАС России заняла следующую позицию.

В соответствии с п. 2 ст. 1231 ГК РФ при признании исключительного права на результат интеллектуальной деятельности или 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 ГК РФ не предусмотрено иное.

Иными словами, если иностранные лица заключают соглашение об использовании результата интеллектуальной деятельности и подчиняют его иностранному праву, то к их договорным отношениям действительно будет применяться иностранное право, однако это никак не повлияет на применение российского права к объему и порядку осуществления права на такой результат интеллектуальной деятельности на территории России. Стороны не могут, подчинив договор иностранному праву, предусмотреть, что объем предоставленного права использования программы для ЭВМ в России будет определяться этим иностранным правом, поскольку само по себе предоставление права использования на территории России оказывается возможным исключительно в силу того, что на основании указанного выше положения ГК РФ право на программы для ЭВМ, созданные за рубежом, признаются в России и объем такого права определяется именно правом России.

Кроме того, при применении исключения, предусмотренного ч. 4 ст. 10 Закона о защите конкуренции, ФАС России основывалась на понятии «осуществление исключительных прав» согласно российскому праву, поскольку данное исключение содержится именно в *российском* законодательстве. В связи с тем, что Закон о защите конкуренции основан на ГК РФ (см. ч. 1 ст. 2 Закона о защите конкуренции), понятие «осуществление исключительных прав» для целей оценки применимости ч. 4 ст. 10 Закона о защите конкуренции подлежит толкованию в соответствии с ГК РФ, несмотря на то, что договор в отношении того или иного объекта интеллектуальной собственности может быть подчинен иностранному праву.

* * *

В данном деле были также затронуты многочисленные иные юридические и экономические вопросы, которые сделали это дело беспре-

цедентным (по крайней мере в российской практике) по сложности и многоаспектности. Как отмечалось, закрытый характер рассмотрения этого дела препятствует анализу всех вопросов в необходимых для этого подробностях. Тем не менее представляется, что даже вышеизложенное позволяет сделать вывод о том, что ФАС России смогла разобраться в крайне сложной индустрии информационных технологий и применить к ней традиционные методы антимонопольного регулирования без ущерба для высоких стандартов доказывания, принятых в ЕС и других ведущих мировых юрисдикциях.

Пристатейный библиографический список:

1. *Юсупова Г.Ф.* ФАС против Google: экономический анализ для особых рынков // Экономическая политика. 2016. Т. 11. № 6. С. 82–99.

2. *B. Edelman and D. Geradin.* 'Android and competition law: exploring and assessing Google's practices in mobile' [2016] // European Competition Journal. P. 1–36.

3. *D. O'Connor.* 'Understanding Online Platform Competition: Common Misunderstandings', *Internet Competition and Regulation of Online Platforms* (May 2016) // Competition Policy International. P. 9–10.

Б.С. Бембеева

ПРАВО НА ЗАЩИТУ ПЕРСОНАЛЬНЫХ ДАННЫХ И РАЗЛИЧНЫЕ КАТЕГОРИИ ПЕРСОНАЛЬНЫХ ДАННЫХ

Аннотация. *В практике Европейского суда по правам человека защита персональных данных рассматривается как часть права на неприкосновенность частной жизни, которое гарантировано ст. 8 Конвенции по правам человека. В статье анализируется практика по делам, в которых категории персональных данных можно разграничить в зависимости от источника информации.*

Ключевые слова: *персональные данные, право на неприкосновенность частной жизни, Европейский Суд по правам человека.*

В 1890 г. судьями Верховного суда США Льюисом Брандейсом и Сэмюэлем Уорреном была опубликована статья «Право на частную жизнь» (*The Right to Privacy*), в которой впервые был использован термин *privacy*[1]. Изначально данный термин трактовался американскими судьями как свобода личности от вмешательства государства. Они подразумевали под этим право на автономность (*the right to be let alone*) и использовали его преимущественно в пространственном аспекте[2]. Необходимо отметить, что право на автономность отождествлялось с правом на жизнь и правом на защиту собственности: «*The right to life has come to mean the right to enjoy life, – the right to be let alone*»[3]. Но сегодня право на уважение частной жизни является отдельной категорией, которая не ограничивается только личным пространством, а включает в себя и информационную «среду обитания» человека.

Стоит отметить, что с одной стороны, глобализация, научно-техническое развитие, информатизация общества создают условия для даль-

[1] *Samuel D. Warren, Louis D. Brandeis.* The Right to Privacy // Harvard Law Review. 1890. Vol. 4, No. 5. P. 193.

[2] *Глинская Н.П.* Юридический термин *privacy* как предмет системно-динамического исследования // Вестник Московского университета. Серия 19: Лингвистика и межкультурная коммуникация. 2010. № 2. С. 36.

[3] *Samuel D. Warren, Louis D. Brandeis.* The Right to Privacy // Harvard Law Review. 1890. Vol. 4, No. 5. P. 193.

нейшего развития индивида как личности, для полноценной и эффективной реализации его прав и свобод. С другой стороны, происходящие изменения способствуют созданию предпосылок для нарушения права человека на уважение частной жизни. В частности, в ст. 11 Венской декларации и Программы действий отмечается, что прогресс в области информационных технологий может иметь потенциально негативные последствия для неприкосновенности, достоинства и прав человеческой личности[1]. Это связано с тем, что современные технологии способствуют расширению возможностей обработки и распространения информации, что в значительной степени обостряет проблему неприкосновенности частной жизни человека и вмешательства в нее со стороны государства.

Как отмечалось в докладе Управления Верховного комиссара ООН по правам человека, во многих государствах практика указывает на отсутствие надлежащего национального законодательства, слабые процедурные гарантии и неэффективный надзор, что в совокупности приводит к отсутствию ответственности за произвольное или незаконное вмешательство в частную жизнь человека со стороны государства[2].

Вместе с тем нельзя не замечать, что защищаемые права, существующие вне цифровой среды, постепенно получают правовую регламентацию. Тогда как по-иному ситуация обстоит с правами на неприкосновенность частной жизни, связанными с цифровым пространством, и прежде всего правом на защиту персональных данных. Право на защиту персональных данных не закреплено в международно-правовых актах как самостоятельное и обычно рассматривается как один из аспектов защиты частной жизни, формируясь под воздействием судебной практики международных судов.

Значительное влияние на развитие международного и национального законодательства в области защиты персональных данных оказывает ЕСПЧ. Практика ЕСПЧ развивает современное представление о правах человека и устанавливает стандарты их обеспечения и защиты: «Практику ЕСПЧ, в ходе которой вырабатываются правовые позиции Суда, характеризует привнесение в современное научно-технологическое

[1] Всемирная конференция по правам человека. Венская декларация и Программа действий. Июнь 1993 г. Нью-Йорк: Организация Объединенных Наций, 1995. С. 21–60.

[2] Управление Верховного комиссара ООН по правам человека (УВКПЧ) URL: http://webcache.googleusercontent.com/search?q=cache:V9hnOlGUwToJ:www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session27/Documents/A-HRC-27-37_en.doc+&cd=1&hl=ru&ct=clnk&gl=ru (дата обращения: 28.03.17).

развитие фундаментальных ограничителей, что позволяет осуществить баланс между интересами научно-технологического развития и интересами человека»[1].

В этих условиях несомненный интерес представляет прецедентная практика ЕСПЧ по толкованию норм, содержащихся в ст. 8 Конвенции по правам человека, которая закрепляет право на уважение частной и семейной жизни: «1. Каждый имеет право на уважение его личной и семейной жизни, его жилища и его корреспонденции.

2. Не допускается вмешательство со стороны публичных властей в осуществление этого права, за исключением случая, когда такое вмешательство предусмотрено законом и необходимо в демократическом обществе в интересах национальной безопасности и общественного порядка, экономического благосостояния страны, в целях предотвращения беспорядков или преступлений, для охраны здоровья или нравственности или защиты прав и свобод других лиц».

Анализ практики ЕСПЧ позволил выделить несколько категорий персональных данных, вопрос о защите которых не раз ставился перед Судом. Предварить обзор о разновидностях персональных данных необходимо ссылкой на Конвенцию о защите физических лиц при автоматизированной обработке персональных данных 1981 г. (далее – Конвенция о персональных данных), согласно которой под персональными данными следует понимать «любую информацию об определенном или поддающемся определению физическом лице»[2].

ДНК и отпечатки пальцев

Эти биометрические данные признаются неповторимым и особенным источником данных о человеке. Осуществление незаконного сбора и хранения таких данных, безусловно, противоречит ст. 8 Конвенции по правам человека. И здесь следует обратить внимание на то, что Рекомендация Совета Европы № R(87)15, регламентирующая вопросы использования информации персонального характера в ходе деятельности полиции, допускает возможность хранения подобной информации с определенными ограничениями. В частности,

[1] *Шугуров М.В.* Защита прав человека в условиях современного научно-технического прогресса: практика Европейского суда по правам человека // Международное публичное и частное право. 2011. № 1. С. 5.

[2] Конвенция о защите физических лиц при автоматизированной обработке персональных данных от 28.01.1981 // Бюллетень международных договоров. 2014. № 4.

предусмотрена обязанность принимать все необходимые меры, чтобы информация личного характера, хранящаяся для целей деятельности полиции, удалялась, если в ней отпадает объективная необходимость[1].

Принцип необходимости хранения информации личного характера в зависимости от преследуемых целей нашел отражение в нескольких решениях ЕСПЧ.

В деле «*S. и Марпер против Соединенного Королевства*»[2] ЕСПЧ, ссылаясь на ст. 7 Конвенции о персональных данных, напомнил, что национальное законодательство государств – участников Конвенции должно предусматривать достаточные гарантии эффективной защиты хранящихся персональных данных от ненадлежащего использования и злоупотреблений.

Заявители по этому делу обвинялись в совершении уголовных преступлений, но впоследствии были оправданы национальным судом. Во время расследования этих преступлений у обвиняемых были сняты образцы отпечатков пальцев, взяты анализы ДНК, а также образцы их клеток. После прекращения уголовного преследования в отношении обоих заявителей они обратились к полиции с требованием уничтожить взятые биологические материалы из национальной базы данных (в которой подобная информация хранилась бессрочно). Но полиция отказалась это сделать, ссылаясь на ст. 64 Акта о полиции и доказательствах по уголовным делам 1984 г., согласно которой отпечатки пальцев или образцы ДНК могли храниться после того, как они были использованы для достижения цели, ради которой они были взяты[3].

ЕСПЧ поддержал позицию заявителей, отметив, что хранение отпечатков пальцев и ДНК по делам, в которых обвиняемые по уголовным делам были оправданы или их уголовное преследование было прекращено, является нарушением ст. 8 Конвенции по правам человека. Ссылаясь на решение по делу «*Леандер против Швеции*»[4], ЕСПЧ отметил, что даже простое хранение информации, относящейся к личной жиз-

[1] Recommendation No R (87) 15 of the Committee of Ministers to Member States regulating the use of personal data in the police sector // OSCE POLIS URL: https://goo.gl/qiz6Ey (дата обращения: 15.04.2017).

[2] S. and Marper v. The United Kingdom, постановление от 04.12.2008, жалобы № 30562/04 и № 30566/04.

[3] Примечательно, что в более ранней редакции этого акта закона возможность уничтожения подобных данных осуществлялась при первой же возможности после окончания производства по делу.

[4] Leander v. Sweden, постановление от 27.03.1987, жалоба № 9248/81. § 48.

ни человека, является вмешательством государства в осуществление его прав по смыслу положений ст. 8 Конвенции по правам человека. По мнению ЕСПЧ, профили ДНК предоставляют государству необходимые средства для установления генетических связей между большим количеством людей, что само по себе достаточно для вывода о том, что их хранение представляет собой вмешательство государства в осуществление этими людьми права на неприкосновенность их личной жизни[1]. Что касается отпечатков пальцев, то Суд подчеркнул, что они объективно содержат уникальную информацию о человеке, а в ряде случаев позволяют точно идентифицировать его личность. Таким образом, это может негативно отразиться на неприкосновенности частной жизни, а хранение подобной информации без согласия лица, которому она принадлежит, нельзя назвать нейтральным или незначительным[2].

При этом ЕСПЧ не отрицает того, что в некоторых случаях вмешательство в право заявителя на неприкосновенность частной жизни может быть признано законным. Но это допустимо лишь при соблюдении некоторых условий, на которые Суд специально обращает внимание.

Так, заявитель по делу «*Ван дер Вельден против Нидерландов*»[3] обвинялся в вымогательстве и содержался в одном из исправительных учреждений г. Дордрехта на основании медицинских заключений сразу нескольких врачей, которые отмечали высокий риск возможности рецидива у заявителя. Государственный прокурор на основании национального законодательства – ст. 2 § 1 Закона о взятии анализа ДНК у лиц, осужденных за уголовные преступления, издал приказ об отборе клеточного материала для определения ДНК-профиля заявителя.

По мнению заявителя, приказ государственного прокурора об отборе у него клеточного материала и хранение полученного образца ДНК-профиля в государственной базе данных, по сути, повлек для него дополнительное наказание по смыслу ст. 7 Конвенции по правам человека, поскольку он уже содержался в исправительном учреждении. Он также обратил внимание на то, что вопрос о его ДНК-профиле вовсе не поднимался во время непосредственного проведения расследования уголовного преступления, что указывало на применение дискриминационных мер в отношении него. Это и стало основанием

[1] *S. and Marper v.* The United Kingdom, постановление от 04.12.2008, жалобы № 30562/04 и № 30566/04, § 75.

[2] Там же. § 84.

[3] Van der Velden v. Netherlands, решение по вопросу приемлемости жалобы от 07.12.2006 по делу жалоба № 29514/05.

для обращения в ЕСПЧ с жалобой на нарушение ст. 8 и 14 Конвенции по правам человека.

ЕСПЧ признал эту жалобу неприемлемой. При этом Суд отметил, что в данном случае хранение ДНК не являлось вмешательством в частную жизнь, так как это было предусмотрено законом, преследовало правомерные цели предупреждения преступлений и защиты прав и свобод других лиц. Кроме того, по мнению ЕСПЧ, рассматриваемое вмешательство было сравнительно незначительным. В своем решении о неприемлемости этой жалобы ЕСПЧ отметил несомненную пользу, принесенную базой ДНК-профилей в сфере обеспечения правопорядка за последние годы. Также Суд указал, что заявитель может извлечь и некоторую выгоду из включения его ДНК-профиля в национальную базу данных, учитывая высокий риск рецидива: в будущем он может быть быстро исключен из списка лиц, подозреваемых в совершении преступлений, что осуществимо путем сравнения его биометрических данных с другими полученными образцами.

Образцы голоса, полученные с помощью прослушивающих устройств

Правовая регламентация использования такой категории информации о человеке, как голосовые данные, составляет одну их проблемных частей в законодательстве многих государств. Вследствие этого на рассмотрение ЕСПЧ передавались дела, связанные со сбором этих персональных данных в ходе оперативно-розыскных мероприятий.

В деле «*P.G. and J.H. против Соединенного Королевства*»[1] устройства секретного прослушивания были установлены в квартире одного из заявителей. Заявители подозревались в подготовке вооруженного ограбления и были задержаны полицией уже после установки прослушивающих устройств. В полицейском участке их допрос был также записан на скрытое прослушивающее устройство, а полученные образцы голосов были отправлены эксперту, который подтвердил их схожесть с образцами голосовых данных, полученных путем секретного прослушивания в квартире.

Заявители обратились с жалобой в ЕСПЧ, указывая на нарушения ст. 6, 8 и 13 Конвенции по правам человека действиями национальных властей при проведении расследования. Заявители, отвечая на вопро-

[1] *P.G. and J.H. v. The United Kingdom*, постановление от 25.09.2001, жалоба № 44787/98.

сы полицейских в участке, не могли знать, что их голос записывается с целью сравнения полученных данных с уже записанными образцами. Полученные голосовые данные впоследствии использовались полицией в суде в качестве доказательств совершения ими уголовного преступления. И, по сути, сам факт того, что заявители отвечали на вопросы полицейских, в данном случае стало свидетельствованием их против самих себя.

В свою очередь, государство-ответчик утверждало, что использование прослушивающих устройств не влечет каких-либо нарушений Конвенции, поскольку эти записи не были сделаны для получения информации непосредственно о частной жизни заявителей. По мнению правительства, записи, сделанные во время допроса заявителей, представляли собой часть формального процесса уголовного правосудия и осуществлялись в присутствии по крайней мере одного офицера полиции[1].

ЕСПЧ пришел к выводу, что установка прослушивающих устройств в квартире и секретная запись допроса на диктофон представляют собой нарушение ст. 8 Конвенции по правам человека. При этом Суд отметил, что в соответствующее время в правовой системе государства-ответчика не существовало законодательного акта, который регулировал использование скрытых подслушивающих устройств полицией в их собственных помещениях. Запись и анализ их голосов по этому поводу все равно должны рассматриваться как обработка персональных данных о заявителях. В связи с этим Суд сделал вывод о том, что в данном случае имело место вмешательство государства в частную жизнь заявителя, что является нарушением ст. 8 Конвенции по правам человека.

В деле «*Веттер против Франции*»[2] заявитель обвинялся в совершении убийства и был приговорен к 20 годам тюрьмы. Обвинения против него основывались на данных, полученных полицией путем установки прослушивающих устройств в квартире жертвы, которую регулярно посещал заявитель.

ЕСПЧ при рассмотрении этого дела отметил, что национальное законодательство Франции хотя и содержит некоторые положения о перехвате телефонных разговоров, но не регламентирует порядок

[1] При этом необходимо отметить, что добровольность дачи показаний, по мнению ЕСПЧ, не распространяется на получение документов и образцов биологического происхождения у живого человека (см. подробнее: Saunders v. The United Kingdom, постановление от 17.12.1996, жалоба № 19187/91).

[2] *Vetter v. France*, постановление от 31.05.2005, жалоба № 59842/00.

установления прослушивающих устройств. В частности, во французском законодательстве не уточняется свобода усмотрения государства в отношении использования прослушивающих устройств, а также процедура, с помощью которой должно осуществляться использование полученных голосовых данных в целях расследования преступлений. Исходя из этого ЕСПЧ признал, что в этом деле имело место нарушение ст. 8 Конвенции по правам человека.

Данные, полученные с помощью системы глобального позиционирования (GPS)

Нарушение ст. 8 Конвенции по правам человека будет отсутствовать, если в деле превалируют вопросы публичных интересов общества, национальной безопасности государства и если вмешательство государства в частную жизнь соответствует основным положениям п. 2 ст. 8 Конвенции.

В деле «*Узун против Германии*»[1] заявитель был причастен к взрывам, совершенным левой экстремистской группировкой, что было подтверждено данными, полученными системой глобального позиционирования (*GPS*), которое было установлено в автомобиле по решению национальных властей. Полиции пришлось прибегнуть к использованию *GPS* после того, как заявитель вместе со своим предполагаемым сообщником уничтожил установленные ранее передатчики слежения в машине и практически перестал использовать мобильную связь, скрываясь от правосудия.

ЕСПЧ подтвердил, что подобное вмешательство соответствовало закону, преследовало законные цели предупреждения преступлений и защиты прав и свобод других лиц и было необходимо в демократическом обществе. Суд подчеркнул, что слежение за передвижением заявителя в общественных местах посредством GPS необходимо отличать от других методов визуального или акустического наблюдения, поскольку оно раскрывает меньше информации о поведении, мнении или чувствах человека и тем самым составляет меньшее вмешательство в его частную жизнь. В связи с этим ЕСПЧ не счел необходимым применять те же строгие гарантии против злоупотреблений, которые он разработал в своей прецедентной практике в отношении перехвата данных, полученных с помощью подобных систем.

[1] *Uzun v. Germany*, постановление от 02.09.2010, жалоба № 35623/05.

Также ЕСПЧ признал, что единодушные выводы национальных судов о том, что наблюдение с помощью использования данных *GPS* было основано на национальном законодательстве, были разумно предвидимыми, поскольку соответствующие положения предусматривали использование технических средств, в частности, «для обнаружения местонахождения правонарушителя». Кроме того, в национальном законодательстве Германии установлены строгие стандарты авторизации *GPS*-наблюдения: оно может быть установлено только против лица, подозреваемого в совершении тяжкого уголовного преступления. В этом деле, по мнению ЕСПЧ, был соблюден и принцип пропорциональности: национальные власти начали использовать *GPS*-наблюдение только после того, как остальные методы оказались неэффективными, продолжительность наблюдения составило около трех месяцев, и было активным только в момент использования заявителем своей машины.

Наблюдение за использованием Интернета, рабочих телефонов и электронной почты

Вопрос о правомерности наблюдения за использованием телефонов, электронной почты и Интернета рассматривался в деле «*Коплэнд против Соединенного Королевства*»[1]. Заявительница по данному делу занимала должность личного помощника директора в одном из учреждений высшего образования, которое одновременно являлось государственным органом (колледж, в котором работала заявительница, имел статус публичной организации, находящейся в государственном ведении). Как было установлено впоследствии, телефон заявительницы, ее электронная почта, а также вообще использование ею Интернета были подвергнуты наблюдению с целью установить, не осуществляет ли заявительница использование технического оборудования колледжа в личных целях. В частности, производился анализ телефонных счетов колледжа, которые содержали номера телефонов, по которым осуществлялись звонки, хранилась информация о датах телефонных звонков и их стоимости. В отношении использования Интернета с рабочего места производилось наблюдение за просмотренными страницами, а также времени, датах и продолжительности таких просмотров. Подобной проверке подверглась также личная корреспонденция заявительницы, о чем она не подозревала.

[1] *Copland v. the United Kingdom*, постановление от 03.04.2007, жалоба № 62617/00.

По смыслу ст. 8 Конвенции по правам человека государство несет на себе негативное обязательство воздерживаться от вмешательства в частную жизнь человека.

Государство-ответчик по этому делу придерживалось позиции, согласно которой получение таким образом информации, как и сама эта информация, не представляло собой вмешательство в частную жизнь и корреспонденцию заявительницы. Правительство указывало, что мониторинг сводился к анализу автоматически генерируемой информации, чтобы определить, использовались ли средства колледжа в личных целях; в отличие от упомянутого дела «*P.G. and J.H. против Соединенного Королевства*» фактического перехвата информации и дальнейшей ее переработки не происходило. Причем, по мнению государства-ответчика, в том случае, если подобные действия ЕСПЧ все же признает вторжением в частную жизнь, то такое вмешательство является оправданным по смыслу п. 2 ст. 8 Конвенции по правам человека.

ЕСПЧ пришел к выводу, что телефонные звонки, электронные сообщения и использование Интернета с рабочего места, по сути, включаются в категории «частная жизнь» и «корреспонденция». Заявительница не была предупреждена работодателем о том, что ее деятельность будет каким-либо образом отслеживаться. Она имела законные основания полагать, что использование рабочего оборудования в личных целях останется незамеченным. Таким образом, сбор и хранение информации, полученной исходя из такого вида наблюдения, были расценены Судом как вмешательство в частную жизнь и соответственно нарушающими ст. 8 Конвенции по правам человека.

К противоположному выводу ЕСПЧ пришел в ходе рассмотрения дела «*Барбулеску* против Румынии»[1]. Заявитель по настоящему делу был уволен работодателем после того, как было обнаружено, что он вел личную переписку в одном из мессенджеров с рабочего оборудования в течение рабочих часов. Работники этой компании уведомлялись о полном запрете использовать рабочее оборудование в личных целях – соответствующее положение содержалось в локальных актах компании.

ЕСПЧ подчеркнул, что помимо негативного обязательства воздерживаться от вмешательства в частную жизнь граждан, установленного ст. 8 Конвенции по правам человека, на государства – участников Кон-

[1] *Bărbulescu v. Romania*, постановление от 12.01.2016, жалоба № 61496/08.

венции возложены и позитивные обязательства, состоящие в принятии определенных мер по защите права на неприкосновенность частной жизни. Граница между позитивными и негативными обязательствами государства не поддается точному определению. В обоих случаях следует учитывать баланс между конкурирующими интересами, который может включать личные и общественные интересы, которые расцениваются с точки зрения свободы усмотрения государства. Однако государства – участники Конвенции обязаны устанавливать достаточно четкие правила, регулирующие использование Интернета на рабочем месте.

В настоящем деле ЕСПЧ признал, что жалоба заявителя должна быть рассмотрена с точки зрения позитивных обязательств государства, поскольку он был нанят частной компанией, за действия которой не может быть ответственно государство. Исходя из этого ЕСПЧ не нашел в этом случае нарушений ст. 8 Конвенции.

С точки зрения позитивных обязательств государства следует обратить внимание на дело «*K.U. против Финляндии*»[1], в котором ЕСПЧ признал нарушение ст. 8 Конвенции по правам человека. Согласно обстоятельствам дела лицо, так и оставшееся неизвестным, поместило объявление сексуального характера на сайте знакомств от имени несовершеннолетнего лица (заявителя). Объявление содержало информацию о возрасте, годе рождения и физических характеристиках заявителя и указывало, что он искал интимных отношений с мужчиной. Оно также включало ссылку на страницу в Интернете, где можно было найти фотографию и номер телефона этого несовершеннолетнего. Соблюдая правила о конфиденциальности, хостинг-провайдер отказался раскрывать информацию о лице, разместившем объявление на сайте.

ЕСПЧ подчеркнул, что в данном случае имеет место нарушение неприкосновенности частной жизни несовершеннолетнего заявителя, которое могло привести к негативным последствиям в виде домогательств со стороны педофилов, создавало потенциальную угрозу его физическому и душевному благополучию. Суд отметил, что пользователи различных средств коммуникации и интернет-услуг должны иметь правовые гарантии неприкосновенности их частной жизни.

[1] *K.U. v. Finland*, постановление от 02.12.2008, жалоба № 2872/02.

Использование данных, полученных посредством фото- и видеосъемки

В практике ЕСПЧ встречаются дела, которые заканчиваются соглашениями о дружественном урегулировании, как это предусматривает ст. 39 Конвенции.

Например, в деле «*Фриедл против Австрии*»[1] заявитель был одним из организаторов демонстрации, направленной на привлечение внимания общественности к проблемам бездомных. Во время проведения демонстрации участники готовили еду, ели и спали на зонах для пешеходов, что стало причиной многочисленных жалоб от горожан. В соответствии с национальным законодательством Австрии любая демонстрация требует соответствующего разрешения, которое должны получить организаторы публичного мероприятия. Проводимая демонстрация требовала разрешения в соответствии с разд. 82 (1) Закона о дорожном движении, который категорически запрещает любые препятствия для пешеходных зон. Национальные власти настаивали на том, чтобы участники демонстрации покинули занимаемое место, что привело к противостоянию. В итоге полиция сделала фотографии демонстрантов для дальнейшего расследования инцидента. Заявитель, являющийся одним из участников демонстрации, счел, что его фотографии были сделаны полицией в индивидуальном порядке с целью идентификации его личности. С жалобой на нарушение права на защиту персональных данных заявитель обратился в Конституционный суд Австрии, но тот вынес решение, в котором признал, что не обладает достаточной юрисдикцией в вопросах использования персональных данных, полученных путем фотосъемки.

К моменту рассмотрения дела в ЕСПЧ в Австрии был принят Закон о службе безопасности, согласно которому независимые административные трибуналы приобрели юрисдикцию в вопросах, поднятых заявителем перед Конституционным судом Австрии. В связи с этим государство-ответчик подняло вопрос об исключении жалобы из списка рассматриваемых ЕСПЧ дел, на что не поступило возражений со стороны заявителя. Таким образом, исход дела был решен посредством дружественного урегулирования.

[1] *Friedl v. Austria*, решение об исключении жалобы из списка рассматриваемых дел от 31.01.1995, жалоба № 15225/89.

Однако в большинстве случаев государству-ответчику и заявителю не удается достигнуть дружественного урегулирования.

В деле «*Хмель против России*»[1] заявитель указывал, что осуществлением видеосъемки без его согласия в отделении милиции и последующей трансляции полученных данных по местному телевидению была нарушена ст. 8 Конвенции по правам человека. На тот момент заявитель являлся депутатом областной думы и был задержан при вождении автомобиля в нетрезвом состоянии. Приглашенные сотрудниками милиции журналисты произвели видеосъемку заявителя без его согласия и затем показали запись по телевидению. После этого частная жизнь заявителя стала объектом повышенного общественного внимания.

Государство-ответчик утверждало, что лицо, совершившее подобное правонарушение, должно претерпевать некоторые ограничения в отношении своих прав, включая право на уважение частной жизни.

По мнению ЕСПЧ, действия национальных властей нарушили ст. 8 Конвенции по правам человека. Суд отметил, что решение начальника милиции пригласить журналистов и разрешить им производить съемку без каких-либо ограничений на ее последующее использование, представляло собой вмешательство в право заявителя на неприкосновенность частной жизни, поскольку не соответствовало закону.

Дмитрий Дедов, судья ЕСПЧ от России, написал особое мнение по этому делу. Он указал, что ст. 3 Закона РФ от 18.04.1991 № 1026-I «О милиции» устанавливала такие принципы уважения прав и свобод человека, как законность, гуманизм и гласность[2]. По его мнению, данное положение позволяет осуществлять вмешательство в право на неприкосновенность частной жизни, так как в данном случае милиция была обязана защитить свободу распространения информации.

Подводя итоги, можно признать, что соблюдение баланса между использованием преимуществ информационных технологий в публичных интересах и интересами личности имеет принципиальное значение при рассмотрении дела в Суде. Практика ЕСПЧ свидетельствует о том, что наиболее частые нарушения ст. 8 Конвенции по правам человека характерны для государств, где слабы процедурные гарантии или отсутствует надлежащее законодательство, позволяющее на на-

[1] *Khmel v. Russia*, постановление от 12.12.2013, жалоба № 20383/04.

[2] Ведомости Съезда народных депутатов Российской Федерации и Верховного Совета Российской Федерации. 1991. № 16. Ст. 503.

циональном уровне обеспечить защиту права на неприкосновенность частной жизни в контексте использования информационных технологий. Отсутствие эффективных гарантий при сборе и хранении персональных данных, которые соответствовали бы требованиям п. 2 ст. 8 Конвенции по правам человека, остается проблемой для многих государств – участников Конвенции.

Важно заметить, что подход ЕСПЧ к разрешению дела в рассмотренной сфере зависит и от специфики сбора персональной информации. Это позволяет ЕСПЧ придерживаться закономерной позиции, согласно которой защита персональных данных имеет основополагающее значение для того, чтобы лицо пользовалось своим правом на неприкосновенность частной жизни в полном объеме.

Пристатейный библиографический список:

1. *Samuel D. Warren, Louis D. Brandeis*. The Right to Privacy // Harvard Law Review. 1890. Vol. 4, No. 5. P. 193.

2. *Глинская Н.П.* Юридический термин «privacy» как предмет системно-динамического исследования // Вестник Московского университета. Серия 19. Лингвистика и межкультурная коммуникация. 2010. № 2.

3. Российский ежегодник международного права. 1993–94. СПб., 1995. С. 340–376.

4. *Шугуров М.В.* Защита прав человека в условиях современного научно-технического прогресса: практика Европейского суда по правам человека // Международное публичное и частное право. 2011. № 1. С. 5.

В.А. Ларионова

ИНФОРМАЦИОННЫЙ БРОКЕР КАК НОВЫЙ СУБЪЕКТ ИНФОРМАЦИОННОГО ПРАВА В ЭПОХУ BIG DATA

Аннотация. *В статье представлен анализ деятельности нового субъекта права – информационного брокера. В работе рассмотрен институт профайлинга, основанный на обработке персональных данных. Представлена характеристика гражданско-правового статуса информационных брокеров. Особое внимание уделено квалификации информационного брокера в качестве ключевых субъектов информационного права.*

Ключевые слова: *информационный брокер, персональные данные, профайлинг, Большие Данные, информационное право, прозрачность деятельности.*

1. Сущность и характеристика профайлинга

1.1. Понятие профайлинга

Современное постиндустриальное общество наряду с развитием информационных технологий породило много вызовов, влияющих на частную жизнь граждан. Одним из таких вызовов является профайлинг. Лица вынуждены раскрывать огромное количество информации о себе по требованию органов власти или в целях получения доступа к каким-либо ресурсам в процессе жизнедеятельности. Как следствие, массивы информации подвергаются практически бесконтрольному сбору и систематизации органами и организациями: граждане не знают точно, как работают информационные системы, какие данные они собирают, где и как происходит обработка этих данных и для чего они используются в дальнейшем[1].

Исследования, проведенные в Европейском союзе и Российской Федерации, подтверждают актуальность проблемы безопасности персональных данных.

[1] *Gurtwirth S., Hert P., Poullet Y.* (2010) Data Protection in a Profiled World. Springer. P. 7.

Так, около 75% граждан ЕС обеспокоены тем, что у них нет полного контроля над их персональными данными[1], при этом 53% опрошенных отметили, что чувствуют дискомфорт в связи с тем, что различные интернет-компании используют информацию об их деятельности в сети[2]. Что касается граждан Российской Федерации, то 65% респондентов опасаются кражи их персональной информации[3]. В отчетах о проведении социальных опросов неоднократно упоминается термин «профайлинг», что обусловливает необходимость углубиться в понятие данного термина.

«Профайлинг» – термин с множеством значений, используемых как специалистами в различных областях, так и гражданами в контексте нейтральных тем. Впервые термин «профайлинг» был употреблен в 1984 г. для описания метода поиска данных, который позволял полиции сопоставлять огромное количество различных данных, чтобы оценить, насколько лицо или событие соответствуют каким-либо характеристикам или насколько ожидаемо от лица определенное поведение.

На базе пяти европейских университетов была создана рабочая группа «Проект профайлинга», ориентированная на выявление и решение проблем, возникающих в области защиты данных в эпоху развития информационных технологий.

Группа разработала свое определение профайлинга – это метод, позволяющий автоматически обрабатывать персональные и иные данные в целях создания профилей из уже имеющихся данных и последующего прогнозирования информации, которая может быть использована в качестве основы для принятия решений[4]. Каждый отдельный профайл представляет собой набор взаимосвязанных данных, которые характеризуют отдельное лицо или группу лиц. Профайлы создаются путем обнаружения неочевидных закономерностей между отдельными данными в больших наборах таких данных. После того как профайлы сконструированы, начинается их практическое применение путем

[1] Data Protection Report. February 2015. March 2015. P. 9 (URL: http://ec.europa.eu/COMMFrontOffice/publicopinion/index.cfm/Survey/getSurveyDetail/instruments/SPECIAL/surveyKy/2075).

[2] Ibid. P. 39.

[3] Безопасность в информационном обществе: вызовы нового века. Пресс-выпуск 3282 (ВЦИОМ: URL: http://wciom.ru/index.php?id=236&uid=116024).

[4] *Bosco G. Cafiero, D'Angelo E., Ferraris V., Suloyeva Y.* Profiling. Protecting citizens' rights fighting illicit profiling. (URL: http://profiling-project.eu/wp-content/uploads/2015/01/Profiling_final_report_20141.pdf (дата обращения: 02.09.2016)). P. 9.

идентификации конкретного субъекта или отождествление отдельного лица с какой-либо группой лиц или с определенной моделью и последующее принятие решений, основанных на предшествующей идентификации[1].

По существу, процесс профайлинга проходит три этапа.

Первый этап, во время которого осуществляется сбор огромных объемов информации об отдельных субъектах (в том числе сбор анонимной информации) и хранение данных, полученных с помощью специальных технологий. Второй этап – анализ собранных данных, в процессе которого полученная информация соотносится с другой информацией о поведении или характеристиках субъектов, и на основе проведенного анализа осуществляется построение определенных моделей (поведения, внешности и т.п.).

Третий – заключительный этап, который выражается в использовании сконструированных моделей в целях выявления деталей в конкретных профайлах, которые соответствуют тем или иным моделям.

Как правило, если речь идет о профайлинге в контексте безопасности, то на основе полученных данных выделяют специфические группы людей, объектов или действий, «заслуживающих внимания»[2] или «особого обращения»[3], а затем выявляют аналогичные характеристики в отдельных профайлах. Фактически профайлинг – это новая форма знаний, которая делает видимыми те факты, которые не видны «невооруженным глазом»[4].

В действительности профайлинг имеет очень широкое применение. Так, существует «этнический профайлинг», основанный на отборе данных, по которым индивиды могут быть дискриминированы, например, людям определенной расы или национальности может быть запрещен вход на мероприятие[5]. Иногда профайлинг относится к простому описанию характеристики личности, которая заслуживает

[1] *Bosco G. Cafiero, D'Angelo E., Ferraris V., Suloyeva Y.* Profiling. Protecting citizens' rights fighting illicit profiling. (URL: http://profiling-project.eu/wp-content/uploads/2015/01/Profiling_final_report_20141.pdf (дата обращения: 02.09.2016)). P. 9.

[2] *Taipale K.* The privacy implications of Government Data Mining Programs. Testimony before the US Senate Committee on the Jurisdiciary, 10 Jabuary. P. 6.

[3] *Lyon D.* Surveillance as Social Sorting: Privacy, Risk and Digital Discrimination. New York: Routledge. P. 20.

[4] *Hildebrandt M.* (2009). Who is Profiling Who? Invisible Visibility, in Gutwirth S., Poullet, Y., De Hert, P., De Terwangne C., Nouwt S. (Eds), Reinventing Data Protection?, Dordrecht, Springer. P. 239–252.

[5] *Gurtwirth S., Hert P., Poullet Y.* (2010) Data Protection in a Profiled World. Springer. P. 279.

особого внимания (например, профайлы потенциальных и осужденных террористов могут быть использованы в ходе борьбы с контртеррористической деятельностью)[1]. Понятие профайлинга можно также встретить в дискуссиях, связанных с безопасностью, когда производится сбор данных в целях конструирования профилей, позволяющих разделять индивидов по категориям.

Использование профайлов крайне востребовано среди ориентированных на потребителей компаний, поскольку это позволяет в большей степени удовлетворять интересы клиентов, а следовательно, увеличивать их прибыль. Главная цель таких компаний – мониторинг потребителей и создание профайлов с данными об их характеристиках (пол, возраст, этническая принадлежность), об их интересах, и, самое главное, об их покупательской активности. Например, рекламные и издательские компании используют профайлинг для показа именно той рекламы, которая наиболее точным образом отображает интересы потребителя в данный момент времени[2].

В качестве примера использования профайлинга в России можно привести деятельность компании ООО «ВонтРезалт», запатентовавшую технологию «определение цифрового следа». Эта технология позволяет владельцам сайтов из открытых источников получить электронные адреса, телефоны, ссылки на аккаунты в социальных сетях потенциальных покупателей – тех, кто провел на веб-сайте значительное количество времени. Среди клиентов ООО «ВонтРезалт» значатся такие компании, как Тинькофф Банк, «ВымпелКом», *Major*, «Эльдорадо» – известные организации, услугами которых граждане пользуются ежедневно[3].

Практически любая информация потенциально может быть использована для создания профайлов. Данные, из которых состоят профайлы, могут быть представлены в любой форме (аналоговой или цифровой). Содержание и структура этих данных также не имеют значения: профайлы могут состоять из информации, представленной в виде таблиц или графических элементов[4].

---

[1] *Ellyne E., Gutwirth S., Fuster G. G.* Profiling in the European Union: A high-risk practice. INEX Policy Brief. No. 10. P. 2.

[2] *Castelluccia C.* Behavioural Tracking on the Internet: A Technical Perspective. Behavioural Tracking on the Internet: A Technical Perspective. Netherlands: Springer. 2012. P. 22.

[3] С сети по нитке: как вундеркинд оседлал торговлю персональными данными // РБК (URL: http://www.rbc.ru/own_business/01/03/2017/58b6934f9a7947dc0fc13939).

[4] *Bosco G. Cafiero, D'Angelo E., Ferraris V., Suloyeva Y.* Working Paper Defining Profiling. P. 12. (URL: http://profiling-project.eu/wp-content/uploads/2013/07/PROFILINGproject_WS1_definition_0208.pdf (дата обращения: 05.01.2017)).

В доктрине выделяют две наиболее распространенные формы данных и, как следствие, два вида профайлинга. К первой группе данных относятся такие, которые можно получить из анализа поведения лица (поведенческий профайлинг), вторую группу составляют данные о местоположении лица.

Поведенческий профайлинг представляет собой изучение закономерностей поведения субъектов и последующую обработку полученных данных в целях их соотнесения с определенными группами. В некоторых случаях обработка данных предназначена для того, чтобы выявить предпочтения (например, с помощью обработки данных может быть получена информация о том, какие продукты питания предпочитают потребители в зависимости от сезона, и на ее основе приняты меры для повышения привлекательности ресторана). В других случаях модель поведения уже, как правило, известна и обработка данных используется для установления того, как изменится поведение, или того, что оно не изменится вообще (например, оператору данных могут быть известны вкусовые предпочтения субъекта персональных данных, а профайлинг используется для того, чтобы быть готовым к изменениям в предпочтениях)[1].

Профайлинг, основанный на местоположении, приобретает свою значимость благодаря возрастающей роли сервисов, определяющих местоположение кого-либо или чего-либо на определенной территории. Данные о местоположении или передвижении объекта могут быть получены с помощью беспроводных технологий: мобильных телефонов, *GPS*-навигаторов, *RFID*[2] и т.д. Такие данные включают в себя не только информацию о том, где человек или вещь находится в конкретный момент времени, но также информацию о том, сколько времени объект находился в определенном месте, и о перемещениях объекта в пространстве[3].

Данные о местоположении составляют основу любого вида профайлинга: они позволяют определить ресторан, в котором объект проводит время, а также частоту его посещений. Если обработка данных

[1] *Bosco G. Cafiero, D'Angelo E., Ferraris V., Suloyeva Y.* Working Paper Defining Profiling. P. 12.

[2] RFID-технология (IDexpert: URL: http://www.idexpert.ru/technology/121/ (дата обращения: 27.01.2017)).

[3] *Friedland G., Sommer R.*Cybercasing the Joint: On the Privacy Implications of Geo-Tagging, 2010 (URL: http://www.icsi.berkeley.edu/pubs/networking/cybercasinghotsec10.pdf/ (дата обращения: 15.01.2017)).

покажет, что в определенный момент времени лица находятся вместе в одной и той же точке, а в другой момент времени – в иной точке, но также вместе, то можно с учетом других данных сделать выводы о родственных связях этих лиц или о круге их общения[1].

В эпоху развития информационных технологий и сети Интернет наибольшего внимания заслуживает профайлинг онлайн-пользователей (или веб-профайлинг), представляющий собой контроль и отслеживание деятельности пользователей в сети Интернет, основанный главным образом на технологии «куки» (механизм, который собирает данные о пользовательской активности в то время, когда они посещают веб-страницы)[2].

При этом веб-сайты сконструированы таким образом, что если пользователь не соглашается с тем, что информация о его деятельности в сети будет направляться администратору, то он не получит доступ к дальнейшему контенту. То есть в случае принятия куки происходит своего рода обмен данных пользователя на возможность просматривать содержимое веб-сайта. Если пользователь не принимает куки, находясь на странице интернет-магазина, он не сможет разместить заказ и получить необходимый товар.

Подобная система используется веб-сайтом *Amazon.com*: создатели интернет-платформы запустили «систему торговой подсказки», которая на основе данных, полученных с помощью куки, сравнивает поисковые запросы и покупки одного пользователя с таковыми других пользователей и показывает потенциальному покупателю товары, купленные лицами с похожим покупательским поведением[3]. Использование торговой подсказки дает возможность пользователям получать информацию о предпочтительных для них товарах, а компании *Amazon* – получать дополнительную прибыль.

Пример профайлинга обнаруживается в судебном деле, возбужденном социальной сетью «ВКонтакте» против компании *Double Data* и НБКИ. Исковые требования соцсети были сведены к обязыванию ООО «Дабл» прекратить использовать открытые данные пользователей для продажи услуг. Деятельность *Double Data* заключается в извлечении из базы данных соцсети фамилий, имен, сведений о месте работы

[1] *Fitsch L.* Profiling and Location-Based Services (LBS) // Profiling the European Citizens. Cross-Disciplinary Perspectives. Springer. P. 154.

[2] *Castelluccia C.* Op. cit. P. 24.

[3] *Macmanus M.* A guide to recommender systems. January, 2009 (URL: http://readwrite.com/2009/01/26/recommender_systems/ (дата обращения: 14.01.2017)).

и учебы и прочей информации. При этом технологии, разработанные компанией, анализируют и агрегируют данные, а затем *Double Data* продает полученные результаты другим организациям, которые принимают решения на основе полученной информации[1].

Выше было изложено определение профайлинга, сформулированное в доктрине. Но с учетом того, что значение сбора и обработки персональных данных граждан возрастает с каждым днем, европейский законодатель озаботился формулировкой легального определения профайлинг.

Если профайл состоит из персональных данных, он подпадает под действие Директивы 95/46 ЕС «О защите данных» от 24.10.1995[2] (*Data Protection Directive*, далее – *DPD*). В Директиве не закреплено определение профайлинга как такового, но его ст. 15 касается автоматизированных решений в отношении физических лиц[3]. В то же время первоначальная версия документа включала слово «профайл» применительно к праву лиц «не оказаться под воздействием решений, принятых исключительно на основании автоматизированной обработки персональных данных и порождающих юридические последствия в отношении субъекта обработки...»[4].

Наиболее полное обеспечение защиты данных в стремительно развивающемся информационном обществе отражено в определении профайлинга, содержащемся в Общем регламенте о защите персональных данных (*General Data Protection Regulation*, далее – *GDPR*). Статья 20 *GDPR* охватывает меры, основанные на профайлинге. В частности, *GDPR*, как и *DPD*, защищает право физических лиц не оказываться под воздействием автоматизированных решений, но вводит положение о том, что обработка данных должна осуществляться в целях профайлинга. Под профайлингом понимается «анализ и построение предположений о деятельности физического лица, кредитоспособно-

[1] Дело А40-18827/2017 // Электронное правосудие (URL: http://kad.arbitr.ru/Card/1f33e071-4a16-4bf9-ab17-4df80f6c1556 (дата обращения: 04.04.2017)).

[2] *Gurtwirth S., Hert P., Poullet Y.* (2010) Data Protection in a Profiled World. Springer. P. 35.

[3] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data / Official Journal of the European Union. L 281/31. Volume 38, 23 November 1995 (URL: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:L:1995:281:TOC).

[4] Proposal for a Directive concerning the protection of individuals in relation to the processing of personal data, COM (90), 314 final, SYN 287 and 288, Brussels, 13 September 1990 (URL: http://aei.pitt.edu/3768/1/3768.pdf/ (дата обращения: 17.01.2017)).

сти, экономической ситуации, местоположении, здоровье, вкусовых предпочтениях и поведении»[1].

Из этого следует, что европейские акты устанавливают своего рода гарантии для граждан, поскольку при создании профайлов должны применяться специальные нормы, например, в части получения дополнительного согласия использования персональных данных тех или иных лиц.

В то же время как *DPD*, так и *GDPR* фокусируют внимание на последствиях, возникающих в процессе использования профайлинга, а не на профайлинге как таковом. Однако, как отмечается в литературе, более эффективно регулировать непосредственно процессы создания и использования персональных профайлов оператором до того, как предположения или конкретные решения будут приняты[2].

Рабочая группа ст. 29 *DPD*, специализирующаяся на аналитике в области персональных данных[3], выработала ряд принципов, которые должны быть заложены в правовой режим профайлинга: а) увеличение прозрачности процесса обработки данных, контроля и согласия субъекта, чьи данные подлежат обработке; б) усиление ответственности операторов в отношении использования техник профайлинга; в) сбалансированный подход к регулированию профайлинга с учетом позитивных и негативных эффектов[4].

Совет Европы, в свою очередь, также разработал основные положения, касающиеся профайлинга. Совет Европы предлагает определение, разделяющее процесс обработки на три этапа: во-первых, наблюдение (в том числе хранение данных); во-вторых, анализ данных; и в-третьих, применение этих данных. Сам же профайлинг определяется как «метод автоматической обработки данных, который заключается в применении профайлов к конкретным индивидам, в частности, для

[1] Regulation of the European Praliament and of the council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) (URL: http://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX:52012PC0011).

[2] Article 29 Working Party (2013), Advice paper on essential elements of a definition and a provision on profiling within the EU General Data Protection Regulation, adopted on 13 May 2013. URL: http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2013/20130513_advice-paper-on-profiling_en.pdf (дата обращения: 19.01.2017).

[3] Article 29 Working Party // The EDPS. URL: https://secure.edps.europa.eu/EDPSWEB/edps/Cooperation/Art29.

[4] Ibidem.

того, чтобы принять решения, касающиеся этих индивидов или чтобы спрогнозировать их поведение и взгляды»[1].

Как будет показано далее, профайлинг используется в различных сферах жизни и имеет свои достоинства и недостатки. Вместе с тем на данном этапе не выявлены все положительные и отрицательные стороны профайлинга, которые определяют дефиницию этого явления. Несмотря на то что проблемы сбора и обработки персональных данных касаются всех, кто живет в эпоху информационного общества, в России (в отличие от Европы, где ведется активная работа по изучению концепции профайлинга) практически отсутствуют работы, посвященные рассматриваемому явлению.

1.2. Положительные и отрицательные стороны профайлинга

В наши дни общество столкнулось с огромным массивом информации, и главная задача – понять, что эта безграничная информация собой представляет и как нужно действовать в процессе работы с ней[2]. М. Хильдербрандт считает, что профайлинг способен избавить общество от двух проблем: от переизбытка информации и от нечеткой границы, разделяющей знания и большие объемы информации, часть из которых не несут смысловой нагрузки[3].

Профайлинг может применяться в совершенно различных сферах и контекстах. Наибольшим спросом рассматриваемые технологии пользуются у правоохранительных органов и коммерческих организаций, которые уже накопили большие объемы данных о гражданах. Иллюстрацией использования технологий профайлинга может выступать сфера деятельности правоохранительных органов (в процессе контртеррористической деятельности), сфера трудоустройства (в процессе анализа деловых качеств сотрудников), в области коммерции (в процессе поиска потенциальных покупателей и клиентов). Однако

[1] Council of Europe, Recommendation CM/Rec(2010)13 of the Committee of Ministers to Member States on the protection of individuals with regard to automatic processing of personal data in the context of pro ling. Adopted by the Committee of Ministers on 23 November 2010 at the 1099th meeting of the Ministers' Deputies (URL: http://www.coe.int/t/dghl/standardsetting/cdcj/CDCJ%20Recommendations/CMRec(2010)13E_Profiling.pdf).

[2] *Hildebrandt M., Gutwirth S.* General Introduction and Overview, in Mireille Hildebrandt and Serge Gutwirth (eds). *Profiling the Europen Citizen: Cross disciplinary perspectives, Dordrecht: Springer Science*. 2008. P. 294.

[3] *Hildebrandt M.* Profiling: from data to knowledge // Datenschutz und Datensuchereit. 2006. № 30. Vol. 9. P. 548.

не стоит забывать, что цели использования профайлинга нередко рискованны, поэтому в целях понимания сущности понятия, его положительных и отрицательных сторон необходимо обратиться к примерам.

Прежде всего следует сказать, что профайлинг пользуется успехом как в публичных, так и в частных сферах жизни общества. Различие между обработкой данных частными и государственными секторами не всегда удается установить[1]. Иногда государственные органы могут использовать персональные данные, собранные частными организациями, по соображениям безопасности. В частности, обработка данных в целях прогнозирования, характерная для коммерческих компаний, пользуется популярностью и у правоохранительных органов[2].

Начать рассмотрение профайлинга следует с области безопасности. Если обратиться к зарубежному опыту, то можно заметить, что, например, в Англии уже создана база данных под названием *E-CAF*, которая содержит в себе огромное количество персональных данных о детях и их семьях. Некоторые публичные институты, включая полицию, школы и иные социальные учреждения, имеют доступ к базе и могут предположить, кто потенциально может совершить преступление, и начать работу с ребенком до того, как он посягнет на конституционные основы и общественные отношения, охраняемые законодательством[3].

Другим примером служит база биометрических данных, созданная ФБР в США, которая содержит записи более чем о 100 млн людей. Более того, планируется создание усовершенствованной базы, которая будет содержать такие биометрические данные, как сетчатка глаза, фотографии лиц, отпечатки ладоней, голосовые записи и т.п.[4] Основная цель сбора и обработки таких данных – оценить угрозы, которые представляет каждый отдельный человек (или несколько лиц в совокупности), и предотвратить преступления, распределив ресурсы соответствующим образом. Проблемным моментом использования

[1] *Boersma K., Van Brakel R., Fonio C., Wagenaar P.* History of State surveillance in Europe and beyond // Rouledge studies in crime and society. 2014. P. 3.

[2] *Bosco G. Cafiero, D'Angelo E., Ferraris V., Suloyeva Y.* Working Paper Defining Profiling. P. 23 (URL: http://profiling-project.eu/wp-content/uploads/2013/07/PROFILINGproject_WS1_definition_0208.pdf (дата обращения: 19.01.2017)).

[3] Common assessment framework – CAF – Child protection – CCLC // Children's Legal Centre (URL http://www.protectingchildren.org.uk/cp-system/child-in-need/caf (дата обращения: 16.01.2017)).

[4] Next Generation Identification (NGI) // Federal Bureau of Investigation (URL https://www.fbi.gov/services/cjis/fingerprints-and-other-biometrics/ngi (дата обращения: 16.01.2017)).

таких баз данных является необходимость действий «на будущее», т.е. дается оценка будущему поведению индивидов, которое может и не наступить, что противоречит конституционно закрепленной презумпции невиновности, согласно которой каждый считается невиновным, пока его виновность не будет доказана.

В России, как и во многих других странах, правоохранительные органы стремятся предотвратить преступление до его начала вместо того, чтобы реагировать на уже произошедшее событие (подп. 13 п. 1; подп 2. п. 2 ст. 37 ФЗ от 07.02.2011 № 3-ФЗ «О полиции»). Однако в России на данный момент не существует единой базы данных, к которой имели бы доступ различные организации, хотя доступ полиции к такого рода базам способствовал бы предотвращению преступлений. В связи с этим начата работа по ее созданию[1].

Профайлинг используется также в целях контроля пассажиров авиа- и железнодорожного транспорта. Так в ФЗ от 09.02.2007 № 16-ФЗ «О транспортной безопасности» закреплена обязанность Правительства РФ создать информационную базу данных пассажиров (ч. 1 ст. 11), которая должна содержать их персональные данные (ч. 5 ст. 11). На базе этой статьи были созданы Автоматизированные централизованные базы персональных данных о пассажирах и персонале (экипаже) транспортных средств (далее – АЦБПДП), являющиеся частью системы информационного обеспечения безопасности населения на транспорте[2]. Вопрос о создании аналогичных баз обсуждается и на европейском уровне[3].

Основная цель таких баз – выявить пассажиров с высоким уровнем риска, на которых сотрудникам аэропортов и вокзалов предлагается обратить повышенное внимание во время регистрации на рейс или по прибытии в место назначения, либо пассажиров, которых желательно не допускать к полету вовсе в целях обеспечения безопасности других пассажиров. Негативным последствием использования подоб-

[1] В России появится единая база с данными всех граждан страны (RT.URL: https://russian.rt.com/article/314043-v-rossii-poyavitsya-edinaya-baza-s-dannymi (дата обращения: 08.02.2016)).

[2] Автоматизированные централизованные базы персональных данных о пассажирах и персонале (экипаже) транспортных средств // ФГУП «ЗащитаИнфоТранс» (URL: http://www.z-it.ru/projects/egis-otb/acbpdp (дата обращения: 09.02.2017)).

[3] EU Passenger Name Records (PNR) directive: an overview // European Parliament News (URL: http://www.europarl.europa.eu/news/en/news-room/20150123BKG12902/eu-passenger-name-record-(pnr)-directive-an-overview (датаобращения: 16.01.2017)).

ных информационных систем может быть нарушение прав граждан на свободу передвижения (ст. 27 Конституции РФ) и действия дискриминационного характера, когда права одних лиц ставятся выше прав других в силу того, что последние обладают определенными характеристиками (проживают в неблагоприятном районе или получают зарплату ниже определенного уровня)[1].

Обработка данных в каждом из упомянутых случаев не в последнюю очередь направлена на борьбу с терроризмом. Использование информации из разных баз данных в контртеррористических целях позволяет выделять характеристики, которые присущи террористам, и определять потенциально возможных преступников, а также выявлять каналы их связи.

При этом опасения вызывает вопрос соблюдения прав человека и дискриминации личности. Так, некоторые авторы обращают внимание на то, что выявление различных террористических организаций, потенциальных преступников может несправедливо основываться на базе религиозных убеждений лиц, их национального или этнического происхождения[2].

Применение профайлинга в финансовой сфере также своей конечной целью нередко ставит борьбу с террористической деятельностью. В процессе выявления отмывания денег и финансового мошенничества используется автоматизированное наблюдение, которое помогает обнаружить подозрительные операции (например, совершение организациями необоснованно крупных сделок), сравнить полученные данные с данными о других организациях и сделать выводы о принадлежности лица к террористической организации.

В то же время финансовый сектор может почерпнуть немало положительного от автоматизированной обработки данных: повысить эффективность работы за счет сокращения времени на принятие решений (так, система может в считанные секунды проанализировать платежеспособность заемщика на основе ранее выданных кредитов и принять решение о выдаче займа и условиях такого займа). С помощью профайлинга финансовые организации могут предлагать оказание таких услуг, которые были бы интересны именно данному клиенту,

[1] *Bosco G. Cafiero, D'Angelo E., Ferraris V., Suloyeva Y.* Working Paper Defining Profiling. P. 24.

[2] *Moeckli D., Thurman J.* Counter-terrorism data mining: legal analysis and best practices. DETECTER project – Detection Technologies, Terrorism, Ethics and Human Rights. Deliverable 08.03. 2008. P. 2.

основываясь на данных о его возрасте, поле, семейном статусе и финансовом положении.

Профайлинг используется и в сфере трудовой деятельности. Во-первых, *HR*-специалисты используют обработанные данные для оценки потенциальных возможностей сотрудников компании и для улучшения управления кадровыми ресурсами[1]. Но использование профайлинга в сфере управления кадрами нередко сопровождается слишком тщательным контролем электронной почты сотрудников и их действий в сети, что снова подвергает сомнению незыблемость фундаментальных прав человека.

Наибольшего успеха технологии профайлинга достигли в сфере коммерции, в частности в сфере использования контекстной рекламы. Такая реклама основана на анализе товаров, потребляемых покупателями. С помощью пройфайлинга продавцы могут предугадать, какие покупки будут совершены лицами, основывая свои предположения на конкретных товарах, уже просмотренных пользователем (например, кто-то может искать книгу или электронный гаджет в *Google*, а затем увидеть рекламу этого же товара или товара-комплемента на совершенно другом сайте)[2]. При этом различные лица, просматривающие одну и ту же веб-страницу, могут увидеть совершенно разную рекламу, основанную на их личных поисковых запросах в браузере[3].

Многие магазины собирают информацию путем введения «программ лояльности». Сначала магазины получают личные данные покупателей для выдачи им пластиковой карты (дата и место рождения, пол, контактная информация), а затем с помощью таких карт собирают подробную информацию о покупке: место, время совершения сделки, конкретный приобретенный продукт[4].

Несмотря на существующую угрозу безопасности персональных данных, преимущества использования профайлинга интернет-магазинами очевидны: организации оптимизируют производство и увели-

[1] *Bosco G. Cafiero, D'Angelo E., Ferraris V., Suloyeva Y.* The impact of profiling on fundamental rights. Working paper 3. P. 10.

[2] How To Block Targeted Ads From Following You Around // Business Insider (URL: http://www.businessinsider.com/how-to-keep-ad-companies-from-tracking-your-web-history-2011-2 (дата обращения: 20.01.2017)).

[3] *Johnson J.P.* Targeted advertising and advertising avoidance. Mimeo, Johnson Graduate School of Management, Cornell University. 2009 (URL: http://sites.northwestern.edu/csio/files/2015/08/Johnson-2hvjmfr.pdf (дата обращения: 20.01.2017). P. 1.

[4] *Wakulowsky L.* Managing the Privacy Side Effects of Rx (and other) Customer Loyalty Programs // Health Law Bulletin. P. 2.

чивают прибыль. Потребители, в свою очередь, могут получать более подробную информацию о товарах и услугах, которые их интересовали, например, информацию о наиболее низких ценах.

Таким образом, проведенный анализ свидетельствует о том, что профайлинг имеет свои положительные и отрицательные стороны. Преимущества использования обработки данных в каждой сфере различаются и могут быть полезными как для оператора, так и для субъекта обработки данных. Однако при этом степень вмешательства в личную жизнь и степень контроля частной жизни отдельно взятого гражданина могут быть весьма высокими. Уже предпринимались попытки решить эту проблему законодательным образом: в частности, целью Закона о персональных данных является обеспечение таких конституционных прав граждан, как право на неприкосновенность частной жизни, на личную и семейную тайну при обработке информации (ст. 2).

В некоторых сферах можно столкнуться с дискриминацией некоторых групп людей на основе возраста, пола, состояния здоровья или места жительства, которая в конечном итоге может привести к отстранению их от каких-либо преимуществ. Указанные негативные аспекты невозможно устранить полностью, их можно только минимизировать путем законодательного ограничения использования тех или иных данных или установления ответственности операторов.

2. Информационный брокер как новый субъект правового регулирования

2.1. Гражданско-правовая характеристика отношений с участием информационного брокера

2.1.1. Правовой статус информационного брокера

Прежде чем приступить к анализу гражданско-правового статуса информационного брокера, необходимо рассмотреть понятие информационного брокера и смысл, который в него вкладывается.

В отечественной правовой литературе понятие информационный брокер отсутствует. Отдельные определения разработаны в зарубежной доктрине.

В частности, Федеральная Торговая Комиссия (ФТК) США определяет информационного брокера (*data broker*) как «компанию, которая

собирает персональные данные потребителей и перепродает их или делится ими с другими компаниями»[1]. Аналогичное определение было разработано Сенатом Соединенных Штатов[2], Счетной палатой США[3], а также Уполномоченным по вопросам частной жизни Канады[4].

Европейские авторы, описывая субъекта, который собирает и перепродает данные, используют другие термины, например, *information reseller* (лицо, занимающееся перепродажей информации), *data vendors* (поставщики данных), *information brokers* (информационный брокер), *consumer data analytics* (анализ данных потребителей), *data warehousing* (хранилище данных) и др.[5] Дефиниции упомянутых терминов мало отличаются от тех, что были разработаны в США применительно к понятию информационного брокера.

Так, Европейский орган защиты данных определяет информационного брокера как организацию, которая «собирает персональные данные потребителей и продает эту информацию другим организациям»[6]. Организация экономического сотрудничества и развития в докладе, посвященном персональным данным, определяет информационного брокера как «фирму, которая собирает агрегированную информацию об индивидах, а затем перепродает для различных целей...»[7].

---

[1] Federal Trade Commission. Data Brokers: A Call for Transparency and Accountability, May 2014 (URL: https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf (дата обращения: 14.02.2017)).

[2] United States Senate Committee Commerce, Science, and Transportation, Office of Oversight and Investigations, Majority Staff. A Review of the Data Broker Industry: Collection, Use, and Sale of Consumer Data for Marketing Purposes. December 18, 2013 (URL: http://educationnewyork.com/files/rockefeller_ databroker.pdf (дата обращения: 14.02.2017)).

[3] United States Government Accountability Office. Information Resellers: Consumer Privacy Framework Needs to Reflect Changes in Technology and the Marketplace, Report to the Chairman, Committee on Commerce, Science, and Transportation, US Senate, September 2013 (URL: http://www.gao.gov/assets/660/658151.pdf (дата обращения: 14.02.2017)).

[4] Office of the Privacy Commissioner of Canada, *Data Brokers: A Look at the Canadian and American Landscape*, September 2014 (URL: https://www.priv.gc.ca/information/research-recherche/2014/db_201409_e.pdf (дата обращения: 14.02.2017)).

[5] *Rieke A., Yu H., Robinson D., von Hoboken J.* Data broker in an open Society. London: Bloomberg. 2016. P. 4.

[6] Datatilsynet. The Great Data Race: How commercial utilisation of personal data challenges privacy, November 2015 (URL: http://www.datatilsynet.no/Global/04_analyser_utredninger/2015/engelsk-kommersialisering- november-2015.pdf (дата обращения: 14.02.2017)).

[7] OECD, Exploring the Economics of Personal Data.URL: http://www.oecd-ilibrary.org/science-and-technology/exploring-the-economics-of-personal-data_5k486qtxldmq-en (дата обращения: 14.02.2017).

В декабре 2012 г. ФТК инициировала проект, целью которого являлось выявление характерных черт информационных брокеров. Для этого комиссия направила ордеры девяти наиболее крупным компаниям с запросом на получение информации об их деятельности, об источнике, из которого они получают информацию, а также об их клиентах, которым информация перепродается. Ниже приведена информация о деятельности наиболее известных компаний.

1. ***Acxiom*** предоставляет данные потребителей и аналитические услуги для проведения маркетинговых кампаний и мероприятий по выявлению мошенничества. Их базы данных содержат информацию о 700 млн потребителей по всему миру[1].

2. ***Corelogic*** прежде всего предоставляет другим компаниям и правительству информацию о недвижимости, о потребителях и финансовую информацию. Также *Corelogic* оказывает аналитические услуги. База данных охватывает более 795 млн сделок с недвижимостью, более 93 млн заявок на ипотеку и иных данных о собственности граждан, в совокупности составляющих информацию о 99% жилой недвижимости США[2].

3. ***Oracle*** предоставляет компаниям сведения практически о всех семьях США и располагает информацией о потребительских сделках более чем на 1 трлн долл.[3] В сентябре 2012 г. *Facebook* объявил о сотрудничестве с *Datalogix* (которая впоследствии была приобретена компанией *Oracle*), чтобы определить, как часто пользователи *Facebook* совершают покупки в офлайн-магазинах после просмотра контекстной рекламы в социальной сети[4].

4. ***eBureau*** предоставляет прогностические оценки и аналитические услуги для маркетологов, финансовых компаний, интернет-магазинов и других компаний. В первую очередь *eBureau* предлагает продукты, которые оценивают платежеспособность потребителей или вероятность заключения мошеннических сделок. *eBureau* располагает миллиардами

[1] Acxiom Corp., Annual Report, 2015 (URL: http://investors.acxiom.com/secfiling.cfm?filingid=733269-15-18&cik=733269#F10K_HTM_4 (дата обращения: 15.02.2017)).

[2] Corelogic, Annual Report 7 (2012) (URL:http://phx.corporate-ir.net/External.File?item=UGFyZW50SUQ9MTkwNDg0fENoaWxkSUQ9LTF8VHlwZT0z&t=1 (дата обращения: 15.02.2017)).

[3] Oracle, Annual Report, 2015. URL: http://www.annualreports.com/HostedData/AnnualReports/PDF/NASDAQ_ORCL_2015.pdf (дата обращения: 15.02.2017)).

[4] Facebook partnership with Datalogix helps measure offline impact of online ads // Adweek (URL: http://www.adweek.com/digital/facebook-partnership-with-datalogix-helps-measure-offline-impact-of-online-ads/ (дата обращения: 15.02.2017)).

записей с информацией о потребителях, при этом более 3 млрд новых записей добавляются каждый месяц[1].

5. ***IDAnalytics*** предоставляет аналитические услуги, предназначенные главным образом для идентификации личности потребителей, а также для выявления мошеннических сделок. База данных этого информационного брокера включает в себя сотни миллиардов агрегированных данных и охватывает около 1,4 млрд потребительских сделок[2].

6. ***Intelius*** предоставляет компаниям и потребителям услуги по проверке информации, а также данные из публичных источников. Базы данных этого брокера содержат более 20 млрд записей[3].

7. ***PeekYou*** запатентовала технологию, которая анализирует контент более 60 социальных сетей, новостных ресурсов и блог-платформ, чтобы обеспечивать клиентов подробными профайлами потребителей[4].

8. ***Rapleaf*** **(до поглощения брокером *TowerData*)** являлся агрегатором данных и располагал информацией, которая позволяла связать один из более 80% адресов электронной почты граждан США с конкретным потребителем. *Rapleaf* дополнял списки адресов электронной почты данными о возрасте, поле, семейном положении и 30 других положений, которые позволяли бы идентифицировать потребителя[5].

9. ***RecordedFuture*** собирает данные о потребителях и компаниях в сети и использует эту информацию в целях прогнозирования будущего поведения субъектов. По состоянию на май 2014 г. брокер имел доступ к информации, собранной из более чем 502 591 различных открытых интернет-сайтов[6].

Согласно российском законодательству организации, преследующие извлечение прибыли в качестве основной цели своей деятельности, являются коммерческими организациями (п. 1 ст. 50 ГК РФ). Поскольку деятельность вышеуказанных компаний направлена в пер-

---

[1] eBureau About us // eBureau (URL: http://www.ebureau.com/about (дата обращения: 15.02.2017)).

[2] Data & Technology // ID Analytics (URL: http://www.idanalytics.com/data-and-technology/ (дата обращения: 15.02.2017)).

[3] *Intelius Facts* // Intelius (URL: http://corp.intelius.com/intelius-facts (дата обращения: 15.02.2017)).

[4] *About Us* // PeekYou (URL: http://www.peekyou.com/about/ (дата обращения: 15.02.2017)).

[5] Email Intelligence Pricing // TowerData (URL: http://www.towerdata.com/email-intelligence/pricing (дата обращения: 15.02.2017)).

[6] Recorded Future // SCmagazine (URL: https://www.scmagazine.com/recorded-future/article/629728 (дата обращения: 15.02.2017)).

вую очередь на извлечение прибыли[1], они являются коммерческими организациями. Как коммерческая организация, занимающаяся видом деятельности, не запрещенной законом (п. 1 ст. 49 ГК РФ), информационные брокеры наделены общей правоспособностью, которая возникает с момента их регистрации в качестве юридического лица, т.е. с момента внесения записи в ЕГРЮЛ[2].

Физические лица также могут заниматься обработкой данных (п. 2 и 3 ст. 3 Закона о персональных данных) с последующим извлечением прибыли, т.е. они также могут являться информационными брокерами, действуя в качестве индивидуального предпринимателя с момента внесения записи в ЕГРИП (ст. 23 ГК РФ).

Поскольку деятельность информационных брокеров не урегулирована специальными правовыми нормами, к вопросам их прав и обязанностей, гарантий деятельности, а также ответственности за нарушение обязательств будут применяться общие положения о коммерческих организациях.

Заслуживает внимания деятельность некоммерческих организаций, связанная с обработкой данных. Они могут осуществлять предпринимательскую деятельность и получать доход в случае, если такая деятельность служит достижению целей организаций и указана в учредительных документах (п. 2 ст. 24 ФЗ от 12.01.1996 № 7-ФЗ «О некоммерческих организациях»).

На практике такая деятельность может быть связана с политическим профайлингом: списки избирателей формируются избирательными комиссиями на основе персональных данных избирателей (ст. 16–17 ФЗ от 12.06.2002 № 67-ФЗ «Об основных гарантиях избирательных прав и права на участие в референдуме граждан Российской Федерации» и ст. 26 ФЗ от 10.01.2003 № 19-ФЗ «О выборах Президента Российской Федерации»). Политические организации, зарегистрированные в качестве НКО, могут получить списки избирателей, содержащие персональные данные граждан Российской Федерации, для проведения предвыборной агитации с учетом ограничений, установленных ст. 15 Закона о персональных данных. Став обладателями информации,

[1] Senator John D. Rockefeller IV, «What Information Do Data Brokers Have on Consumers, and How Do They Use It?» December 18, 2013 (URL: https://www.commerce.senate.gov/public/index.cfm/ hearings?Id=a5c3a62c-68a6-4735-9d18-916bdbbadf01&Statement_id=A47C081A-D653-4272-8D12- D6EDC1E04DC6).

[2] *Белов В.А.* Что изменилось в Гражданском кодексе?: практ. пособие. М.: Юрайт, 2014. С. 51.

политические партии могут использовать технологии профайлинга в целях разделения людей на группы в зависимости от их политических взглядов, а затем продавать полученные списки, выступая информационными брокерами в гражданском обороте.

Таким образом, организация, зарегистрированная в качестве НКО, может являться информационным брокером, но, скорее всего, столкнется с определенными законодательными ограничениями, главным из которых является необходимость соответствия деятельности целям организации.

Деятельность информационного брокера, будучи связанной с обработкой персональных данных, затрагивает такие конституционные права человека, как право на неприкосновенность частной жизни, право на тайну переписки и телефонных разговоров, поэтому необходимо рассмотреть вопрос о том, как законодательно закрепить необходимость таких организаций соответствовать повышенным требованиям. Разрешить данный вопрос может институт лицензирования, поскольку именно он способствует «укреплению гарантий государства по защите прав и законных интересов человека»[1].

Согласно действующему законодательству лица, получившие доступ к персональным данным, обязаны обеспечивать конфиденциальность этих данных (ст. 7 Закона о персональных данных). В свою очередь, деятельность по технической защите конфиденциальной информации подлежит лицензированию (ст. 17 ФЗ от 04.05.2011 № 99-ФЗ «О лицензировании отдельных видов деятельности»).

Однако в силу упомянутой ст. 7 Закона о персональных данных федеральным законом могут быть предусмотрены случаи, когда к операторам не предъявляются требования обеспечения конфиденциальности полученных данных. Например, если информация получена из общедоступных источников (ст. 8 Закона о персональных данных) или информация необходима уполномоченным государственным органам, осуществляющим оперативно-розыскную деятельность (п. 1.1 ст. 64 ФЗ от 07.07.2003 № 126-ФЗ «О связи»). То есть если информационный брокер осуществляет сбор, хранение и обработку данных из публичных источников (как, например, брокер *Intellius*), у него нет обязанности обеспечивать конфиденциальность информации, а следовательно, и получать лицензию.

[1] *Ласкина Н.В., Степаненко О.В.* Комментарий к Федеральному закону от 04.05.2011 № 99-ФЗ «О лицензировании отдельных видов деятельности» (СПС «КонсультантПлюс». 2015).

Тем не менее даже те информационные брокеры, которые обрабатывают общедоступную информацию, совершают такие манипуляции с персональными данными, которые затрагивают права человека (ст. 2 Закона о персональных данных), в связи с чем можно говорить о необходимости закрепления в законодательстве обязанности информационного брокера получать специальную лицензию, которая предписывала бы повышенные требования для рассматриваемого субъекта права. По аналогии с требованиями к лицам, осуществляющим выполнение работ или оказание услуг по защите информации от несанкционированного доступа, утечки по техническим каналам или иного воздействия на информацию[1], к повышенным требованиям для информационных брокеров может относиться наличие специального образования у субъекта или его работников, наличие сертифицированных автоматизированных систем для обработки информации, наличие на праве собственности или ином законном основании средств, обеспечивающих защищенность информации от несанкционированного доступа.

Поскольку осуществление предпринимательской деятельности без лицензии, если таковая предусмотрена законодательством, влечет риск наступления неблагоприятных последствий (ст. 14.1 КоАП; ст. 171 УК РФ), стимул информационного брокера соответствовать повышенным требованиям возрастет, вследствие чего вопрос о защищенности персональных данных граждан не будет стоять столь остро.

Среди возможных вариантов решения проблемы нарушений конституционных прав человека компаниями – информационными брокерами можно выделить создание саморегулируемых организаций информационных брокеров. Согласно п. 1 ст. 2 ФЗ от 01.12.2007 № 315-ФЗ «О саморегулируемых организациях» (далее – Закон о СРО) под саморегулированием понимается «самостоятельная и инициативная деятельность, которая осуществляется субъектами предпринимательской или профессиональной деятельности и содержанием которой являются разработка и установление стандартов и правил указанной деятельности, а также контроль за соблюдением требований указанных стандартов и правил».

[1] Постановление Правительства РФ от 03.02.2012 № 79 «О лицензировании деятельности по технической защите конфиденциальной информации» (вместе с «Положением о лицензировании деятельности по технической защите конфиденциальной информации»).

В соответствии со ст. 4 Закона о СРО саморегулируемые организации разрабатывают стандарты и правила профессиональной деятельности, которым должны соответствовать все члены саморегулируемой организации. Как правило, такие стандарты и правила предъявляют более жесткие требования, нежели предусмотрены законодательством. Соответственно санкции за нарушение правил и стандартов также более строгие, чем санкции за нарушение норм законов[1].

В настоящий момент Закон о СРО допускает возможность закрепления иными федеральными законами случаев обязательного членства субъектов в СРО (п. 2 ст. 5), в связи с чем представляется возможным при принятии федерального закона, регулирующего деятельность информационных брокеров, предусмотреть обязательное членство компаний в СРО.

Поскольку рынок информационных брокеров остается неурегулированной на законодательном уровне отраслью даже в США (где было выявлено преобладающее количество компаний-брокеров), контроль над ними осуществляется на основе стандартов, разработанных самими информационными брокерами. Как отмечается в доктрине, к преимуществам саморегулирования относятся гибкость и независимость от времени: в отличие от стандартов и правил процесс принятия законодательных актов долгий, бюрократичный и зависит от лиц, не являющихся специалистами в сфере *IT*-технологий и в области персональных данных[2].

На первый взгляд обязательное членство в СРО по аналогии с оценочной деятельностью выглядит обоснованной мерой, способной защитить граждан от бесконтрольного вмешательства: исключение информационных брокеров из СРО за нарушение установленных правил наряду с запретом сотрудникам компаний заниматься видами деятельности, связанными с персональными данными, лишит работы и последующего трудоустройства многих людей. Потенциальная возможность наложения подобного рода мер будет стимулировать компании соблюдать законодательство и иные требования.

Вместе с тем сравнение деятельности информационных брокеров с другими видами деятельности, подконтрольными СРО, не совсем корректно, поскольку для данной индустрии характерна непрозрач-

[1] *Соколова О.С.* Правовые основы саморегулирования // Юрист. 2008. № 4.

[2] *Cavoukian A.* Privacy as a Fundamental Human Rights vs. Economic Right: An Attempt at Conciliation, 1999.

ность, которая выгодна абсолютно каждой компании – потенциальному члену СРО. Из этого следует в первую очередь необходимость увеличения прозрачности отрасли, например, путем размещения на централизованном веб-сайте информации о каждом информационном брокере, о путях получения и продажи информации.

Подводя итог анализа создания СРО в области деятельности информационных брокеров, необходимо отметить, что членство в саморегулируемой организации способно обеспечить эффективную регламентацию отношений, создать условия для более тесного взаимодействия между информационными брокерами, их клиентами и источниками получения информации, что благотворно скажется на рынке персональных данных в целом.

2.1.2. Правовая квалификация договора по предоставлению персональных данных

Деятельность информационного брокера состоит в первую очередь в приобретении и последующей перепродаже данных, поэтому далее в работе будут рассмотрены источники получения данных, а также проанализирована правовая природа договоров, на основе которых брокеры покупают и продают информацию.

Исследование федеральной торговой комиссии США показало, что девять из упомянутых выше брокеров получают информацию из следующих ресурсов:

1) федеральные и региональные органы власти: суды могут предоставлять брокерам информацию о банкротстве тех или иных лиц; миграционная служба – данные о смене мест жительства граждан; избирательные комиссии – данные об избирателях (п. 12 ст. 16 Закона об основных гарантиях избирательных прав и права на участие в референдуме граждан Российской Федерации; данные о регистрации недвижимого имущества того или иного лица могут быть получены из ЕГРП и т.д. Стоит заметить, что многие из указанных источников информации недоступны для информационных брокеров в Российской Федерации в силу ограничения законодательством распространения некоторых видов информации[1];

[1] Справочная информация: «Перечень нормативных актов, относящих сведения к категории ограниченного доступа» // СПС «Консультант Плюс» (дата обращения: 27.02.2017).

2) публично доступные источники информации: более половины информационных брокеров собирают данные (телефонные номера, адреса, иные контактные данные) с помощью информации, которую индивид сам о себе размещает в Интернете, в том числе в социальных сетях;

3) коммерческие организации: информацию о покупках индивида, его денежных тратах, подписках на журналы или газеты информационные брокеры получают у магазинов, издателей печатной продукции, телекоммуникационных компаний. Кроме того, некоторая информация может быть получена от другого информационного брокера[1].

Правовая квалификация договора, на основе которого информационный брокер осуществляет свою деятельность, зависит от правовой квалификации данных.

В литературе изложены различные точки зрения, согласно которым данные (в том числе персональные данные) могут быть квалифицированы как, во-первых, объекты интеллектуальной собственности (произведение, база данных или ноу-хау (ст. 1225 ГК РФ)), во-вторых, как услуга или, в-третьих, как объект гражданских правоотношений.

1. Квалификация информации в качестве объекта интеллектуальной собственности (исключительных прав) в целом не получила поддержки в отечественной доктрине.

По поводу квалификации информации в качестве произведения отрицательно высказывался В.А. Дозорцев. Он считал, что информация хотя и содержится в произведениях, охраняемых авторских правом, сама по себе еще не является таковым, поскольку не обладает характерными для произведения признаками, в частности, творческим началом[2]. Кроме этого, авторское право охраняет форму, а не содержание произведения, в то время как для защиты персональных данных имеет значение именно содержание (ФИО лиц, конкретные вкусовые предпочтения, конкретные геолокации и т.п.).

Признание информации и персональных данных в качестве ноу-хау также было раскритиковано. Это объясняется тем, что режим ноу-хау предполагает отсутствие у третьих лиц свободного доступа к охраняе-

[1] Federal Trade Commission. Data Brokers: A Call for Transparency and Accountability, May 2014 (URL: https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf (дата обращения: 26.02.2017)).

[2] *Дозорцев В.А.* Интеллектуальные права: Понятие. Система. Задачи кодификации. М.: Статут. 2003. С. 234.

мым сведениям (ст. 1465 ГК РФ), в то время как большая часть персональных данных, собранных информационными брокерами, получена из социальных сетей, т.е. из общедоступных источников. Кроме того, информация, являющаяся ноу-хау, должна иметь ценность в силу ее неизвестности третьим лицам, что весьма спорно в отношении персональных данных хотя бы потому, что эти сведения доступны самому субъекту персональных данных как источнику этих данных, так и на законном основании – другим лицам (гл. 2 Закона о персональных данных).

По мнению М.А. Рожковой, для того чтобы база данных стала объектом авторского права, необходимо, чтобы отбор и компоновка ее составляющих соответствовали такому признаку, как креативность[1]. Это вполне соответствует деятельности информационных брокеров, поскольку они классифицируют персональные данные таким образом, что появляются новые группы лиц: граждане «за чертой бедности», «из многодетных семей», «получающие доход выше среднего» и пр. Но авторско-правовую охрану получают не сами данные, включенные в базу, а именно их систематизация, позволяющая находить и обрабатывать эти данные[2].

Для того чтобы база данных охранялась как объект смежных прав, как подчеркивает М.А. Рожкова, она должна стать результатом существенных финансовых, материальных, организационных или иных вложений (инвестиций) и содержать не менее 10 тыс. самостоятельных информационных элементов[3].

База данных, создаваемая информационным брокером, как правило, превышает указанный объем информационных элементов. Но здесь встает вопрос факта существенных финансовых, материальных, организационных или иных затрат при создании базы данных. Дело в том, что до настоящего времени этот момент нередко ставился под сомнение со ссылкой на то, что базы данных «собираются» из информации, ставшей доступной компании при осуществлении ее основного вида деятельности[4]. В качестве примера приводится телефонная компания, создавшая подборку телефонных номеров абонентов, их фамилий,

[1] *Рожкова М.А.* Интеллектуальная собственность: основные аспекты охраны и защиты: учеб. пособие. М.: Проспект, 2017. С. 41.

[2] Там же. С. 40.

[3] Там же. С. 75.

[4] *Войникас Е.А., Калятин В.О.* База данных как объект правового регулирования: учеб. пособие для вузов. М.: Статут, 2011. С. 70–71.

имен и адресов, что вряд ли влечет для этой компании существенные затраты.

Однако информационный брокер как изготовитель базы данных обычно может «похвастаться» вложением колоссальных затрат в создание и поддержание подборки информации, поскольку именно этот вид деятельности для него основной. В то же время если компания (например, занимающаяся перепродажей данных, полученных от осуществления основного вида деятельности, для достижения цели создания) выступит на рынке в качестве информационного брокера, то здесь, действительно, сложно говорить о существенных затратах на создание базы данных.

Таким образом, если база данных, созданная информационным брокером, отвечает указанным критериям инвестиционных вложений и объема данных, то она может рассматриваться в качестве объекта смежных прав. Это позволяет изготовителю базы распоряжаться принадлежащим ему исключительным правом и заключать, в частности, лицензионные договоры на использование базы данных (п. 1 ст. 1334 ГК РФ).

В остальных случаях можно сделать вывод о невозможности классификации договора по передаче данных в качестве лицензионного договора.

На практике же договоры о передаче персональных данных обычно именуются лицензионными. При этом суды не рассматривают вопрос квалификации персональных данных в качестве того или иного объекта исключительного права.

Например, договор, заключенный между ООО «Юниверсал Мьюзик» и UMG «Рекордингс Сервисиз Инк», по условиям которого Центр передавал исключительные права в отношении личных данных артистов, именовался договором о предоставлении исключительных прав (лицензионным договором)[1].

2. Получила развитие точка зрения, согласно которой массив данных, обрабатываемых информационным брокером, представляет собой услугу[2]. Например, в случае если компания предоставляет

[1] Постановление Второго ААС от 18.10.2016 № 02АП-8828/2016 по делу № А82-4938/2016.

[2] *Begoli E., Gunasekaran R., Horey J., Lim S., Nutaro J.* Big Data Platforms as a Service: Challenges and Approach // Computational Sciences & Engineering. Oak Ridge National Laboratory (URL: https://www.usenix.org/system/files/conference/hotcloud12/hotcloud12-final61.pdf (дата обращения: 27.02.2017)).

клиентам сервис, с помощью которого возможен анализ больших объемов данных.

Следование такой точке зрения позволяет применять конструкцию ст. 779 ГК РФ, которая регламентирует договор возмездного оказания услуг и нормы которой распространяются и на информационные услуги.

В то же время признается, что такая конструкция применима лишь к отношениям информационного брокера и клиента, поскольку их правоотношения соответствуют определению договора возмездного оказания услуг. Информационный брокер, выступая на стороне исполнителя. совершает определенные действия (предоставляет облачный сервис в пользование заказчику), а клиент, будучи заказчиком, оплачивает оказанные услуги.

В то же время вряд ли возможно квалифицировать в качестве договора возмездного оказания услуг саму деятельности информационных брокеров по сбору данных. В этом случае нет деятельности, осуществляемой в интересах заказчика, – информационный брокер сам выступает в роли некоего заказчика. При этом платит он не за предоставление права (т.е. не за факт заключения договора), а за фактически потребленные мощности[1].

Выбор договора возмездного оказания услуг позволяет также учесть и вопросы качества предоставляемого сервиса, применяя общие положения о договоре подряда (ст. 783 ГК РФ). В договоре может быть уточнено, какие именно услуги предоставляются заказчику, каким образом услуга будет оказана, кто будет ответствен за исполнение, за перебои в оказании услуги и пр.

В российской судебной практике дела, связанные с предоставлением персональных данных граждан путем использования программного обеспечения как сервиса, еще не встречались. Однако практика квалификации предоставления доступа к программному обеспечению в качестве договора возмездного оказания услуг уже сформировалась. Таким образом был квалифицирован договор между ГУЗ «Городская поликлиника № 8» (заказчик) и ОАО «Ростелеком» (исполнитель) по предоставлению сервиса ИС МИС[2], между ОАО «Ростелеком» (Исполнитель) и ГУЗ «Калганская центральная районная больница» (за-

[1] *Савельев А.И.* Правовая природа облачных сервисов: свобода договора, авторское право и высокие технологии // Вестник гражданского права. 2015. Т. 5. № 5.

[2] Постановление Четвертого ААС от 19.12.2014 № 04АП-4738/2014 по делу № А78-5032/2014.

казчик) на использование информационной системы «Медицинская информационная система»[1].

3. Анализируя природу договора о передаче данных, нельзя обойти стороной конструкцию непоименованного договора в контексте животрепещущего вопроса о том, является ли информация объектом гражданских прав.

С введением в действие части четвертой ГК РФ информация была исключена из ст. 128, посвященной объектам гражданских прав. В литературе до сих пор ведутся дискуссии относительно целесообразности изменения законодательства[2], причем высказывается мнение, что отныне информация не вписывается в систему гражданско-правовых отношений[3].

Между тем думается, что поскольку гражданское законодательство состоит в том числе из федеральных законов (п. 2. ст. 3 ГК РФ), а Закон об информации упоминает допустимость для информации выступать в качестве объекта гражданских прав (ст. 11), то в теории возможно заключение непоименованного договора, объектом которого будет являться информация[4].

Такая трактовка представляется наиболее удачной, поскольку исключает искусственное приравнивание информации к объектам исключительных прав или к услуге. Но судебная практика не единодушна в отношении того, может ли информация выступать в качестве объекта гражданского права. Следствие признания того, что информация не подпадает в круг объектов гражданских отношений и, следовательно, не может выступать в качестве предмета непоименованного договора, приведет к тому, что такой договор будет являться незаключенным в связи с несоблюдением существенных условий договора (п. 1 ст. 432 ГК РФ).

Таким образом, форма взаимодействия информационных брокеров с «поставщиками данных» и с клиентами напрямую зависит от того, как законодатель квалифицирует информацию, в частности персональные

[1] Решение АС Забайкальского края от 26.01.2015 по делу №А78-14182/2014.

[2] *Савельев А.И.* Направления эволюции свободы договора под влиянием современных информационных технологий // Свобода договора. М.: Статут, 2015.

[3] *Войникас Е.* Право интеллектуальной собственности в цифровую эпоху: парадигма баланса и гибкости. М.: Юриспруденция, 2013.

[4] *Инюшкин А.А.* Информация в системе объектов гражданских прав и ее взаимосвязь с интеллектуальной собственностью на примере баз данных // Информационное право. 2016. № 4. С. 6.

данные: это может быть лицензионный договор, договор оказания услуг или непоименованный договор. Каждая из таких конструкций имеет свои достоинства и недостатки.

Сказанное позволяет настаивать на внесении изменений в законодательство в части определения правовой природы информации, что даст возможность определить вид договоров, на основании которых такая информация будет передана.

Кроме того, нельзя не заметить, что отсутствие регулирования деятельности информационного брокера как нового субъекта права не означает отсутствия необходимости такой регламентации. В настоящий момент правовой статус рассматриваемого субъекта может быть определен путем сопоставления ряда признаков, присущих компаниям – информационным брокерам, и тех конструкций, которые уже существуют в законодательстве. Однако такой подход представляется не слишком удачным в связи с тем, что существующие правовые нормы созданы для урегулирования деятельности других субъектов права, обладающих соответствующей спецификой. Таким образом, необходима разработка норм, определяющих деятельность информационных брокеров.

2.2. Правовой статус информационного брокера в контексте информационного права

Итак, предметом деятельности информационного брокера является информация (в частности, персональные данные), что обусловливает необходимость регулирования данного субъекта соответствующими нормами права. В настоящий момент российское законодательство об информации не содержит положений, которые в полной мере регулировали бы деятельность информационного брокера, однако анализ деятельности уже существующих брокеров показывает, что им присущи черты сразу нескольких субъектов права, которые упомянуты в Законе об информации.

В соответствии с действующим законодательством информационного брокера можно квалифицировать в качестве:

– во-первых, **обладателя информации** (ст. 6 Закона об информации).

Согласно п. 5 ст. 2 Закона об информации обладатель информации – это «лицо, самостоятельно создавшее информацию либо получившее на основании закона или договора право разрешать или ограничивать доступ к информации, определяемой по каким-либо при-

знакам». Законом не ограничен перечень лиц, которые могут выступать в качестве обладателя информации: таковым может быть и юридическое лицо, и индивидуальный предприниматель. Следовательно, информационный брокер, получив информацию по договору с правом разрешать или ограничивать доступ к этой информации, может быть квалифицирован в качестве обладателя информации. Опрос, проведенный ФТК, показал, что большинство компаний, покупая и перепродавая данные, устанавливают в договорах ограничения относительно использования информации[1], что подтверждает тезис о квалификации информационного брокера в качестве обладателя информации.

Статья 6 Закона об информации закрепляет перечень прав обладателя информации, которые в общем виде можно свести к следующим: установление порядка и условий доступа к информации, использование информации и защита от несанкционированного получения и использования информации[2].

Осуществление права информационного брокера как обладателя информации устанавливать режим доступа к информации возможно на стадии перепродажи имеющихся данных третьим лицам. При этом обладатель информации не может произвольно ограничивать доступ к любой информации. В частности, ст. 5 ФЗ от 29.07.2004 № 98-ФЗ «О коммерческой тайне» закрепляет перечень сведений, в отношении которых коммерческая организация не может установить режим «коммерческой тайны»; определенные лимиты в отношении ограничения доступа к информации установлены и п. 4 ст. 8 Закона об информации.

В то же время информационный брокер как обладатель информации ограничен в действиях в отношении некоторых категорий данных. Согласно ст. 10 Закона о персональных данных обработка данных о национальной принадлежности, политических и религиозных взглядах, состоянии здоровья, интимной жизни ограниченна. Потенциально информационный брокер может собрать персональные данные специальной категории, например, путем получения согласия субъекта персональных данных на обработку его персональных данных (подп. 1

[1] Federal Trade Commission. Data Brokers: A Call for Transparency and Accountability, May 2014 (URL: https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf (дата обращения: 14.02.2017)).

[2] *Савельев А.И.* Комментарий к Федеральному закону от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и защите информации». М.: Статут, 2015.

п. 2 ст. 10 Закона о персональных данных). Но для того, чтобы осуществить главную цель своей деятельности, т.е. извлечь прибыль за счет перепродажи данных, относящихся к категории специальных, информационный брокер должен получить от субъекта согласие на совершение любых действий с данными, в особенности на использование и передачу.

Квалификация информационного брокера в качестве обладателя информации позволяет ему использовать, в том числе распространять или передавать по договору, полученные данные на законном основании с условием соблюдения ограничений, установленных законодательством об информации и о персональных данных.

Правовой статус обладателя информацией предполагает обязанность принимать меры по защите информации от несанкционированного доступа, в том числе не допускать ее модификации. Возложение на информационных брокеров указанной обязанности представляется целесообразным в целях защиты интересов клиентов брокеров как слабых сторон договора, а также в целях защиты интересов субъектов персональных данных как лиц, теряющих контроль над данными, которые при грамотной обработке могут составить портрет того или иного лица.

Несмотря на то что квалификация информационного брокера в качестве обладателя информации накладывает определенные ограничения на предпринимательскую деятельность субъекта, они все же необходимы в целях защиты прав граждан, чьи данные подвергаются обработке[1];

– во-вторых, **организатора распространения информации в сети Интернет** (ст.10.1 Закона об информации);

Организатор распространения информации в сети Интернет (далее – ОРИвСИ) – это «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 сети Интернет» (п. 1 ст. 10.1 Закона об информации). В свою очередь, информационная система является не чем иным, как совокупностью содержащихся в базах данных информации и технологий, обеспечивающих ее обработку.

[1] *Терещенко Л.К.* Правовой режим персональных данных и безопасности личности // Закон. 2013. С. 37.

Принимая законопроект о регулировании деятельности организатора распространения информации в сети Интернет, Государственная Дума руководствовалась необходимостью борьбы с терроризмом[1]. Действительно, преступники все чаще используют Интернет, социальные сети и мессенджеры для коммуникации, что, безусловно, дает основания возлагать дополнительные обязанности на определенных субъектов права. Страны Европы руководствовались теми же принципами, принимая аналогичный по содержанию акт – Директиву ЕС 2006/24/ЕС «О хранении данных»[2], которая, несмотря на последующее признание неконституционной, была имплементирована в национальное законодательство большинства стран ЕС. Согласно этой Директиве организаторы обязаны хранить метаданные, т.е. данные о трафике, о местонахождении клиентов, другими словами, персональные данные пользователей.

Квалификация информационных брокеров в качестве ОРИвСИ представляется оправданной, поскольку деятельность брокеров направлена на получение и перепродажу именно тех данных, которыми обладают ОРИвСИ.

Широкая формулировка дефиниции ОРИвСИ позволяет квалифицировать информационного брокера (юридическое или физическое лицо) в качестве организатора распространения информации, обладающего правами на базы данных и чья деятельность преимущественно осуществляется в сети Интернет. Однако использование ОРИвСИ информационных систем в целях обработки электронных сообщений ставит под сомнение возможность квалификации информационных брокеров в качестве таковых.

Подзаконные акты, дополняющие нормы федерального законодательства, в частности Правила хранения данных[3], позволяют отнести к ОРИвСИ таких лиц, которые осуществляют функционирование

[1] Решение Комитета по безопасности и противодействию коррупции от 12.02.2014 № 91/3 (СПС «КонсультантПлюс» (дата обращения: 01.03.2017)).

[2] Directive 2006/24/EC «On retention of data generated or processed in connection with the provision of publicly available electronic communication services or of public communications netowrks and amending Directive 2002/58/EC» // OJ L 105/54. 13.04.2006.

[3] Постановление Правительства РФ от 31.07.2014 № 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

коммуникационного интернет-сервиса. Это ограничивает круг лиц, которых можно отнести к ОРИвСИ, теми субъектами, которые позволяют взаимодействовать пользователям между собой.

В качестве ОРИвСИ регистрируются такие компании, как ООО «ВКонтакте», ООО «Мэйл.Ру», ЗАО «Мамба», ООО «Редакция журнала «Закон»», т.е. сервисы, предоставляющие возможность ведения дискуссий между пользователями[1]. В то же время эти компании занимаются сбором, хранением, использованием и передачей метаданных, которые хотя и зашифрованы, но представляют интерес для профайлинга, поскольку показывают, кто с кем общался, в какой период времени, как долго происходило общение.

Однако анализ деятельности существующих компаний – информационных брокеров показывает, что, как правило, здесь взаимодействие происходит между пользователем и машиной. И только в случае если информационный брокер включает в свой функционал коммуникационные сервисы, позволяющие взаимодействовать пользователям между собой, он, без сомнений, будет подпадать под категорию ОРИвСИ.

С учетом изложенного можно сделать вывод о том, что не всякая компания, имеющая доступ к персональным данным пользователей и зарегистрированная в качестве ОРИвСИ, является информационным брокером. В то же время нельзя квалифицировать всех информационных брокеров в качестве ОРИвСИ – такой подход влечет возложение на информационного брокера ненужных обязанностей, в частности, по уведомлению Роскомнадзора об осуществлении деятельности (п. 2 ст. 10.1 Закона об информации);

– в-третьих, **оператора информационной системы** (п. 12 ст. 2 Закона об информации);

Оператором информационной системы может быть как физическое, так и юридическое лицо, «осуществляющее деятельность по эксплуатации информационной системы, в том числе по обработке информации, содержащейся в ее базах данных» (п. 12 ст. 2 Закона об информации). По общему правилу, закрепленному в п. 2 ст. 13 Закона об информации, для квалификации лица в качестве оператора инфор-

государственным органам, осуществляющим оперативно-розыскную деятельность или обеспечение безопасности Российской Федерации».

[1] Реестр организаторов распространения информации в сети «Интернет» // Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций (URL: https://rkn.gov.ru/opendata/7705846236-InformationDistributor/ (дата обращения: 06.03.2017)).

мационной системы необходимо наличие двух условий: наличие права собственности на технические средства, используемые для обработки информации, содержащейся в базах данных, а также правомерное использование этих баз данных (например, по лицензионному договору).

Информационный брокер не всегда может иметь технические средства для обработки информации на праве собственности. Но закон допускает заключение оператором информационной системы договора об эксплуатации информационной системы с собственником технических средств.

Возможна и другая проблема: как было указано выше, не всегда информация, используемая информационным брокерами, может быть квалифицирована как база данных. В таком случае информационный брокер вряд ли может быть отнесен к числу операторов информационной системы. И здесь надо отметить, что в связи с тем, что в настоящий момент законодательство не содержит четких определений, которые позволили бы определить правовой статус информации, в частности персональных данных, открываются широкие возможности для манипуляции правовыми дефинициями и отнесения информационных брокеров к числу операторов информационных систем;

– в-четвертых, **оператора персональных данных** (гл. 4 Закона о персональных данных);

Оператором персональных данных, которым является информационный брокер «по умолчанию» (в силу того, что осуществляет действия по обработке информации в отличие от оператора информационной системы), может выступать государственный и муниципальный орган. Это позволяет причислить к числу информационных брокеров также субъектов публичного права. Например, уже упоминавшийся политический профайлинг базируется на основе данных, сбором которых занимаются муниципальные образования.

При этом необходимо подчеркнуть, что в отличие от ОРИвСИ статус оператора персональных данных не подразумевает возложение на юридическое или физическое лицо чрезмерных обязанностей. Необходимость предоставления субъекту персональных данных информации об операторе до начала сбора данных (п. 3 ст. 18 Закона о персональных данных), обеспечение безопасности персональных данных (п. 2 ст. 19 Закона о персональных данных), сообщение субъекту данных информации о наличии соответствующих данных (п. 1 ст. 20 Закона о персональных данных) являются сбалансированными мерами, позволяющими защитить права и интересы граждан.

Квалификация информационного брокера в качестве оператора персональных данных позволяет решить еще одну проблему, уже обнаружившую себя в США в процессе деятельности упомянутых компаний, – отсутствие прозрачности в деятельности информационных брокеров: граждане не знают, какая именно информация о них была получена. Например, *Experian* и *Equifax* не разрешают субъектам просматривать, какие их персональные данные были получены брокером. Усугубляет проблему тот факт, что у граждан нет информации о том, какие компании являются информационными брокерами, т.е. они могут даже не предполагать, что являются субъектом персональных данных, обрабатываемых какой-либо компанией[1].

Поскольку российское законодательство содержит право субъекта персональных данных на доступ к таковым (ст. 14 Закона о персональных данных), то данная проблема может быть решена путем закрепления обязанности информационного брокера сообщать об осуществлении деятельности по обработке и перепродаже данных в федеральные органы власти под угрозой административного наказания (соответствующие поправки необходимо внести и в КоАП РФ). За органами власти, в свою очередь, необходимо закрепить обязанность по созданию реестра информационных брокеров по аналогии с реестром ОРИвСИ. Такой подход обеспечит соблюдение прав граждан, поскольку они будут знать, какая именно компания является информационным брокером и занимается сбором их персональных данных, но при этом не нанесет ущерба предпринимательской деятельности коммерческих лиц и индивидуальных предпринимателей.

Больше всего вопросов в свете последних изменений законодательства вызывает обязанность оператора персональных данных, установленная ч. 5 ст. 18 Закона о персональных данных. Она возлагает на оператора обязанность при сборе данных обеспечить обработку данных граждан Российской Федерации с помощью информационных систем, находящихся на территории Российской Федерации.

Поскольку большинство баз информационных брокеров, содержащих персональные данные граждан, были созданы до вступления в силу Закона, т.е. до 01.09.2015, то на них не распространяется указанное положение. При этом обратная сила закона может быть установлена при его принятии, но этого сделано не было. В то же время базы

[1] United States Senate (2013). A review of thedata brokers: collection, use and sale of consumer data for marketing purposes. Washington D. C.: Staff report. P. 33.

данных информационных брокеров в силу специфики деятельности должны постоянно обновляться: у субъектов данных меняются предпочтения, меняется их семейное положение и т.д., поэтому положения Закона распространяются и на такие «обновленные» базы данных.

Актуален данный вопрос также в связи с тем, что большинство существующих информационных брокеров – иностранные компании, которые собирают информацию о гражданах Российской Федерации. Наложение на брокеров подобного рода обязательств вынуждает делить базы данных: часть данных хранить по месту осуществления деятельности организации, а другую часть – в стране граждан, чьи данные подвергаются обработке.

С одной стороны, данная норма значительно усложняет деятельность иностранных компаний – информационных брокеров, и в итоге им проще отказаться от обработки данных граждан России (что с учетом положительных сторон профайлинга для субъектов обработки данных не является лучшим решением проблемы).

С другой стороны, существуют определенные сложности применения санкции к компаниям – информационным брокерам: если социальные сети, нарушающие российское законодательство, можно заблокировать (как в случае с *LinkedIn*[1]), то повлиять на компании, не ведущие деятельность в сети Интернет, практически невозможно[2].

Изложенное позволяет заключить, что информационный брокер, обрабатывая данные граждан, неизбежно становится оператором персональных данных, что накладывает на него определенные обязанности, направленные на защиту прав граждан. В то же время квалификация иностранных компаний в качестве оператора порождает целый ряд вопросов, ответы на которые еще предстоит найти;

– в-пятых, **информационного посредника** (ст. 17 Закона об информации).

Закон об информации выделяет два вида информационных посредников.

Первый вид информационных посредников – это лица, оказывающие услуги по передаче информации, предоставленной иным лицом, без ее изменения или исправления в процессе передачи (п. 1 ч. 3 ст. 17 Закона об информации). Характерной чертой деятельнос-

[1] Определение Московского городского суда от 10.11.2016 по делу № 33-38783/2016.

[2] *Беломестнова Н.* Повеяло сервером. Иностранным интернет-магазинам придется заняться обработкой персональных данных в России // Юрист спешит на помощь. 2015. № 9.

ти такого посредника является выполнение функции «проводника» информации – они не изменяют и не исправляют информацию в процессе передачи.

Информационный брокер, получив персональные данные из одного источника, в большинстве случаев подвергает их обработке путем сопоставления друг с другом, выделения общих и различных черт в полученном массиве персональных данных, а после этого передает данные своим клиентам. Следовательно, информационный брокер не может быть включен в число информационных посредников первого вида.

Второй вид информационных посредников – это лица, оказывающие услуги по хранению информации и обеспечению доступа к ней (п. 2 ч. 3 ст. 17 Закона об информации). Как правило, в эту группу попадают провайдеры хостинга или владельцы сайтов в сети Интернет, предоставляющих возможность размещения пользовательского контента, поисковые серверы[1].

На первый взгляд основная деятельность информационных брокеров по получению и перепродаже персональных данных практически не связана с возможностью оказания услуг по хранению информацию. Однако некоторые брокеры – это социальные сети (*Facebook*, «ВКонтакте», *LinkedIn*), и они могут использовать свои веб-сайты в качестве платформы для размещения пользователями информации о себе.

Поскольку ст. 17 Закона об информации регулирует в первую очередь освобождение от ответственности информационных посредников, то следует признать, что придание информационному брокеру статуса информационного посредника в определенных случаях может позитивно сказаться на их деятельности.

Так, в уже рассмотренном выше судебном деле «ВКонтакте» против ООО «Дабл» было установлено, что ООО «Дабл» собирает специальные категории персональных данных о гражданах. Соцсеть «ВКонтакте» в данном случае стала лишь информационным посредником, а потому была освобождена от ответственности. В то же время это не исключает возможности квалификации ООО «ВКонтакте» в качестве информационного брокера в отношении других персональных данных.

Таким образом, на практике признание информационного посредника информационным брокером маловероятно – это два параллельно

[1] *Савельев А.И.* Комментарий к Федеральному закону от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и защите информации». М.: Статут, 2015.

существующих статуса одного лица, которые вряд ли могут пересечься. Следовательно, это не влечет освобождение информационных брокеров от ответственности как информационных посредников.

Подводя итог, необходимо отметить, что информационный брокер, будучи субъектом права, чья основная деятельность связана с обработкой информации, в частности с персональными данными граждан, не может остаться за рамками регулирования Закона об информации и Закона о персональных данных. Однако отсутствие прозрачности в деятельности существующих компаний – информационных брокеров, а также отсутствие в законодательстве легальной дефиниции нового субъекта права не позволяет в полной мере соотнести его с уже существующими субъектами и, как следствие, определить правовые рамки его деятельности.

Пристатейный библиографический список:

1. *Белов В.А.* Что изменилось в Гражданском кодексе?: практ. пособие. М.: Юрайт, 2014.

2. *Ласкина Н.В., Степаненко О.В.* Комментарий к Федеральному закону от 04.05.2011 № 99-ФЗ «О лицензировании отдельных видов деятельности» // СПС «КонсультантПлюс». 2015.

3. *Савельев А.И.* Комментарий к Федеральному закону от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и защите информации». М.: Статут, 2015.

4. *Castelluccia C.* Behavioural Tracking on the Internet: A Technical Perspective. Behavioural Tracking on the Internet: A Technical Perspective. Netherlands: Springer, 2012.

5. *Fitsch L.* Profiling and Location-Based Services (LBS) // Profiling the European Citizens. Cross-Disciplinary Perspectives. Springer, 2008.

6. *Gurtwirth S., Hert P., Poullet Y.* Data Protection in a Profiled World. Springer, 2010.

7. *Hildebrandt M.* Who is Profiling Who? Invisible Visibility // Gutwirth S., Poullet, Y., De Hert, P. De Terwangne C., Nouwt S. (eds), Reinventing Data Protection? Dordrecht, Springer, 2009.

8. *Hildebrandt M., Gutwirth S.* General Introduction and Overview // Mireille Hildebrandt and Serge Gutwirth (eds), Profiling the Europen Citizen: Cross disciplinary perspectives. Dordrecht: Springer Science, 2008.

9. *Lyon D.* Surveillance as Social Sorting: Privacy, Risk and Digital Discrimination. New York: Routledge, 2003.

10. *Moeckli D., Thurman J.* Counter-terrorism data mining: legal analysis and best practices. DETECTER project – Detection Technologies, Terrorism, Ethics and Human Rights. Deliverable 08.03.2008.

11. *Rieke A., Yu H., Robinson D., von Hoboken J.* Data broker in an open Society. London: Bloomberg, 2016.

12. *Taipale K.* The privacy implications of Government Data Mining Programs. Testimony before the US Senate Committee on the Jurisdiciary, 10 January.

13. United States Senate. (2013). A review of thedata brokers: collection, use and sale of consumer data for marketing purposes. Washington D.C.: Staff report.

14. *Соколова О.С.* Правовые основы саморегулирования // Юрист. 2008. № 4.

15. *Cavoukian A.* Privacy as a Fundamental Human Rights vs. Economic Right: An Attempt at Conciliation. 1999.

16. *Савельев А.И.* Направления эволюции свободы договора под влиянием современных информационных технологий // Свобода договора. М.: Статут, 2015.

17. *Терещенко Л.К.* Правовой режим персональных данных и безопасности личности // Закон. 2013. № 6.

18. *Gurtwirth S., Hert P., Poullet Y.* (2010) Data Protection in a Profiled World. Springer.

19. *Ellyne E., Gutwirth S., Fuster G. G.* Profiling in the European Union: A high-risk practice. INEX Policy Brief, No. 10.

20. *Hildebrandt M.* Profiling: from data to knowledge // Datenschutz und Datensuchereit. 2006. N 30. Vol. 9.

21. *Boersma K., Van Brakel R., Fonio C., Wagenaar P.* History of State surveillance in Europe and beyond // Rouledge studies in crime and society, 2014.

22. *Johnson J.P.* Targeted advertising and advertising avoidance. Mimeo, Johnson

23. *Wakulowsky L.* Managing the Privacy Side Effects of Rx (and other) Customer Loyalty Programs // Health Law Bulletin. 2014.

24. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data / Official Journal of the European Union. L 281/31. Vol. 38, 23 November 1995. (URL:

http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:L:1995:281:TOC).

25. Regulation of the European Praliament and of the council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) (URL: http://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX: 52012PC0011).

26. Directive 2006/24/EC «On retention of data generated or processed in connection with the provision of publicly available electronic communication services or of public communications networks and amending Directive 2002/58/EC» // OJ L 105/54. 13.04.2006.

27. *About Us* // PeekYou (URL: http://www.peekyou.com/about/ (дата обращения: 15.02.2017)).

28. Acxiom Corp., Annual Report, 2015 (URL: http://investors.acxiom.com/secfiling.cfm?filingid=733269-15-18&cik=733269#F10K_HTM_4 (дата обращения: 15.02.2017).

29. Article 29 Working Party (2013), Advice paper on essential elements of a definition and a provision on profiling within the EU General Data Protection Regulation, adopted on 13 May 2013. URL: http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2013/20130513_advice-paper-on-profiling_en.pdf (дата обращения: 19.01.2017).

30. Article 29 Working Party // The EDPS (URL: https://secure.edps.europa.eu/EDPSWEB/edps/Cooperation/Art29).

31. *Begoli E., Gunasekaran R., Horey J., Lim S., Nutaro J.* Big Data Platforms as a Service: Challenges and Approach // Computational Sciences & Engineering. Oak Ridge National Laboratory. (URL: https://www.usenix.org/system/files/conference/hotcloud12/hotcloud12-final61.pdf (дата обращения: 27.02.2017)).

32. *Bosco G. Cafiero, D'Angelo E., Ferraris V., Suloyeva Y.* Profiling. Protecting citizens' rights fighting illicit profiling (URL: http://profiling-project.eu/wp-content/uploads/2015/01/Profiling_final_report_20141.pdf (дата обращения 02.09.2016)).

33. *Bosco G. Cafiero, D'Angelo E., Ferraris V., Suloyeva Y.* Working Paper Defining Profiling. P. 12. (URL: http://profiling-project.eu/wp-content/uploads/2013/07/PROFILINGproject_WS1_definition_0208.pdf (дата обращения: 05.01.2017)).

34. *Bosco G. Cafiero, D'Angelo E., Ferraris V., Suloyeva Y.* Working Paper Defining Profiling. P. 23 (URL: http://profiling-project.eu/wp-content/uploads/2013/07/PROFILINGproject_WS1_definition_0208.pdf (дата обращения: 19.01.2017).

35. Common assessment framework – CAF – Child protection – CCLC // Children's Legal Centre (URL http://www.protectingchildren.org.uk/cp-system/child-in-need/caf (дата обращения: 16.01.2017)).

36. Corelogic, Annual Report 7 (2012) (URL: http://phx.corporate-ir.net/External.File?item=UGFyZW50SUQ9MTkwNDg0fENoaWxkSUQ9LTF8VHlwZT0z&t=1 (дата обращения: 15.02.2017)).

37. Council of Europe, Recommendation CM/Rec(2010)13 of the Committee of Ministers to Member States on the protection of individuals with regard to automatic processing of personal data in the context of pro ling. Adopted by the Committee of Ministers on 23 November 2010 at the 1099th meeting of the Ministers' Deputies (URL: http://www.coe.int/t/dghl/standardsetting/cdcj/CDCJ%20Recommendations/CMRec(2010)13E_Profiling.pdf).

38. Data & Technology // ID Analytics (URL: http://www.idanalytics.com/data-and-technology/ (дата обращения: 15.02.2017)).

39. Data Protection Report. February 2015 – March 2015 (URL: http://ec.europa.eu/COMMFrontOffice/publicopinion/index.cfm/Survey/getSurveyDetail/instruments/SPECIAL/surveyKy/2075 (дата обращения: 15.02.2017)).

40. Datatilsynet. The Great Data Race: How commercial utilisation of personal data challenges privacy, November 2015 (URL: http://www.datatilsynet.no/Global/04_analyser_utredninger/2015/engelsk-kommersialisering-november-2015.pdf (дата обращения: 14.02.2017)).

41. eBureau About us // eBureau (URL: http://www.ebureau.com/about (дата обращения: 15.02.2017)).

42. Email Intelligence Pricing // TowerData (URL: http://www.towerdata.com/email-intelligence/pricing (дата обращения: 15.02.2017)).

43. EU Passenger Name Records (PNR) directive: an overview // European Parliament News (URL http://www.europarl.europa.eu/news/en/news-room/20150123BKG12902/eu-passenger-name-record-(pnr)-directive-an-overview (дата обращения: 16.01.2017)).

44. Facebook partnership with Datalogix helps measure offline impact of online ads // Adweek (URL: http://www.adweek.com/digital/facebook-partnership-with-datalogix-helps-measure-offline-impact-of-online-ads/ (дата обращения: 15.02.2017)).

45. Federal Trade Commission. Data Brokers: A Call for Transparency and Accountability,May 2014 (URL: https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report- federal-trade-commission-may-2014/140527databrokerreport.pdf (дата обращения: 14.02.2017)).

46. Federal Trade Commission. Data Brokers: A Call for Transparency and Accountability, May 2014 (URL: https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf (дата обращения: 26.02.2017)).

47. Federal Trade Commission. Data Brokers: A Call for Transparency and Accountability, May 2014 (URL: https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf (дата обращения: 14.02.2017)).

48. *Friedland G., Sommer R.* Cybercasing the Joint: On the Privacy Implications of Geo-Tagging, 2010 (URL: http://www.icsi.berkeley.edu/pubs/networking/cybercasinghotsec10.pdf/ (дата обращения: 15.01.2017)).

49. Graduate School of Management, Cornell University, 2009 (URL: http://sites.northwestern.edu/csio/files/2015/08/Johnson-2hvjmfr.pdf (дата обращения: 20.01.2017)).

50. How To Block Targeted Ads From Following You Around // Business Insider (URL http://www.businessinsider.com/how-to-keep-ad-companies-from-tracking-your-web-history-2011-2 (дата обращения: 20.01.2017)).

51. Intelius Facts // Intelius (URL: http://corp.intelius.com/intelius-facts (дата обращения: 15.02.2017)).

52. *Macmanus, M.* A guide to recommender systems. January, 2009 (URL: http://readwrite.com/2009/01/26/recommender_systems/ (дата обращения: 14.01.2017)).

53. Next Generation Identification (NGI) // Federal Bureau of Investigation (URL https://www.fbi.gov/services/cjis/fingerprints-and-other-biometrics/ngi (дата обращения: 16.01.2017)).

54. OECD, Exploring the Economics of Personal Data (URL: http://www.oecd-ilibrary.org/science-and-technology/exploring-the-economics-of-personal-data_5k486qtxldmq-en (дата обращения: 14.02.2017)).

55. Office of the Privacy Commissioner of Canada, *Data Brokers: A Look at the Canadian and American Landscape*, September 2014 (URL: https://www.priv.gc.ca/information/research-recherche/2014/db_201409_e.pdf (дата обращения: 14.02.2017)).

56. Oracle, Annual Report, 2015 (URL: http://www.annualreports.com/HostedData/AnnualReports/PDF/NASDAQ_ORCL_2015.pdf (дата обращения: 15.02.2017)).

57. Proposal for a Directive concerning the protection of individuals in relation to the processing of personal data, COM (90), 314 final, SYN 287

and 288, Brussels, 13 September 1990 (URL: http://aei.pitt.edu/3768/1/3768.pdf/ (дата обращения: 17.01.2017)).

58. Recorded Future // SCmagazine (URL: https://www.scmagazine.com/recorded-future/article/629728ь (дата обращения: 15.02.2017)).

59. Senator John D. Rockefeller IV «What Information Do Data Brokers Have on Consumers, and How Do They Use It?» December 18, 2013 (URL: https://www.commerce.senate.gov/public/index.cfm/ hearings?Id=a5c3a62c-68a6-4735-9d18-916bdbbadf01&Statement_id=A47C 081A-D653-4272-8D12- D6EDC1E04DC6 (дата обращения: 15.02.2017)).

60. United States Government Accountability Office. Information Resellers: Consumer Privacy Framework Needs to Reflect Changes in Technology and the Marketplace, Report to the Chairman, Committee on Commerce, Science, and Transportation, US Senate, September 2013 (URL: http://www.gao.gov/assets/660/658151.pdf (дата обращения: 14.02.2017)).

61. United States Senate Committee Commerce, Science, and Transportation, Office of Oversight and Investigations, Majority Staff. A Review of the Data Broker Industry: Collection, Use, and Sale of Consumer Data for Marketing Purposes. December 18, 2013 (URL: http://educationnewyork.com/files/rockefeller_ databroker.pdf (дата обращения: 14.02.2017)).

62. Автоматизированные централизованные базы персональных данных о пассажирах и персонале (экипаже) транспортных средств // ФГУП «ЗащитаИнфоТранс» (URL: http://www.z-it.ru/projects/egis-otb/acbpdp (дата обращения: 09.02.2017)).

63. Безопасность в информационном обществе: вызовы нового века. Пресс-выпуск 3282 // ВЦИОМ (URL: http://wciom.ru/index.php?id=236&uid=116024 (дата обращения: 09.02.2017)).

64. В России появится единая база с данными всех граждан страны // RTU (URL: https://russian.rt.com/article/314043-v-rossii-poyavitsya-edina-ya-baza-s-dannymi (дата обращения: 08.02.2016)).

65. Реестр организаторов распространения информации в сети «Интернет» // Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций (URL: https://rkn.gov.ru/opendata/7705846236-InformationDistributor/ (дата обращения: 06.03.2017)).

66. Решение Комитета по безопасности и противодействию коррупции от 12.02.2014 № 91/3 // СПС «КонсультантПлюс» (дата обращения: 01.03.2017).

67. Справочная информация: «Перечень нормативных актов, относящих сведения к категории ограниченного доступа» // СПС «КонсультантПлюс» (дата обращения: 27.02.2017).

М.З. Али

ОГРАНИЧЕНИЕ ДОСТУПА К ИНФОРМАЦИОННЫМ РЕСУРСАМ В СЕТИ ИНТЕРНЕТ (ПРАКТИЧЕСКИЕ ПРОБЛЕМЫ ПРИЗНАНИЯ ИНФОРМАЦИИ ЗАПРЕЩЕННОЙ К РАСПРОСТРАНЕНИЮ)

Аннотация. *В статье на примере реальных судебных дел о блокировке сайтов рассматриваются сложности, с которыми сталкиваются суды при определении оснований для признания информации запрещенной к распространению. Кроме того, дается оценка правильности соблюдения процессуальных норм и принципов при рассмотрении таких дел.*

Ключевые слова: *судебная практика, блокировка сайтов, распространение информации.*

1. История вопроса

Начиная с 2012 г. Закон об информации стал дополняться специальными статьями, регулирующими ограничение доступа к информационным ресурсам в сети Интернет, первой из которых стала ст. 15.1, предусматривающая создание «Единого реестра доменных имен, указателей страниц сайтов в сети «Интернет» и сетевых адресов, позволяющих идентифицировать сайты в сети «Интернет», содержащие информацию, распространение которой в Российской Федерации запрещено» (далее – Единый реестр), а также основания включения в него адресов, отсылающих к сайтам с запрещенной информацией. По сути, это положило начало полноценному законодательному закреплению оснований для блокирования интернет-сайтов, процедура которого осуществляется через Роскомнадзор и приводится в действие операторами связи.

В соответствии с подп. 1 п. 5 ст. 15.1 Закона об информации к запрещенной для распространения в Интернете информации стала относиться: (а) порнография с участием несовершеннолетних; (б) информация о способах создания/использования наркотических средств; (в) информация о способах самоубийства; (г) сведения о несовершеннолетнем, пострадавшем в результате противоправного деяния;

(д) информация, нарушающая запрет на проведение азартных игр в сети Интернет.

Кроме того, отдельным подп. 2 п. 5 ст. 15.1 Закона об информации установлено, что решением суда запрещенной может быть признана и иная информация на усмотрение суда.

В дальнейшем Закон об информации пополнился нормами об ограничении доступа к информационным ресурсам и по иным основаниям, в том числе: при наличии на них «пиратского» контента (ст. 15.2[1], ст. 15.6[2]), призывов к массовым беспорядкам/экстремизму (ст. 15.3); при неисполнении обязанностей[3] организатором распространения информации в сети Интернет (ст. 15.4); информации, обрабатываемой с нарушением законодательства в области персональных данных (ст. 15.5[4]).

Обобщая имеющиеся на сегодняшний день основания для блокировки сайтов, можно отметить, что такие ограничения доступа могут быть направлены как на защиту общественных интересов (например, для целей пресечения экстремизма), так и на защиту частных интересов конкретного лица (например, для защиты его персональных данных или интеллектуальной собственности).

Регулярное введение законодателем специальных оснований для блокировки интернет-сайтов, однако, не означает, что ранее требование о блокировке информационного ресурса в Интернете было невозможным в принципе. Она могла быть и ранее предписана в судебном решении для целей реализации тех или иных норм законодательства.

Как следует из п. 1 ст. 10, п. 5 ст. 15 Закона об информации, свободное распространение информации гарантируется при условии соблюдения требований и ограничений, предусмотренных законо-

---

[1] Введена так называемым антипиратским законом (см. ФЗ от 02.07.2013 № 187-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации по вопросам защиты интеллектуальных прав в информационно-телекоммуникационных сетях»).

[2] Регулирует «пожизненную» блокировку сайта, на котором неоднократно и неправомерно размещалась информация, содержащая объекты авторских (смежных) прав.

[3] Речь идет о хранении информации о передаче сообщений пользователями такого организатора и иных обязанностях, предусмотренных ст. 10.1 Закона об информации.

[4] Введена «законом о локализации персональных данных» (см. ФЗ от 21.07.2014 № 242-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации в части уточнения порядка обработки персональных данных в информационно-телекоммуникационных сетях».

дательством. Следовательно, если распространение информации нарушает законодательство, то такое распространение может быть ограничено. В соответствии с этим судебная практика по блокированию интернет-ресурсов появилась еще до введения ст. 15.1 Закона об информации.

В рамках рассмотрения вопроса об основаниях ограничения доступа к сайту до введения специальных норм показательной представляется правовая позиция, сформулированная в Определении ВС РФ от 10.05.2011 № 58-Впр11-2. Согласно данной позиции, предоставляя техническую возможность доступа к запрещенной законом информации, оператор телематических услуг связи *«фактически выступает ее распространителем в отношении других лиц»*. Имея техническую возможность, он должен в силу закона принять меры по ограничению доступа к интернет-сайту.

Данная правовая позиция практически по сей день достаточно часто используется судами для удовлетворения требований прокуроров об ограничении доступа к тому или иному ресурсу[1].

Более того, как указал Санкт-Петербургский городской суд в определении от 11.03.2014 № 33-3652/2014, наличие в Законе об информации порядка ограничения доступа к сайтам, установленного ст. 15.1, не освобождает оператора связи от обязанности ограничить доступ к материалам, даже не включенным в Единый реестр, если такие сайты содержат информацию, признанную запрещенной[2].

В связи с этим следует признать, что введение специальных оснований для блокировки информации, во-первых, конкретизировало случаи, когда такое ограничение доступа к информации возможно, а во-вторых, обеспечило существование специального поэтапного

[1] См., например, определения: ВС РФ от 09.10.2012 № 91-КГПР12-3; Санкт-Петербургского городского суда от 18.03.2014 № 33-3515/2014; апелляционные определения Суда Ханты-Мансийского автономного округа – Югры от 17.07.2012 по делу № 33-3106 / 2012; Омского областного суда от 16.10.2013 по делу № 33-6677 / 2013; Московского городского суда от 16.01.2014 по делу № 33-988 / 2014; Верховного суда Республики Дагестан от 14.04.2016 по делу № 33-1393/2016.

[2] Тем не менее, как отмечает А.И. Савельев, существует немногочисленная судебная практика в суде Ямало-Ненецкого автономного округа и Калужского областного суда, в соответствии с которой прокурор не вправе обращаться с подобными требованиями непосредственно к операторам связи, если спорные *IP*- или *URL*-адреса не включены в Единый реестр (см.: *Савельев А.И.* Комментарий к Федеральному закону от 27 июля 2006 г. «Об информации, информационных технологиях и защите информации» (постатейный) (СПС «КонсультантПлюс»)).

механизма блокировки. Данный механизм подразумевает участие Роскомнадзора, хостинг-провайдеров и операторов связи, и в большинстве случаев он включает стадию уведомления владельца сайта о планируемом ограничении доступа к сайту, что дает последнему возможность устранить нарушение добровольно.

Тем не менее нельзя признать, что в законодательстве были выработаны в достаточной мере полные и системные подходы к ограничению доступа к сайтам в сети Интернет, ввиду чего и законодательные основания для блокировки сайтов, и практика их применения возникают весьма хаотично, что приводит к появлению достаточно спорных правоприменительных актов.

Особую актуальность в проблематике ограничения доступа к информации в Интернете придает статистика блокировки сайтов. По данным ресурса «Роскомсвобода»[1] блокировке в России за все время подверглись более 3,99 млн доменных имен, из которых более 2,57 млн заблокированы по решению суда. Можно обратить внимание и на то, что Международная неправительственная организация «Репортеры без границ» отнесла Российскую Федерацию к числу «врагов Интернета»[2].

В рамках настоящей статьи хотелось бы остановиться на возникающих в правоприменительной практике проблемах, связанных с признанием судами информации, запрещенной к распространению в порядке ст. 15.1 Закона № 149-Ф, в том числе с основаниями и порядком признания информации в качестве таковой[3].

---

[1] https://reestr.rublacklist.net/visual/

[2] См.: «nemies of the Internet 2014: entities at the heart of censorship and surveillance (URL: http://12mars.rsf.org/wp-content/uploads/EN_RAPPORT_INTERNET_BD.pdf).

[3] При этом автор не претендует на рассмотрение всех возможных проблем практического характера, вызванных блокировкой сайтов. Например, за рамками настоящей статьи остаются такие проблемы, как ограничение доступа к доменным именам, не адресующим к запретной информации, когда блокировка осуществляется по сетевому (*IP*-) адресу, охватывающему не только «нелегальные», но и «легальные» доменные имена. Кроме того, еще одной из проблем имеющегося механизма блокировки является относительная простота в ее обходе техническими средствами, например, путем создания сайтов-«зеркал» (идентичных тому ресурсу, к которому ограничен доступ) или использования *VPN*-сервисов, которые помогают скрыть личность пользователя и его местоположение. Тем самым на текущий момент ограничение доступа к интернет-сайтам имеет во многом «имиджевый» эффект: государство объявляет конкретный ресурс «вне закона», однако последний продолжает функционировать, приучая своих посетителей использовать инструменты по преодолению блокировки.

2. Проблема ограничения доступа к информации, за распространение которой предусмотрена административная или уголовная ответственность

Как было сказано выше, суд, руководствуясь ст. 15.1 Закона об информации, вправе признать запрещенной в том числе ту информацию, которая прямо не поименована в качестве таковой в Законе.

Как правило, суды в таких случаях ссылаются на п. 6 ст. 10 Закона об информации, устанавливающий запрет на распространение информации, которая направлена на пропаганду войны, разжигание национальной, расовой или религиозной ненависти и вражды, а также иной информации, за распространение которой предусмотрена уголовная или административная ответственность.

К информации, распространение которой дает возможность применения блокировки на основании п. 6 ст. 10 Закона об информации, относятся, в частности:

(1) информация с ограниченным доступом[1], в том числе сведения, составляющие личную или семейную тайну[2], коммерческую, налоговую или банковскую тайну[3], государственную тайну[4];

(2) сведения, содержащие клевету[5] или оскорбление[6];

(3) агитационные материалы, распространяемые в нарушение закона[7];

(4) информация, составляющая кредитную историю[8].

---

[1] Статьей 13.14 КоАП РФ установлена административная ответственность за их разглашение, если в таком деянии нет состава преступления.

[2] Уголовная ответственность за ее распространение установлена ст. 137 УК РФ.

[3] Уголовная ответственность за незаконное разглашение таких сведений установлена ст. 183 УК РФ.

[4] Уголовная ответственность за незаконное разглашение таких сведений установлена ст. 283 УК РФ.

[5] Статьей 128.1 УК РФ предусмотрена уголовная ответственность за распространение заведомо ложных сведений, порочащих честь и достоинство другого лица или подрывающих его репутацию.

[6] Оскорбление, содержащееся в публичном выступлении, публично демонстрирующемся произведении или средствах массовой информации, влечет административное наказание согласно ч. 2 ст. 5.61 КоАП РФ.

[7] Административная ответственность за их незаконное распространение установлена ст. 5.12 КоАП РФ.

[8] Соответствующая административная ответственность предусмотрена ст. 5.53 КоАП РФ.

Однако на практике достаточно часто суды подменяют понятие *информации, за распространение которой* предусмотрена административная или уголовная ответственность, понятием *информации о действиях, за совершение которых* предусмотрена административная или уголовная ответственность.

Такого (ошибочного, по мнению автора) подхода придерживается в том числе ВС РФ.

В частности, Определением ВС РФ от 26.02.2013 № 6-КГПР13-1 были отменены постановления нижестоящих судов по делу, в котором прокурор требовал прекратить доступ к «вредоносным интернет-ресурсам», содержащим сведения о способах приготовления взрывных устройств. ВС РФ не согласился с доводами нижестоящих судов о том, что информация на сайтах не признана в установленном порядке экстремистским материалом, а также о том, что бесспорных доказательств возможности с использованием данной информации изготовить взрывное устройство («бомбу»), пригодное для совершения террористического акта, не было представлено. Отправляя дело на новое рассмотрение, ВС РФ указал, что «*предоставление возможности доступа к информации о способах приготовления взрывных устройств с использованием информационно-телекоммуникационных услуг сетей, в том числе сети Интернет, фактически является информационным пособничеством террористической деятельности, создающим опасность причинения вреда жизни и здоровью граждан, безопасности государства, за осуществление которого предусмотрена уголовная ответственность*».

Таким образом, мотивы, приведенные судом, противоречат смыслу п. 6 ст. 10 Закона об информации, который явно устанавливает запрет на распространение сведений, только если *само по себе распространение информации* образует состав административного или уголовного правонарушения.

Ожидаемо, что такая практика ВС РФ дает нижестоящим судам возможность придерживаться столь же произвольного подхода к толкованию Закона об информации.

К примеру, Кронштадтский районный суд Санкт-Петербурга[1] признал запрещенной размещенную в сети Инструкцию по даче взятки полицейскому, сославшись лишь на то, что непосредственно дача взятки является уголовно наказуемым деянием.

[1] См.: решение Кронштадтского районного суда Санкт-Петербурга от 26.08.2014 по делу № 2-824 / 2014.

Аналогичным образом Санкт-Петербургский городской суд[1], поддерживая решение суда первой инстанции об ограничении доступа к интернет-сайту в другом деле, сослался на то, что на нем размещена информация о способах взяточничества и уклонения от уголовной ответственности, тогда как положениями ст. 290, 291 УК РФ установлена уголовная ответственность за получение и дачу взятки.

Еще в одном похожем деле Алтайский краевой суд также признал[2] запрещенной информацию об изготовлении взрывчатых веществ. При этом суд сослался на ст. 223.1 УК РФ, согласно которой незаконное изготовление взрывчатых веществ предусматривает уголовное наказание.

Во всех перечисленных случаях суды не упомянули, какой нормой предусмотрена административная или уголовная ответственность за распространение заблокированной ими информации. По сути, суды берут на себя роль законодателя, дополняя по своему усмотрению основания для блокировки интернет-ресурсов.

Такой расширительный подход к определению оснований для ограничения доступа к интернет-сайту может привести к весьма абсурдным результатам правоприменения. Сведения о совершенных преступлениях и способах их совершения нередко содержатся в художественных произведениях или даже в обучающих материалах по криминалистике. Однако это вовсе не значит, что такого рода информация действительно запрещена на территории Российской Федерации и ее распространение должно приводить к блокировке информационного ресурса.

3. Проблема использования судами произвольных оснований для ограничения доступа к интернет-сайту

Еще одним серьезным недостатком текущей судебной практики по делам об ограничении доступа к информации является использование судами не основанных на законе мотивов к блокировке того или иного ресурса, которые не имеют отношения к той или иной норме законодательства в принципе.

Можно считать показательными апелляционные определения Тульского областного суда от 06.06.2013 по делу № 33-1377, от 16.05.2013 по делу № 33-1209, от 16.05.2013 по делу № 33-1184, от 04.04.2013

[1] См.: определение Санкт-Петербургского городского суда от 11.03.2014 № 33-3652 / 2014.

[2] См.: апелляционное определение Алтайского краевого суда от 14.10.2015 по делу № 33-9677 / 2015.

по делу № 33-831/13, а также кассационное определение Тульского областного суда от 12.01.2012 по делу № 33-79.

В указанных судебных актах в качестве мотива к блокировке интернет-сайта указывалось, что *«наличие доступа неограниченного круга граждан к сайтам с азартными играми способствует подрыву морально-нравственных устоев общества и вырабатыванию психологической зависимости граждан от азартных игр»*.

В то же время суд не приводил конкретных, основанных на законе, доводов к тому, почему сайт с азартными играми (а) подрывает морально-нравственные устои и (б) способствует психологической зависимости от азартных игр, а также почему (в) данные обстоятельства должны быть поводом для блокировки ресурса[1].

По сути, суд самостоятельно создал критерий по признанию информации, запрещенной к распространению, с одной стороны, взяв на себя полномочия законодателя[2], а с другой – нарушив принцип свободного распространения информации (разумеется, при условии соблюдения ограничений, установленных законом)[3].

Интересно, что использование такой вольной мотивировки для блокирования онлайн-казино встречалось и в практике иных судов.

Например, Московский городской суд в апелляционном определении от 28.01.2015 по делу № 33-2697 указал, что предоставление доступа к онлайн-казино *«подрывает основы материального благополучия неопределенного круга лиц, посягает на общественную нравственность посредством создания условий для вовлечения в азартные игры несовершеннолетних лиц»*.

Похожее в части правовой позиции суда дело приводится в Обзоре судебной практики по гражданским делам за октябрь 2011 года, подготовленным Белгородским областным судом. В нем приводится дело по иску Старооскольского городского прокурора к оператору связи об

[1] Следует отметить, что данные дела были рассмотрены еще до принятия ФЗ от 21.07.2014 № 222-ФЗ «О внесении изменений в Федеральный закон «О государственном регулировании деятельности по организации и проведению азартных игр и о внесении изменений в некоторые законодательные акты Российской Федерации» и отдельные законодательные акты Российской Федерации», которым содержащийся в п. 5 ст. 15.1 Закона об информации перечень сведений, включаемых в Единый реестр, был дополнен пунктом «д», относящим к запретной информацию, нарушающую запрет на проведение азартных игр и лотерей в сети Интернет.

[2] В нарушение принципа разделения властей, установленного ст. 10 Конституции РФ.

[3] См. ч. 4 ст. 27 Конституции РФ, п. 1 ст. 10 Закона об информации.

ограничении доступа к сайтам, содержащим информацию о способах самоубийства.

Суд первой инстанции отказал в данном требовании прокурора ввиду того, что федеральным законом не предусмотрен запрет на распространение спорной информации. В то же время суд апелляционной инстанции счел такие доводы неверными[1].

Во-первых, он сослался на декларативные нормы о целях регулирования общественных отношений в области развития детей. В частности, на то, что п. 1 ст. 4 ФЗ от 24.07.1998 № 124-ФЗ «Об основных гарантиях ребенка в Российской Федерации» установлены такие цели государственной политики, как содействие физическому, интеллектуальному, психическому, духовному и нравственному развитию детей, а также защита детей от факторов, негативно влияющих на их физическое, интеллектуальное, психическое, духовное и нравственное развитие. Кроме того, суд указал, что необходимо исходить из приоритета интересов несовершеннолетних детей, закрепленного п. 1 ст. 3 Конвенции о правах ребенка, одобренной Генеральной Ассамблеей ООН 20.11.1990.

Во-вторых, суд указал, что распространенная в Интернете информация: «*Оказывает негативное воздействие на психическое состояние детей подросткового и юношеского возраста*»; «*подрывает духовное и нравственное развитие несовершеннолетних, смещает моральные акцепты, отторгает их от традиционных нравственных национальных ценностей*»; «*не только провоцирует суицидальные поступки, но и инициирует поиск ассоциаций и аморальной информации, провоцирует действия шантажирующего характера у подростков*».

Представляется неверным подход к расширительному толкованию ограничений распространения информации, основанный на прямом применении принципов правового регулирования в той или иной области, поскольку это в существенной степени подрывает принцип правовой определенности и свободу слова. Самостоятельно определив основание для блокировки сайта, Белгородский областной суд, как и в рассмотренных выше случаях, помимо судебной, вторгся в область ответственности федерального законодателя, так как только последний может устанавливать ограничения доступа к информации.

[1] Необходимо отдельно обратить внимание то, что данное дело было рассмотрено до введения в Закон об информации ФЗ от 28.07.2012 № 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» ст. 15.1.

По мнению автора, подобная мотивировка судебных постановлений является крайне сомнительной, даже если наряду с абстрактными доводами суда о *«подрыве морально-нравственных устоев»* суд все-таки приводит иные доводы, которые уже основаны на конкретных нормах законодательства. Указание не следующих из закона мотивов принятия судебного постановления не только нарушает требования к содержанию решения суда (ст. 198 ГПК РФ), но и может нарушить единообразие в правоприменительной деятельности судов, что, к слову, является основанием для признания судебного постановления незаконным в силу ст. 391.9 ГПК РФ.

Попытки судов, ограничивающих доступ к веб-ресурсам, сослаться на нормы материального права нередко приводят к указанию нерелевантных ссылок на нормативно-правовые акты вкупе с правовыми позициями, которые из них не следуют.

Именно такой случай имел место в упомянутом выше решении Кронштадтского районного суда Санкт-Петербурга, где была признана запрещенной распространенная в сети Интернет «Инструкция по даче взятки полицейскому». Суд в данном деле, помимо не относящейся к сути спора[1] ссылки на п. 6 ст. 10 Закона об информации, указал, что распространение таких сведений *«подрывает конституционный строй и авторитет Российской Федерации, а также основы нравственности граждан России, способствует развитию коррупции, чем нарушает права и законные интересы неопределенного круга лиц, получающих доступ к незаконной информации, в связи с чем подлежит ограничению»*.

4. Процессуальные проблемы признания информации запрещенной к распространению

Отдельно следует остановиться на процессуальных проблемах признания информации запрещенной, учитывая, что в законодательстве отсутствуют прямые указания о порядке рассмотрения дел такого рода.

Изначально практика рассмотрения подобных дел складывалась следующим образом. Как правило, имело место обращение прокурора в интересах Российской Федерации и неопределенного круга лиц с иском к оператору, оказывающему телематические услуги связи, с требованием об ограничении доступа к конкретному информацион-

[1] Поскольку распространение информации о даче взятки не является административным или уголовным правонарушением, запрещенным указанной нормой Закона об информации.

ному ресурсу, в том числе путем фильтрации указателей страниц или сетевых адресов. Именно в рамках рассмотрения дела по подобному требованию было вынесено упомянутое в начале Определение ВС РФ от 10.05.2011 № 58-Впр11-2, и в целом такая практика была достаточно распространенной[1].

Кроме того, требования такого рода заявляются прокурором лишь к одному из операторов телематических услуг связи[2]. Очевидно, что в условиях существования целого рынка услуг по предоставлению доступа в сеть Интернет решение об ограничении доступа к сайтам (например, путем «фильтрации» определенных указателей или сетевых адресов), адресованное лишь одному провайдеру, скорее будет отвечать цели увеличения количественных показателей органов прокуратуры по ограничению распространения вредоносной информации в Интернете, нежели цели реального запрета на распространение информации.

Пожалуй, единственный действительно позитивный эффект от судебного акта, обязывающего конкретного оператора ограничить доступ к сайту, может быть достигнут в случае, если в том же судебном акте информация будет признана запрещенной к распространению. Это позволит по меньшей мере требовать включения указателя (сетевого адреса) сайта в Единый реестр, после чего его блокировка уже в течение суток станет обязательной для всех операторов связи (п. 10 ст. 15.1 Закона об информации). По сути, в таком случае оператор связи будет выступать «*номинальным*» (или «*техническим*») ответчиком.

Дальнейшее развитие судебной практики пошло по пути рассмотрения требований о запрете распространения информации в рамках особого производства по установлению фактов, имеющих юридическое значение (п. 1 ч. 1 ст. 262 ГПК РФ).

В связи с этим следует обратить внимание на Определение ВС РФ от 09.06.2015 № 51-КГПР15-7, которым были отменены нижестоящие судебные постановления и признан ошибочным вывод судов о том, что при рассмотрении требования о признании информации запрещенной

[1] См., например, определения: Липецкого областного суда от 21.12.2011 по делу № 33-3505/2011; Кировского областного суда от 01.12.2011 по делу № 33-4167; кассационные определения Суда Ханты-Мансийского автономного округа – Югры от 15.11.2011 по делу № 33-5028 / 2011; Рязанского областного суда от 19.10.2011 № 33-2115.

[2] Справедливости ради стоит отметить, что в ряде случаев прокуроры обращаются с иском не к одному, а сразу к нескольким интернет-провайдерам: см., например: кассационное определение Белгородского областного суда от 22.12.2011 по делу № 33-4662; определение Самарского областного суда от 12.10.2011 № 33-10673.

имеет место спор о праве[1]. Верховный Суд РФ указал, что по такого рода делам юридически значимым обстоятельством является сам факт распространения в сети Интернет запрещенной информации.

Приведенное постановление было воспринято нижестоящими судами, и вслед за ним судебная практика сложилась аналогичным образом[2]. Суды в обоснование отсутствия спора о праве ссылаются на то, что признание тех или иных информационных материалов запрещенными для распространения означает констатацию того факта, что они нарушают запреты, установленные федеральным законодательством.

Безусловно, с точки зрения цели ограничения распространения вредной информации в Интернет быстрая и эффективная блокировка в большей степени может быть достигнута за счет использования механизма особого производства (в порядке гл. 28 ГПК РФ).

В то же время аргументы ВС РФ о том, что в таких делах нет спора о праве, трудно назвать безупречными.

Во-первых, исходя из содержания подп. 2 п. 5 ст. 15.1 Закона об информации блокируемая информация должна быть признана запрещенной для распространения в Российской Федерации. Иными словами, Закон говорит о том, что судом в первую очередь должна быть дана правовая квалификации информации[3], а не просто установлен факт ее распространения. Суду в таком деле необходимо признать, что существуют легальные основания для ограничения права на свободное распространение информации, закрепленное в ч. 4 ст. 29 Конституции РФ.

Во-вторых, ограничение доступа к информации и признание ее запрещенной непосредственным образом касаются распространителя сведений (например, администратора сайта). Кроме того, признание запрещенным того или иного произведения может затрагивать интересы правообладателя, например, в связи с дальнейшим отказом

[1] С этой позицией категорически не согласна М.А. Рожкова, считающая, что подобные дела не могут быть рассмотрены в порядке производства об установлении фактов, имеющих юридическое значение (см.: *Рожкова М.А.* О процессуальных нюансах рассмотрения дел о признании информации, размещенной на интернет-сайте, запрещенной к распространению // Комментарий судебной практики / под ред. К.Б. Ярошенко. Вып. 21. М.: Ин-т законодательства и сравнительного правоведения при Правительстве РФ, 2016. С. 76–83.

[2] См., например, апелляционные определения: Московского городского суда от 04.12.2015 по делу № 33-45526 / 2015, Новосибирского областного суда от 27.09.2016.

[3] К примеру, что распространение такой информации образует состав административного или уголовного правонарушения.

со стороны русскоязычных информационных ресурсов в размещении этой информации и соответствующим уменьшением рыночной стоимости исключительного права на такое произведение. В то же время указанные лица не имеют возможности участвовать в деле и заявлять свои доводы, если оно рассматривается в порядке производства по установлению фактов, имеющих юридическое значение.

В контексте критики рассмотрения споров в порядке особого производства представляет интерес достаточно резонансное дело № 33-13765/2016 о блокировке сайта YouPorn по требованию прокурора. Мотивом к отмене решения суда[1] в апелляционной инстанции[2] стало то, что иностранная компания – владелец домена *youporn.com* – не была привлечена к участию в деле в нарушение п. 4 ч. 4 ст. 330 ГПК РФ.

Тем не менее, признавая недопустимость рассмотрения дела «*YouPorn*» в особом производстве, суд пришел к удивительному выводу о том, что оно подлежит рассмотрению в соответствии с нормами КАС РФ. Апелляционный суд в определении[3] ссылается на то, что дела о признании информации, распространяемой посредством сети Интернет, запрещенной информацией относятся согласно «Иерархическому справочнику категорий гражданских дел и административных дел» к гл. 22 КАС РФ, а следовательно, заявленные прокурором требования должны рассматриваться в порядке указанной главы. С данным выводом суда трудно согласиться, учитывая, что гл. 22 КАС РФ регулирует случаи оспаривания действий (бездействия) и решений лиц, наделенных публичными полномочиями (ч. 1 ст. 218), а не споры о признании информации запрещенной.

Таким образом, получается, что в судебной практике отсутствует адекватный подход к определению порядка признания информации в сети Интернет запрещенной: ни использование номинального ответчика, ни особое производство, ни тем более производство в порядке гл. 22 КАС РФ не отвечают закону.

Обращение в суд с иском к не имеющему материально-правового интереса оператору связи или вообще обращение в порядке гл. 28 ГПК РФ, где не подразумевается наличие процессуального оппонента, безусловно, выгодно лицу, заинтересованному в блокировке сайта.

[1] Решение Первореченского районного суда г. Владивостока Приморского края от 09.2016 по делу № 2-2391/2016.

[2] См.: апелляционное определение Приморского краевого суда по делу от 17.01.2017 № 33-13765/2016 (280/2017).

[3] См. там же.

Однако в таком случае отправление правосудия происходит без участия тех, чьи права будут непосредственно затронуты судебным решением: в первую очередь речь идет о владельцах сайтов и администраторах доменных имен. Соответственно, подобные дела должны рассматриваться в порядке искового производства, где администратор домена/владелец сайта должен выступать ответчиком по делу. Безусловно, такой порядок сопряжен со сложностями практического толка, связанными с идентификацией владельца того или иного ресурса.

Вероятно, выходом из ситуации, который сбалансировал бы интересы лиц, чьи права затрагиваются противоправной информацией, и интересы распространителей такой информации, могло стать введение упрощенного порядка в отношении подобной категории дел. Преимуществами такого порядка должны были бы стать, с одной стороны, возможность быстрого вынесения решения суда в случае отсутствия информации о владельце сайта (администраторе домена) или связи с ним, а с другой – обеспечение таким лицам возможности в режиме «онлайн» отслеживать информацию о судебных процессах, касающихся их информационного ресурса. Что интересно, шаги по упрощению разбирательств о блокировке сайта уже предпринимаются. Например, Минкомсвязью России разрабатывается законопроект[1], позволяющий блокировать с помощью судебных приказов упоминавшиеся выше сайты-«зеркала» (копии сайтов), если они являются производными от сайтов, подвергшихся «пожизненной» блокировке.

Заключение

Следует крайне осторожно подходить к мерам по ограничению распространения в сети Интернет информации, которая по тем или иным причинам признается законодателем запрещенной.

В первую очередь нужно помнить о конституционном праве на свободное распространение информации, которое гарантировано ч. 4 ст. 29 Конституции РФ. Кроме того, блокировка тех или иных ресурсов нарушает целостность Интернета и тем самым вредит структуре глобальной сети. В связи с этим статистику блокировок и подходы к их применению можно без преувеличения назвать пугающими.

[1] См.: проект федерального закона «О внесении изменений в некоторые законодательные акты Российской Федерации» (ID 02/04/04-16/00048370) (http://regulation.gov.ru/projects#npa=48370).

Суды не склонны руководствоваться балансом интересов «блокиратора» и распространителя информации, вместо этого последний в большинстве случаев фактически лишается возможности участвовать в судебном процессе, где решается вопрос о том, будет доступен тот или иной информационный ресурс на территории России или нет.

Ситуация осложняется отсутствием единого и корректного подхода к процедуре рассмотрения дел о блокировке сайтов, а также использованием судами достаточно неосторожных и размытых формулировок (таких, как «подрыв морально-нравственных устоев» и т.п.) в обоснование блокировки сайтов, что не способствует повышению качества правосудия в данной области.

Представляется, что судейское усмотрение в вопросах признания информации запрещенной должно быть ограничено. В противном случае, если идти по пути расширительного толкования закона, можно оказаться в правовом поле, где легальность публичного распространения тех или иных сведений будет определяться в первую очередь мнением судьи, а не конкретными законодательными критериями.

Пристатейный библиографический список:

1. *Савельев А.И.* Комментарий к Федеральному закону от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и защите информации (постатейный)». М.: Статут, 2015.

2. Защита деловой репутации в случаях ее диффамации или неправомерного использования (в сфере коммерческих отношений): науч.-практ. пособие / М.А. Рожкова, Д.В. Афанасьев, М.Е. Глазкова и др.; под общ. ред. М.А. Рожковой. М.: Статут, 2015.

3. Enemies of the Internet 2014: entities at the heart of censorship and surveillance (URL: http://12mars.rsf.org/wp-content/uploads/EN_RAPPORT_INTERNET_BD.pdf).

4. Роскомсвобода. Статистика блокировок (URL: https://reestr.rublacklist.net/visual/).

Ю.С. Харитонова

КОНТЕКСТНАЯ (ПОВЕДЕНЧЕСКАЯ) РЕКЛАМА И ПРАВО: ТОЧКИ ПЕРЕСЕЧЕНИЯ

Аннотация. *Распространение информации, которая называется таргетированной, контекстной или поведенческой рекламой, сопряжено со сбором и анализом данных, позволяющих определить интересы, ценности, благосостояние субъекта. Ограничение понятия персональных данных субъекта и их содержания в российском правопорядке не позволяют защититься с помощью применения профильного закона. Для защиты прав лиц в случае посягательств на сбор, хранение и обработку данных о них целесообразно использовать применяемое в практике Конституционного Суда РФ понятие юридических интересов.*

Ключевые слова: *персональные данные, право на тайну частной жизни, защита персональных данных, частные интересы, реклама; контекстная реклама, волевые действия субъекта.*

Экономика быстро и неуклонно трансформируется в информационную. С каждым днем растет число экономических субъектов, осуществляющих свою деятельность в рамках виртуальной среды, что способствует расширению способов их взаимодействия с клиентами посредством технических устройств – персональных компьютеров, планшетов, смартфонов. На протяжении последних лет неизменно не теряет своей актуальности утверждение о том, что «XXI век – век знаний, наукоемких производств, высоких технологий и стремительных инноваций»[1].

И каждый пользователь неизменно сталкивается с необходимостью терпеть вторжение в его жизнь информации, которая называется таргетированной, или контекстной, рекламой. Контекстная реклама – это инструмент, «направленный на увеличение продаж и привлечение новых клиентов через Интернет. Контекстное объявление видят пользователи, которые ищут в Интернете то, что предлагает рекламодатель. Таким образом, рекламное сообщение воспринимается пользователем

[1] Россия XXI века. Образ желаемого завтра. М.: Экон-Информ, 2010. С. 14.

как ответ на заданный вопрос и помогает найти нужный ему товар или услугу. Даже если товар ищет всего один пользователь из миллиона, контекстная реклама позволяет показать предложение именно ему»[1], успокаивают нас рекламодатели.

С.Ю. Филиппова, давая обобщенное определение, указывает, что «контекстная реклама – способ размещения рекламы в сети Интернет путем демонстрации рекламного объявления при введении посетителем интернет-сайта поискового запроса с использованием определенных ключевых слов»[2].

Такими ключевыми словами являются слова запроса, в том числе того, который производился пользователем ранее, в том числе и по другому поводу, нежели тот, что заставил его обратиться к соответствующему ресурсу. В судебной практике указывается: «...контекстная реклама представляет собой вид размещения интернет-рекламы, в основе которой лежит принцип соответствия появления рекламного материала в зависимости от контекста (содержания) просматриваемой пользователем интернет-страницы. Данный вид рекламы является наиболее эффективным с точки зрения продвижения товара, так как избирательно отображается посетителям интернет-страницы – потенциальным покупателям (целевой аудитории рекламируемого объекта)»[3].

Продвижение товаров и услуг строится на подборе и анализе данных запросов, которые делает пользователь сети Интернет по различным вопросам[4]. Причем сейчас учитываются не только поиски какого-то конкретного товара для предложения его аналога или магазина, где можно приобрести такой продукт, но и данные иных запросов, позволяющие, например, оценить кредитоспособность пользователя Интернета, его склонность к получению кредитных средств, возможности возврата заемных средств и склонности к умышленному уклонению от исполнения принятых договорных обязательств[5]. По истории оценок пользователя просмотренным кинолентам можно, проанализировав

[1] Определение Яндекс (https://advertising.yandex.ru/context/).

[2] Настольная книга руководителя организации: правовые основы / отв. ред. И.С. Шиткина. М.: Юстицинформ, 2015.

[3] Постановление Девятого ААС от 13.06.2012 № 09АП-14264/2012-АК по делу № А40-112441/11-90-469.

[4] *Бабаев А., Евдокимов Н., Иванов А.* Контекстная реклама. СПб., 2011.

[5] См., например: *Афанасьев Д., Гладько А., Семенихин В.* Банкам нужны данные. Большие и маленькие // Банковское обозрение. 2016. № 1. С. 72–77.

их в совокупности, составить прогноз и порекомендовать зрителю тот фильм, который ему понравится и который он купит у рекламодателя. Недаром еще одним названием контекстной рекламы является – «поведенческая».

Поведенческая реклама – это контекстная реклама с привязкой к конкретным интересам пользователя. В руководствах для маркетологов указывается: «К примеру, посетитель ищет в поисковике ноутбук, посещает сайты магазинов компьютерной техники, читает различные форумы, сравнивает характеристики моделей ноутбуков. Вся эта информация передается системам контекстной рекламы и на основе интересов пользователя выдается соответствующая реклама на других сайтах, которые посетит данный человек. Поэтому так и получается, что пользователь, искавший ноутбуки, на сайте о рыбках, увидит рекламу ноутбуков, а не морских животных. Таким образом, владельцы не столь популярных тем, смогут немного повысить свой доход от рекламы, за счет поведенческого фактора, который присутствует в каждой современной системе контекстной рекламы»[1].

Российские суды пока весьма формально оценивают характеристики контекстной рекламы. В одном из судебных решений указывалось, что истец не представил доказательств нарушения ответчиком его прав, ведь «наличие контекстной рекламы на поисковой странице сайта http://www.yandex.ru/ является результатом работы поисковой системы, которая с помощью контекста и ключевых слов осуществляет автоматическую привязку запроса пользователя с выдаваемыми на странице результатами, ключевые слова никак не связаны с рекламной ссылкой, они являются техническим параметром, не представляя собой часть рекламного объявления»[2]. В связи с этим не было признано нарушение права истца на товарный знак в смысле ст. 1484 ГК РФ. По логике судебной инстанции, следовательно, подбор и предоставление реклам пользователю вообще может выпадать из правового поля, раз оно носит технический характер.

В другом случае истец, ссылаясь на оказание ответчиком рекламных услуг ненадлежащим образом, потребовал вернуть перечисленную ответчику сумму предварительной оплаты. Однако в удовлетворении требования было отказано, поскольку надлежащее исполнение ответчиком услуг, по мнению суда, было доказано, услуги приняты истцом,

[1] http://www.kursidvd.ru/povedencheskaya-reklama/

[2] Постановление Двенадцатого ААС от 20.06.2012 по делу № А12-1125/2012.

правом на отказ от договора истец не воспользовался[1]. При этом суды двух инстанций отклонили доводы истца о том, что использование ответчиком технологии поведенческого таргетинга (показ рекламных объявлений пользователям, выделенным на основании их предшествующего поведения) не позволило учесть интересы пользователей, который хотя и осуществлялся автоматически, не в полной мере соответствовал тематике объявлений, интересам пользователя.

Однако нельзя сводить всю операцию размещения такого рода рекламы к технической стороне дела. Основной целью контекстной рекламы является немедленная продажа товара или услуги. Но это далеко не единственная цель, которую ставят перед собой маркетологи. Данный инструмент позволяет также добиться реализации таких целей, как увеличение количества пользователей на сайте; повышение узнаваемости бренда; напоминание пользователям о существовании своей организации; выход на уровень рентабельности; максимизация прибыли; информирование пользователей о новом товаре или услуге; быстрая продажа товара с ограниченным спросом и др.[2] Все эти цели можно объединить в одну – заставить пользователя совершить желаемое рекламодателем целевое действие. Тем самым рекламодатель стремится воздействовать на поведение потребителя, участвовать в формировании его воли.

В судебных актах встречаются повторения того, что известно из разработанных крупнейшими операторами и рекламодателями в отношении контекстной рекламы.

Так, в одном из судебных актов указывается: «...основным содержанием принципов поисковой, контекстной рекламы является то, что рекламное объявление показывается пользователю, если текстовый запрос, введенный им в строку поиска поисковой системы, содержит слово/словосочетание, заранее включенное рекламодателем (при заказе рекламной кампании) в перечень ключевых слов/словосочетаний (критериев для показа рекламного объявления), либо если содержание веб-страницы, которую просматривает пользователь, соответствует тематике рекламного объявления, определяемой ключевыми словами/словосочетаниями»[3]. В другом можно прочесть: «Сервис «Яндекс.

[1] Постановление АС Московского округа от 30.12.2014 № Ф05-13500/2014 по делу № А40-107924/13-135–985.

[2] См.: Контекстная реклама в Интернете. Настольная книга рекламиста. СПб., 2011.

[3] Постановление Шестнадцатого ААС от 24.02.2016 № 16АП-5540/2015 по делу № А63-6586/2015.

Директ» оказывает услуги по размещению рекламы рекламодателя в сети Интернет по принципам поисковой, контекстной рекламы в соответствии с условиями оферты. Согласно п. 1.1 оферты контекстная реклама – принцип показа рекламы на рекламных местах, согласно которому показ рекламного объявления осуществляется при условии наличия автоматически установленного Яндексом потенциального соответствия тематики (контекста) веб-страницы, на которой показывается рекламное объявление, и/или соответствие интересов пользователя, которому показывается рекламное объявление, тематике такого рекламного объявления, определяемой по совокупности ключевых слов-словосочетаний, указанных рекламодателем в соответствующей рекламной кампании в качестве критерия показа для данного рекламного объявления, или иным способом»[1].

В подавляющем большинстве споров, рассмотренных судами в данной сфере, участвуют предприниматели, заказывающие размещение рекламы либо проведение анализа рынка, а не конечные потребители рекламной информации. В то же время достаточного регулирования поведенческой рекламы в современном законодательстве просто нет.

Юрист в применении таких инструментов рекламирования и продвижения товара сразу увидит множество проблем. Прежде всего необходимо определить применимость к данным отношениям механизма защиты персональных данных. Согласно действующему российскому законодательству сбор и анализ, а также хранение данных о пользователях тех или иных ресурсов подпадают под ограничения, закрепленные в Законе о персональных данных.

Согласно Закону о персональных данных любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации, в том числе в информационно-телекоммуникационных сетях с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных юридическими лицами и физическими лицами, должны осуществляться на законной и справедливой основе. В том числе с учетом гарантий соблюдения прав человека на неприкосновенность частной жизни, личную и семейную тайну.

[1] Постановление АС Московского округа от 30.12.2014 № Ф05-13500/2014 по делу № А40-107924/13-135-985.

В частности, к персональным данным, доступ к которым третьих лиц ограничен, относят не только дату рождения и адрес регистрации, но и сведения о заработной плате[1] лица, а также о принадлежащей ему недвижимости, ее характеристиках и границах[2] и т.д. Недопустимо также раскрытие такого нестоимостного критерия при закупках, как «Квалификация участников закупки», путем требования представления копий трудовых договоров, трудовых книжек работников, приказов о приеме на работу, а также копий дипломов о профессиональном образовании работников, поскольку эти данные также являются персональными и не могут быть предоставлены третьим лицам без согласия субъектов данных[3].

При достаточно обширной практике применения названного законодательного акта можно сделать вывод, что притязание на защиту персональных данных в случае с поведенческой рекламой не работает.

Заложенный в Законе подход к защите персональных данных сегодня не учитывает реалий и тенденций развития технологий. Одним из трендов индустрии продвижения стала оценка управления доходностью с помощью контекстной рекламы и анализа *Big Data*. Например, предлагается решать проблему оценки заемщиков МФО с помощью анализа (с учетом сложности процесса и необходимостью использования специальных формул, большого количества переменных и при высокой производительности *IT*-систем) 7 тыс. переменных, созданных с учетом специфики заемщика МФО и контекста его активности получить достоверный ответ на вопрос: «Вернет ли заемщик сумму займа с доходностью 120% с просрочкой до 45 дней?»[4]. Психологи считают, что «на высших уровнях своего проявления воля предполагает опору на духовные цели и нравственные ценности, на убеждения и идеалы»[5]. Исследование запросов пользователя позволяет определять характеристики его личности и поведения в конкретный период вре-

[1] Письмо Роскомнадзора от 07.02.2014 № 08КМ-3681 «О передаче работодателем третьим лицам сведений о заработной плате работников».

[2] Письмо ФГБУ «ФКП Росреестра» от 05.05.2014 № 11-1635-КЛ «О направлении информации» (вместе с письмом Росреестра от 23.04.2014 № 14-05499/14 «О предоставлении информации»).

[3] Решение Алтайского краевого УФАС России от 24.06.2014 по делу № 295/14.

[4] *Ференец В.* Big Data как управление стоимостью привлечения клиента // https://bosfera.ru/event_report/big-data-kak-upravlenie-stoimostyu-privlecheniya-klienta. Обзор сообщений участников конференции: «BIG DATA: банки, финансовые компании, e-commerce, телекомы. Практические кейсы от лидеров индустрии» (14.04.2016).

[5] *Немов Р.С.* Психология. Т. 1. М., 2003. С. 424.

мени, а также в определенной перспективе. В то же время эти «высоты» стали доступны для покорения именно в связи с возможностями получить те самые 7 тыс. переменных, которые характеризуют клиента МФО и контекст его активности.

В данном случае встает вопрос о поисках баланса между возможностями ограничить законом доступ к личным данным и свободой предпринимательской деятельности, предпринимательской активности. На самом высшем уровне в России неоднократно указывалось, что «свобода для развития в экономике, социальной сфере, в гражданских инициативах – это лучший ответ как на внешние ограничения, так и на наши внутренние проблемы»[1]. В данном контексте продвижение и сбыт товаров и услуг имеет важное значение.

Напомним, что согласно Закону о персональных данных к последним относят любую информацию, относящуюся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных). В процессе обработки информации о запросах пользователя возможно получение информации о запросах, поступающих как от определяемого лица (зарегистрированного на сайте, предоставившего свои данные при регистрации), так и из оперативной памяти компьютера.

В первом случае идентификация пользователя происходит при его регистрации на сайте. Как представляется, регистрация и заключение пользовательского соглашения давно позволяют решить вопросы с получением разрешения на обработку персональных данных в практически любом объеме. Решающее значение в таких случаях будет иметь выверенное определение необходимой для обработки информации, ее объем и иные характеристики.

Так, на сайте *HeadHunter.ru* в «Политике обработки персональных данных в ООО «Хедхантэр»»[2] определен круг информации, которую собирают, объем действий, которые совершают с этой информацией, и, соответственно, определены цели, ради которых все это делается, что позволяет соблюсти требования законодательства о защите персональных данных. На сайте компании *Mercedes-Benz* в России в разделе «Защита данных» указано: «При посещении сайтов *Daimler AG* наши сетевые серверы стандартно регистрируют *IP*-адрес, присвоенный Вам

[1] Послание Президента РФ Федеральному Собранию от 04.12.2014 (URL: http://www.kremlin.ru/news/47173).

[2] https://hh.ru/article/1365

Вашим провайдером интернет-услуг, название страницы, с которой Вы к нам пришли, названия страниц, которые Вы посещаете у нас, а также дату и продолжительность Вашего посещения. Персональные данные сохраняются лишь при условии указания их Вами, например, в рамках регистрации, анкетирования, призового конкурса или в целях осуществления договора»[1].

Как представляется, анализ данных, позволяющих ответить на вопросы о возврате долгов или склонности к получению кредитных средств, не укладывается в рамки традиционных политик обработки персональных данных и далеко не всегда связан с получением согласия пользователя на обработку запросов с его устройства в отсутствие согласия, выраженного при регистрации. В этом случае определить конкретного пользователя, отправившего запрос с персонального устройства, затруднительно. Такая информация, как правило, даже не связывается с *IP*-адресом пользовательского устройства. Можно ли в такой ситуации говорить о том, что происходит сбор информации об определимом лице в контексте Закона о персональных данных? Думается, вряд ли.

Полагаем, поиск с определенного устройства путевки на море или валенок не подпадает под понятие персональных данных, хотя этот термин и получил достаточно широкое применение. В то же время анализ ценовой категории поиска, направления поездки и времени отпуска, количества отдыхающих позволяет вполне определенно составить представление о пользователе.

В связи с этим интерес представляет возможность установления взаимосвязи поведения лица и границ защиты тайны частной жизни, предоставляемой на основании публичных норм, а также такой его составляющей, как право на тайну переписки.

В известном деле ООО «Гугл» это вопрос рассматривался довольно подробно. Гражданин обратился в суд с иском к ООО «Гугл» и просил запретить ответчику чтение его личной корреспонденции и взыскать с ответчика компенсацию морального вреда. В обоснование своих требований истец указал, что является пользователем электронного почтового ящика с адресом «****@gmail.com», при прочтении своей личной переписки 21.02.2014 обнаружил, что рекламные объявления, встроенные в текст письма, соответствуют содержанию текста элек-

[1] http://www.mercedes-benz.ru/content/russia/mpc/mpc_russia_website/ru/home_mpc/privacy_statement.html

тронной переписки истца, что нарушает его конституционное право на личную тайну, тайну переписки.

Истец полагал, что действия ответчика по сканированию личной переписки и размещению на основании данной переписки рекламы являются неправомерными, нарушают права истца. ООО «Гугл», осуществляя рекламную деятельность и оказывая услуги по продаже рекламных мест на сайтах, размещению рекламных объявлений на основании заключенных договоров, не считало себя надлежащим ответчиком, поэтому суд первой инстанции ошибочно отклонил иск[1].

Вышестоящим судом было установлено, что сервис бесплатной электронной почты *Gmail* предоставляется американской компанией на основании соглашения – Условий использования продукта *Google*. Головной американской компанией в России было зарегистрировано ООО «Гугл», которое при стопроцентном участии материнской компании в уставном капитале использует логотип продукта *Google*, а также технический инструментарий, к которому в том числе относится программное обеспечение, принадлежащие головной компании, и т.д.

При рассмотрении дела также были учтены условия политики конфиденциальности продукта *Google*: «...системы автоматически анализируют ваш контент (в том числе электронные письма), чтобы предоставлять функции, полезные вам. Это могут быть отобранные для вас результаты поиска, релевантные рекламные объявления, выявление спама и вредоносных программ...».

Исходя из изложенного судебная коллегия пришла к выводу, что ответчик ООО «Гугл» при исполнении обязательств перед третьими лицами по договорам размещения рекламы и ее эффективного распространения в своем сегменте продукта *Google* проводит мониторинг, в том числе электронных писем, и осуществляет размещение данных рекламных сообщений, в том числе и в частной переписке пользователей Российской Федерации, воспользовавшихся продуктом *Google* на основании результатов мониторинга конкретного пользователя продукта.

Суд указал, что на основании ст. 23 Конституции РФ каждому гражданину гарантируется тайна переписки и другой корреспонденции, поэтому мониторинг электронной корреспонденции может быть расценен как посягательство на конституционные права граждан.

[1] Решение Замоскворецкого районного суда г. Москвы от 21.04.2015.

Таким образом, судебная коллегия пришла к выводу, что ответчик, размещая рекламу в сообщении истца, руководствовался результатами мониторинга электронной корреспонденции истца, тем самым нарушил тайну его переписки. Суд вынес решение об удовлетворении требований истца, в том числе запретить ООО «Гугл» чтение личной корреспонденции гражданина[1].

В приведенном примере, рассмотренном в российской юрисдикции, речь шла об использовании данных лица, состоящих в выраженных письменно интересах, не в связи с защитой персональных данных, а именно в связи с защитой конституционного права на тайну переписки. Однако практика в данной сфере только складывается, выявляются различного рода нюансы, имеющие значение для защиты прав граждан в рассматриваемой сфере. В частности, иногда суды полагают, что оператор связи не имеет права ознакомиться с содержанием SMS-отправлений и вмешиваться в их распространение. А раз так, то оператор как поставщик услуг связи, который только обеспечил подключение к сети электросвязи и не осуществляет непосредственно распространение рекламы, рекламораспространителем не является[2].

Следует отметить, что в зарубежном законодательстве право на защиту персональных данных трактуется шире, чем в России. Так, согласно ст. 2 Директивы ЕС № 95/46/ЕС[3] «персональные данные» определены как любая информация, относящаяся к определенному или определяемому физическому лицу («субъекту данных»); определяемым является лицо, которое может быть определено, прямо или косвенно, в частности, через идентификационный номер либо через один или несколько признаков». Важным представляется указание в Директиве на то, что это могут быть признаки, характерные для физической, психологической, умственной, экономической, культурной или социальной идентичности лица.

---

[1] Апелляционное определение Московского городского суда от 16.09.2015 по делу № 33-30344/2015.

[2] *Евстратова Л.А.* О тарифах, расчетах и рекламе // Услуги связи: бухгалтерский учет и налогообложение. 2014. № 5. С. 70–78.

[3] Директива № 95/46/ЕС Европейского парламента и Совета Европейского союза «О защите физических лиц при обработке персональных данных и о свободном обращении таких данных» [рус., англ.] (Принята в г. Люксембурге 24.10.1995) (с изм. и доп. от 29.09.2003) (Документ утрачивает силу 24.05.2018 в соответствии с Регламентом № 2016/679 Европейского парламента и Совета Европейского союза от 27.04.2016 (официальный сайт законодательства Европейского союза: http://eur-lex.europa.eu/ (по состоянию на 19.12.2016)).

В названной Директиве также подчеркнуто, что «для определения того, является ли лицо идентифицируемым, следует принимать в расчет все средства, в равной мере могущие быть вероятно и разумно использованными либо оператором, либо любым иным лицом для идентификации указанного лица» (п. 26 Преамбулы).

Опираясь на зарубежные исследования в данной сфере, А.И. Савельев показывает: «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»[1].

В то же время отмечается[2], что в европейской практике права субъекта данных в соответствии со ст. 7 и 8 Хартии Европейского союза об основных правах[3] на уважение личной жизни и защиту персональных данных обычно перевешивают экономический интерес оператора поисковой системы и интерес общественности в доступе к информации через поиск, хотя может возникнуть исключение, если интерес в доступе преобладает, например, в связи с ролью, которую играет субъект данных в общественной жизни.

Российское законодательство пока не предполагает такого широкого охвата данных, которые могут быть отнесены к персональным. В то же время можно было бы рассматривать возможности защиты прав на тайну частной жизни как базу для расширения охраны личного информационного пространства лица.

В США в настоящий момент активно действуют принципы такой организации, как *Advertising Initiative* (*NAI* сети, Сеть рекламной инициативы), и «Саморегулятивный кодекс по использованию поведенческой онлайн-рекламы». Данная организация направляет свои усилия на принятие добровольных норм поведения, касающихся рекламной деятельности. В частности? они объявили, что собираются начать

---

[1] *Савельев А.И.* Электронная коммерция в России и за рубежом: правовое регулирование. М.: Статут, 2016.

[2] Компании «Гугл Спейн СЛ» и «Гугл Инк.» против Испанского агентства по защите данных (AEPD) и Марио Костехи Гонсалеса // Бюллетень Европейского Суда по правам человека. Российское издание. 2014. № 9. С. 22–23.

[3] Хартия Европейского союза об основных правах (2007/C 303/01) [рус., англ.] (Вместе с «Разъяснениями...» (2007/C 303/02)) (Принята в г. Страсбурге 12.12.2007).

продвигать программу *Advertising Option Icon*, которая позволит пользователям узнать, какие сайты принимают участие в поведенческом отслеживании. Это даст возможность пользователям отказываться от любой направленной рекламной деятельности, если это для них имеет значение[1].

В аналогичном ключе развивается и европейское законодательство: 27.04.2016 был принят общеевропейский Регламент о защите персональных данных (*General Data Protection Regulation*), в соответствии со ст. 3 которого его положения применяются к обработке персональных данных, осуществляемой подразделением оператора или «обработчика» на территории ЕС. В рамках данного документа профилирование пользователей станет возможным только с их согласия, например, при заключении договора.

В отсутствие подобных разработок в российском правопорядке представляется допустимым обратиться к возможностям защиты законного интереса гражданина. Проблема регулирования управления волей индивида заключается в том, что сама по себе воля вне действия не является самостоятельным юридическим фактом, а представляет собой юридически значимое обстоятельство. В то же время, как указывает О.М. Родионова, «воля, будучи элементом деятельности, не может противоречить ее цели и социальному назначению»[2].

Притязание на защиту персональных данных выступает элементом конституционного права на неприкосновенность частной жизни. Понимание понятия «частная жизнь» позволяет включить в него различные аспекты жизнедеятельности, связанные с личностным развитием человека в обществе, не ограничиваясь только теми, которые относятся к неформальной сфере. Но требуется выработать критерии отнесения тех или иных событий к частной жизни лица. В этом может помочь практика Европейского суда по правам человека.

В практике ЕСПЧ понятие частной жизни толкуется расширительно: она не исчерпывается так называемым внутренним кругом[3], в котором лицо может жить своей личной жизнью по своему усмотрению, полностью исключая внешний мир, не входящий в данный круг, но включает аспекты «внешнего мира», социальной сферы, в которой

[1] URL: http://www.itsec.ru/newstext.php?news_id=78838#sthash.J0ldkLYv.dpuf

[2] *Родионова О.М.* Правовые формы реализации волевых отношений в механизме гражданско-правового регулирования: дис. ... д-ра юрид. наук. М., 2017. С. 193.

[3] Постановление ЕСПЧ от 04.12.2008 по делу «Марпер против Соединенного Королевства».

субъект права «налаживает и развивает отношения с другими людьми и внешним миром»[1] и подразумевает наполнение смыслом самой личности в процессе жизнедеятельности. Тем самым данным понятием охватывается целый ряд разноплановых элементов жизнедеятельности и сознания человека.

А.А. Рождественский писал, что «могут существовать юридически защищаемые интересы, не будучи в то же время юридически индивидуализированными сферами интересов, т.е. не будучи субъективными правами»[2]. Г.А. Гаджиев высказал мнение о том, что позитивно не закрепленные в конституционном тексте интересы чаще всего получают свое оформление в судебном порядке[3]. Однако, как было показано выше, в России пока такая практика не сложилась. Для защиты прав граждан может использоваться применяемое в практике КС РФ понятие юридических интересов.

Такой подход позволит развивать российское законодательство в русле новейших тенденций. Признавая за любым лицом право на неприкосновенность частной жизни, ограничивая возможности по обработке данных о нем получением согласия субъекта данных, мы сможем учесть и в случае нарушения защищать такую сферу интересов гражданина, даже если она неопределима пока на основании законодательства как самостоятельное субъективное право.

Пристатейный библиографический список:

1. *Афанасьев Д., Гладько А., Семенихин В.* Банкам нужны данные. Большие и маленькие // Банковское обозрение. 2016. № 1.

2. *Бабаев А., Евдокимов Н., Иванов А.* Контекстная реклама. СПб., 2011.

3. *Гаджиев Г.А.* Конституционные принципы рыночной экономики (Развитие основ гражданского права в решениях Конституционного Суда Российской Федерации). М.: Юристъ, 2002.

[1] Постановление ЕСПЧ от 21.06.2011 по делу «Шимоволос (Shimovolos) против России» (жалоба № 30194/09).

[2] *Рождественский А.А.* Теория субъективных публичных прав. М.: Печ. А.И. Снегиревой, 1913. С. 26–27.

[3] См.: *Гаджиев Г.А.* Конституционные принципы рыночной экономики (Развитие основ гражданского права в решениях Конституционного Суда Российской Федерации). М.: Юристъ, 2002. С. 145.

4. *Евстратова Л.А.* О тарифах, расчетах и рекламе // Услуги связи: бухгалтерский учет и налогообложение. 2014. № 5.

5. Контекстная реклама в Интернете. Настольная книга рекламиста. СПб., 2011.

6. Настольная книга руководителя организации: правовые основы / отв. ред. И.С. Шиткина. М.: Юстицинформ, 2015.

7. *Немов Р.С.* Психология. Т. 1. М., 2003.

8. *Родионова О.М.* Правовые формы реализации волевых отношений в механизме гражданско-правового регулирования: дис. ... д-ра юрид. наук. М., 2017.

9. *Рождественский А.А.* Теория субъективных публичных прав. М.: Печ. А.И. Снегиревой, 1913.

10. Россия XXI века. Образ желаемого завтра. М.: Экон-Информ, 2010.

11. *Савельев А.И.* Электронная коммерция в России и за рубежом: правовое регулирование. 2-е изд. М.: Статут, 2016.

12. *Ференец В.* Big Data как управление стоимостью привлечения клиента (https://bosfera.ru/event_report/big-data-kak-upravlenie-stoimostyu-privlecheniya-klienta). Обзор сообщений участников конференции: «BIG DATA: банки, финансовые компании, e-commerce, телекомы. Практические кейсы от лидеров индустрии» (14.04.2016).

М.Ю. Козлова

ТРЕБОВАНИЯ К РЕКЛАМЕ В СЕТИ ИНТЕРНЕТ

Аннотация. *В статье исследуется влияние особенностей сети Интернет на распространение и восприятие рекламной информации. Реклама, распространяемая посредством сети Интернет, должна быть добросовестной и достоверной, она не должна нарушать права и законные интересы как потребителей, так и конкурентов лица, рекламирующего свои товары и услуги. Реклама, распространяемая в сети Интернет, доступна круглосуточно и, как правило, с территории любой страны. Рекламная информация может быть просмотрена неоднократно, если возникает такая необходимость. Потребитель в большинстве случаев не может контролировать наличие рекламы. Интернет-сайты могут достаточно легко менять свое содержание, поэтому процесс доказывания размещения ненадлежащей рекламы может быть затруднен. Таким образом, сеть Интернет как средство, с помощью которого распространяется реклама, обладает объективно существующими особенностями, которые влияют на специфику восприятия, распространения, воспроизведения, поиска и удаления информации. Эти особенности должны учитываться как законодателем, так и правоприменителем в целях недопущения распространения ненадлежащей рекламы.*

Ключевые слова: *реклама, сеть Интернет, контекстная реклама, ненадлежащая реклама, спам, Product Placement, скрытая реклама.*

Информация, представляющая собой рекламу, может быть распространена любым способом, при этом адресат ее конкретно не определяется. Цель рекламы – привлечь внимание к объекту рекламирования, сформировать или поддержать интерес к нему, а также обеспечить продвижение на рынке.

Как в законодательстве других стран, так и в доктрине для определения сущности рекламы используются термины «информация» и «сведения». Так, авторы комментария к ФЗ от 13.03.2006 № 38-ФЗ «О рекламе» (далее – Закон о рекламе) считают, что реклама – это сведения о товаре, услуге, их свойствах, производителе, продавце таких товаров, их местоположении, реквизитах, товарных знаках и фирмен-

ных наименованиях и видах деятельности, а также об иных объектах, в продвижении которых заинтересован участник рекламного рынка[1].

В Международном кодексе рекламной практики используется словосочетание «рекламное послание», которое употребляется в самом широком смысле, включающем любую форму рекламного послания относительно изделий, услуг и благ, независимо от вида СМИ, которое используется, в том числе рекламные надписи и изображения на упаковках, этикетках[2].

Учитывая, что Интернет именуется в российских нормативных актах как «информационно-телекоммуникационная сеть» и определяется как технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники[3], реклама может распространяться и в Интернете.

Возникает закономерный вопрос о том, обладает ли информация, распространяемая в Интернете, или сама сеть Интернет такими свойствами, которые приводят к необходимости особым образом регулировать отношения, связанные с распространением рекламы в Интернете.

Представляется, что сама по себе информация рекламного характера, размещаемая в сети Интернет, не обладает какой-либо спецификой, требующей особого подхода к регулированию. Однако имеются особенности в ее доступности, возможностях передачи, восприятия и удаления. Эти особенности должны учитываться как законодательством, так и судебной практикой. Реклама, распространяемая любыми способами, в том числе посредством сети Интернет, должна быть добросовестной и достоверной, она не должна нарушать права и законные интересы как потребителей, так и конкурентов лица, рекламирующего свои товары и услуги.

В рекламе, размещенной в сети Интернет, могут быть использованы средства, недоступные при передаче информации иными способами, и данное обстоятельство может иметь существенное значение для рассмотрения юридического конфликта.

---

[1] Постатейный комментарий к Федеральному закону «О рекламе» / Д.С. Бадалов, И.И. Василенкова, Н.Н. Карташов и др. М.: Статут, 2012.

[2] Международный кодекс рекламной практики. Публикация Международной торговой палаты в Париже. Июнь 1987 г.

[3] См.: постановление Правительства РФ от 10.09.2007 № 575 «Об утверждении Правил оказания телематических услуг связи».

Так, ООО (истец), являющееся застройщиком жилого комплекса «Оазис» в Новосибирске, обнаружило, что при введении в поисковую строку системы *Google* слов «жилой комплекс оазис Новосибирск» поисковый механизм отображает список рекламных ссылок, в котором на первом месте стоит ссылка с заголовком: «Ищете квартиры в ЖК Оазис? – www.gorod-v-gorode.ru», которая отсылает пользователя на страницу сайта, содержащего информацию о жилом комплексе «Премьер», застройщиком которого является другое ООО (ответчик).

То есть обозначение, применяемое в предпринимательской деятельности одного юридического лица, было использовано в рекламе другого, вследствие чего имело место паразитирование одного юридического лица на деловой репутации другого. Причем осуществлено это действие было средствами, характерными для сети Интернет.

Суд признал, что таким образом за счет использования наименования строящегося истцом объекта недвижимости – ЖК «Оазис» – привлекается внимание к сайту ответчика, причем реклама создает впечатление, что к продаже предлагаются квартиры в ЖК «Оазис», что вводит в заблуждение потребителя рекламы. С учетом этого реклама была признана недостоверной антимонопольным органом, и этот вывод в дальнейшем был подтвержден судами[1].

В сети Интернет используется так называемая контекстная реклама. Контекстная реклама – это разновидность рекламной информации, которая демонстрируется пользователю в соответствии с его поисковыми запросами. Показ базируется на анализе ключевых слов, которые указываются рекламодателями при размещении рекламы[2] в таких поисковых системах, как Яндекс, *Google* т.д.

Указание ключевых слов, даже если эти слова вместе или по отдельности представляют собой фирменное наименование юридического лица или элемент товарного знака, не рассматривается в качестве нарушения интеллектуальной собственности. Ключевые слова, используемые для рекламного объявления одного лица, не могут рассматриваться как обозначения, которые создают угрозу смешения с товарным знаком или фирменным наименованием другого лица. Использование слов, которые являются элементом товарного знака,

[1] Постановление Седьмого ААС от 24.11.2015 по делу № А45-12842/2015 (https://kad.arbitr.ru/Card/f089fa6c-0e2e-46da-a9cd-84e23223be9a (дата обращения: 07.03.2017)).

[2] При размещении рекламы рекламодатель определяет, по каким ключевым словам пользователю должно выдаваться рекламное объявление.

не рассматривается как использование товарного знака и поэтому не нарушает исключительное право правообладателя.

Такие выводы подтверждаются судебной практикой.

В частности, в одном из дел суд указал, что ключевое слово не обладает индивидуализирующей способностью даже в отношении конкретного рекламного объявления, так как на основании ключевого слова невозможно выделить конкретное объявление из всех существующих[1].

В другом деле истец требовал от ООО «Гугл» пресечь действия, нарушающие исключительное право на товарный знак, выразившиеся в размещении рекламных объявлений в системе *Google AdWords*, которые демонстрируются пользователю после введения им ключевых слов, являющихся элементом товарного знака истца. Суд усмотрел в действиях истца признаки нарушения прав других лиц на доступ к информации. В обоснование своей позиции суд указал, что поисковый сервис *Google* ориентирован на свободный доступ пользователей к информации, релевантной словам, по которым пользователи осуществляют поиск. Требование истца о запрете использования вошедших во всеобщее употребление для обозначения товаров определенного вида слов, являющихся элементом товарного знака истца, при проведении рекламных кампаний пользователями программы ответчика де-факто представляет собой ограничение доступа определенного круга интернет-пользователей (осуществляющих поиск по этим словам) к информации, в том числе к информации о конкурентах истца и предлагаемых ими товарах и услугах в аналогичной сфере деятельности[2].

Рекламные материалы, размещенные в сети Интернет, безусловно, должны соответствовать требованиям, предъявляемым Законом о рекламе. Причем должны учитываться также особенности восприятия этих рекламных объявлений потребителем и возможность использования тех средств, которые недоступны при других способах размещения.

Так, антимонопольным органом была признана ненадлежащей реклама банковских продуктов, размещенная на сайте «Бизнес-газеты», в связи с тем, что существенная информация об услугах была выполнена мелким нечитаемым шрифтом.

---

[1] Постановление Суда по интеллектуальным правам от 19.11.2013 № С01-202/2013 по делу № А40-159412/2012 (https://kad.arbitr.ru/Card/1f82b49e-b4b1-451e-96c1-be039da8afa1 (дата обращения: 07.03.2017)).

[2] Решение АС г. Москвы от 31.01.2014 по делу № А40-145068/13 (https://kad.arbitr.ru/Card/e81e1868-c485-46c1-84c4-d987b365af46 (дата обращения: 07.03.2017)).

Суды при рассмотрении заявления об оспаривании этого решения антимонопольного органа пришли к следующим выводам. В соответствии с общими правилами пользования Интернетом и технологиями переходов между web-страницами по принципу «от общего к частному» для получения любой дальнейшей информации надо навести указатель мыши на гиперссылки и инициировать переход с одного читаемого указателя (гиперссылка) на подстраницу с приложением путем нажатия (левого клика мыши) на любой участок исследуемого указателя. При этом способ размещения информации позволяет просматривать анимационные баннеры неоднократно, без ограничения количества просмотров. Кроме того, при желании возможно увеличить текст на экране компьютера до любого размера шрифта. Исходя из сказанного суд сделал вывод, что потребитель интернет-рекламы при просмотре объявлений в полном объеме автоматически получает из него всю необходимую информацию по соответствующим финансовым услугам и их получению[1].

Возможности сети Интернет порождают и новые недобросовестные методы, с помощью которых может распространяться нежелательная информация рекламного характера. В первую очередь речь идет о спаме.

Спам как нежелательное сообщение может быть различных видов: данное сообщение может носить характер коммерческого предложения, иметь целью совершение мошенничества, может направляться исключительно из хулиганских побуждений. Рассылка спама коммерческого содержания без получения согласия абонента может быть оценена как недобросовестная конкуренция, а также как действие, нарушающее Закон о рекламе.

Законодательство, в той или иной степени направленное на ограничение рассылки и получение спама, имеется в различных странах. Цель такого рода нормативных актов – ограничение возможностей массовой рассылки по случайным адресам с использованием автоматических средств (роботов), создание условий рассылки исключительно на основании предварительно полученного согласия получателя сообщений, а также установление административной и гражданско-правовой ответственности за нарушение правил.

[1] Постановление Одиннадцатого ААС от 03 апреля 2013 г. по делу № А65-27882/2012 (https://kad.arbitr.ru/Card/5101d0e1-6d42-4830-a037-b02d31ee523e (дата обращения: 12.03.2017)).

Понятие «спам» определяется в российском законодательстве как 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[1].

Обработка информации, которая происходит во время пользования интернет-браузером, по итогам которой пользователю предлагается «личный набор» рекламной информации в соответствии с его предпочтениями, не рассматривается как спам или иная незаконная деятельность.

Так, Федеральная антимонопольная служба не усмотрела нарушений законодательства в деятельности почтового сервиса *Gmail* компании *Google*. Популярная почтовая служба анализирует тексты сообщений своих пользователей с целью подбора рекламы[2].

В своей «Политике конфиденциальности» *Google* прямо утверждает: «Мы собираем информацию, которая помогает улучшить наши службы, начиная с языковых настроек и заканчивая более сложными вещами, например интересными для конкретного пользователя объявлениями или людьми в Интернете». Действия данной компании законны, поскольку пользователь дает свое согласие на использование данных о себе, приступая к работе с *Google* и создавая аккаунт.

Все актуальнее становится вопрос о защите от нежелательной информации, в том числе от спама. На наш взгляд, потребитель имеет право выбирать – получать информацию рекламного характера или нет.

Есть специальные технические средства, которые позволяют защититься от рекламной информации. В частности, разработано программное обеспечение, которое блокирует рекламу, – *AdBlock Plus* и *uBlock Origin*.

Есть программы, которые не защищают, а атакуют – в фоновом режиме, не мешая пользователю, «кликают» все рекламные объявления. Речь идет о программном продукте компании *AdNauseam*. Такой вариант оказался крайне нежелательным для компании *Google*, поскольку пользователь, использующий эту программу, теряет черты

[1] См.: постановление Правительства РФ от 10.09.2007 № 575 «Об утверждении Правил оказания телематических услуг связи».

[2] Информационное сообщение (http://fas.gov.ru/fas-in-press/fas-in-press_37509.html (дата обращения: 07.03.2017)).

индивидуальности, которые позволяют предлагать ему конкретные товары и услуги, в которых он заинтересован. Компания *Google* удалила не только эту программу из своего сетевого магазина, но и дополнение в браузере *Chrome*, а также использует программу, препятствующую установлению *AdNauseam*[1]. Представляется, что в данном случае компания *Google* действует недобросовестно, ограничивая своих пользователей в выборе не только программного обеспечения, но и варианта поведения.

Наибольшую потенциальную опасность как для интересов потребителей, так и для интересов конкурентов может представлять скрытая реклама, распространяемая в сети Интернет. Скрытая реклама, под которой понимается реклама, оказывающая не осознаваемое потребителями рекламы воздействие на их сознание, в том числе посредством использования специальных видеовставок (двойной звукозаписи) и иных способов, запрещается. Скрытой является реклама, которая оказывает воздействие на сознание потребителей в форме, препятствующей осознанию данного вида вмешательства, влияющего на свободу выбора потребителя[2]. Как отмечается в литературе, в данном случае учитывается, что подсознание человека слабо контролируется, и, воздействуя на него, можно заставить человека принимать нерациональные решения[3].

Скрытая реклама очень близка к так называемому *Product Placement* (в дословном переводе – размещение товара, далее – «продакт плейсмент»). И скрытая реклама, и «продакт плейсмент» могут иметь место в играх, распространяемых в социальных сетях, в блогах, в электронных СМИ, видеороликах, распространяемых в сети Интернет, и т.п.

Законодательные акты различных государств предъявляют к рекламе требование распознаваемости. Это требование нельзя рассматривать как сущностный признак рекламы – оно применяется к рекламной продукции в целях контроля. Так, согласно ст. 3 Закона Эстонской Республики от 01.07.1997 «О рекламе» содержание, дизайн и форма

[1] Информационное сообщение (https://adnauseam.io/free-adnauseam.html (дата обращения: 07.03.2017)).

[2] Это скрытые побуждения, воздействующие на бессознательный уровень восприятия (постановление ФАС Северо-Западного округа от 30.08.2010 по делу № А52-6308/2009 (https://kad.arbitr.ru/Card/2c4caf4a-67a0-412f-9a6a-5150db610946 (дата обращения: 03.03.2017)).

[3] *Рузанов И.В.* Бихевиоральная наука как метод исследования правоотношений между государством и бизнесом (на примере рекламного рынка) // Законодательство и экономика. 2016. № 6. С. 56–63.

исполнения рекламы должны гарантировать, что они будут интерпретированы как реклама при обычном внимании общества[1]. В соответствии со ст. 6 Закона Республики Казахстан от 19.12.2003 № 508-II «О рекламе» реклама независимо от формы или используемого средства распространения, размещения должна быть достоверной, распознаваемой без специальных знаний или применения специальных средств непосредственно в момент ее представления[2].

Применительно к «продакт плейсмент» распознаваемость присутствует далеко не всегда. Но «продакт плейсмент» обычно не рассматривается как скрытая реклама, поскольку особые технические приемы для применения этого способа распространения информации не применяются. Полагаем, что целью законодателя при введении данного запрета явилось ограждение потребителей от такого воздействия, которое невозможно распознать без специальных технических средств. В случае с «продакт плейсмент» такого элемента, как правило, нет, но не всегда рекламное послание можно распознать.

«Продакт плейсмент» можно определить как один из способов продвижения товара на рынок, связанный с включением в произведение искусства упоминания о товаре, его производителе, товарном знаке. Примером могут служить так называемые рекламирующие игры (*advergame*). Сюжет игры строится вокруг бренда одной компании, а цель игры – привлечь потенциальных потребителей к сайту и в конечном счете – к товарам и услугам компании.

Выделяют три подхода к использованию «продакт плейсмент».

Согласно первому подходу рекламное размещение продукта в произведениях науки, литературы, искусства запрещается. Такой подход существовал в ряде европейских стран до принятия Директивы ЕС 2007/65/ЕС, допускающей при определенных условиях рекламное размещение продукции[3]. В настоящее время в странах ЕС рекламное размещение продукта запрещается.

Второй подход, используемый в США, – допустимость применения такого способа размещения рекламной информации, как «продакт плейсмент».

И третий подход, используемый в России, – исключение «продакт плейсмент» из сферы действия законодательства о рекламе.

[1] http://www.MEDIALAW.ru/ (дата обращения: 01.03.2017).

[2] Казахстанская правда. 2003. 26.12. № 367-368 (24307-24308).

[3] http://ec.europa.eu/avpolicy/docs/reg/modernisation/proposal_2005/avmsd_cons_may07_en.pdf (дата обращения: 05.03.2017).

Согласно п. 2 ст. 2 Закона о рекламе Закон не распространяется на упоминания о товаре, средствах его индивидуализации, об изготовителе или о продавце товара, которые органично интегрированы в произведения науки, литературы или искусства и сами по себе не являются сведениями рекламного характера.

Полагаем, что в случае использования как узкого (реклама понимается как информация, сообщение, представление), так и широкого подхода к пониманию рекламы (реклама понимается в том числе как совокупность определенных действий (мероприятий), а также как «послание»), результат «продакт плейсмент» можно квалифицировать как рекламу. Вместе с тем применительно к собственно «продакт плейсмент» более подходящим является указание на то, что это не сама рекламная информация, а совокупность действий по размещению рекламной информации в произведении.

Что касается целей использования «продакт плейсмент», то, несомненно, его целями было продвижение конкретного товара или производителя на рынке, формирование положительного образа у потребителей, увеличение количества продаж, что в целом совпадает с целями рекламы.

Наиболее сложным является вопрос об органичности или неорганичности размещения информации. Необходимо учитывать общий контекст произведения и соответствие (несоответствие) фрагмента, содержащего упоминание о товаре или его производителе; оправданно ли включение такого фрагмента сюжетной линией; представляется ли акцентирование на товаре, его производителе излишним или неестественным; преследует ли упоминание о товаре цель формирования интереса к товару среди потенциальных производителей. Вместе с тем следует особо обратить внимание на то, что органичность вплетения упоминания о товаре, товарном знаке, производителе в сюжет произведения как раз является особой чертой, характерной для «продакт плейсмент».

По мнению специалистов ФАС России, признаками органичной интеграции следует признать включение информации в состав общего сюжета произведения или его части; возможность оценки информации как дополнительной характеристики героя или созданной ситуации; отсутствие нарушения сюжета и невозможность изъятия из него без ущерба для целостного восприятия произведения[1].

[1] Письмо ФАС России от 25.05.2011 № АК/20129 «О признании рекламы неорганично интегрированной в теле-, радиопередачу» (документ опубликован не был (СПС «КонсультантПлюс»)).

«Продакт плейсмент» сходен с рекламой хотя бы в силу того, что «размещение» стимулирует интерес к товару или его производителю (продавцу) и при этом осуществляется на основе договора между создателями произведения и правообладателем. Таким образом, «продакт плейсмент» можно определить как совокупность мероприятий, в результате которых в сюжетную линию произведения науки, литературы, искусства внедряется информация о товаре, услуге, их производителе, средстве индивидуализации юридического лица таким образом, что она становится неотделимой частью самого произведения с целью создания положительного образа товара, услуги, их производителе, средстве индивидуализации юридического лица и продвижения на рынке.

Утверждение о том, что результат «продакт плейсмент» не является рекламой, не лишает его основных качественных характеристик рекламы. Полагаем, что общие ограничения рекламы должны распространяться и на «продакт плейсмент».

Учитывая разнообразие форм рекламы, распространяемой в сети Интернет, а также особенности самой сети, необходимо отражение данных особенностей в законодательстве.

В Законе о рекламе отражена далеко не вся специфика размещения и восприятия рекламной информации в Интернете. Более конкретными и крайне полезными для практиков являются разъяснения ФАС России. Например, в одном из таких разъяснений указывается, что по общему правилу не является рекламой информация, размещенная на сайте производителя; уделяется внимание вопросу фиксации нарушения (акт осмотра сайта по аналогии с осмотром сайта нотариусом, принт-скрины страниц сайта); указывается на возможность поиска в архиве Интернета (https://archive.org/web/)[1].

Итак, реклама, распространяемая в сети Интернет, доступна круглосуточно и, как правило, с территории любой страны. Рекламная информация может быть просмотрена неоднократно, если возникает такая необходимость. Потребитель в большинстве случаев не может контролировать наличие рекламы. Интернет-сайты могут достаточно легко менять свое содержание, и поэтому процесс доказывания размещения ненадлежащей рекламы может быть затруднен. Таким образом, сеть Интернет как средство, с помощью которого распро-

[1] См., например, Письмо ФАС России от 28.08.2015 № АК/45828/15 «О рекламе в сети «Интернет»». Документ опубликован не был (СПС «КонсультантПлюс»).

страняется реклама, обладает объективно существующими особенностями, которые влияют на специфику восприятия, распространения, воспроизведения, поиска и удаления информации. Эти особенности должны учитываться как законодателем, так и правоприменителем.

Пристатейный библиографический список:

1. Постатейный комментарий к Федеральному закону «О рекламе» / Д.С. Бадалов, И.И. Василенкова, Н.Н. Карташов и др. М.: Статут, 2012.

2. *Рузанов И.В.* Бихевиоральная наука как метод исследования правоотношений между государством и бизнесом (на примере рекламного рынка) // Законодательство и экономика. 2016. № 6.

А.Ю. Чурилов

ИСПОЛЬЗОВАНИЕ ТЕХНОЛОГИИ БЛОКЧЕЙН: ПЛАТЕЖНАЯ СИСТЕМА, «УМНЫЕ» КОНТРАКТЫ, ПРИНЯТИЕ КОЛЛЕГИАЛЬНЫХ РЕШЕНИЙ, ХРАНЕНИЕ ИНФОРМАЦИИ

Аннотация. *Статья посвящена оценке технологии блокчейн с точки зрения перспектив правового регулирования и возможности использования в предпринимательской и иной деятельности с учетом правового поля Российской Федерации. Автор рассматривает технологию блокчейн с точки зрения выполнения функций платежной системы и иных способов применения, таких как использование для распределенного хранения информации, децентрализованного принятия решений, в качестве замены традиционным договорам.*

Ключевые слова: *криптовалюта, блокчейн, договор, деньги*.

Первое упоминание технологии блокчейн (*Blockchain*) можно обнаружить в работе, написанной человеком или группой людей под псевдонимом Сатоши Накамото (*Satoshi Nakamoto*), – «Биткоин: пиринговая электронная денежная система»[1]. Прежде чем рассматривать особенности применения и правового регулирования этой технологии, необходимо осветить основы и особенности ее функционирования.

Блокчейн представляет собой базу данных, распределенную между всеми включенными в сеть блокчейн (*Blockchain Network*) устройствами, с использованием которой пользователи осуществляют передачу информации. Как известно, любая информация, в том числе информация о транзакциях, может быть представлена объемом данных, который в ней содержится – один символ представляет собой 1 бит, 8 бит – 1 байт и т.д. Так, и информация о транзакциях в системе блокчейн представляет объем данных, объединенных в своего рода звенья, которые, в свою очередь, объединены в хронологическом порядке в цепочку блоков, в которой каждый предыдущий блок подтверж-

[1] *Satoshi Nakamoto*. Bitcoin: A Peer-to-Peer Electronic Cash System (URL: https://bitcoin.org/bitcoin.pdf (дата обращения 25.01.2017)).

дает действительность последующего путем включения информации о предыдущих транзакциях в виде особого криптографического ключа в заголовок каждого последующего блока транзакций[1]. Таким образом, каждый блок идентифицируется с помощью криптографического ключа, хэша (*hash*), который генерируется с использованием криптографического алгоритма SHA256[2]. При этом каждый из участников сети хранит как минимум часть всей базы данных, что обеспечивает ее устойчивость к противоправным действиям со стороны как третьих лиц, так и самих участников.

Безусловное преимущество такой системы перед классическими платежными системами или системами хранения информации состоит в том, что для изменения единственного блока транзакции предполагаемому злоумышленнику необходимо изменить все блоки, которые были добавлены в цепь транзакции после взламываемого блока. Такой механизм осуществления транзакций приводит к невозможности так называемой двойной траты (*double spending*) одной и той же виртуальной единицы, которой оперирует система блокчейн.

Ключевой особенностью рассматриваемой технологии является отсутствие какого-либо центра контроля и управления транзакциями, осуществляющимися в сети блокчейн, поскольку транзакции подтверждаются с помощью особого криптографического механизма. Основной способ подтверждения транзакций состоит в обеспечении их публичности – каждая проведенная операция в системе передается всем устройствами сети, и только после подтверждения с их стороны запись о ней заносится в публичную книгу транзакций (*shared public ledger*). В связи с этим разработчики данной технологии теоретически не могут воздействовать на целостность и достоверность транзакций.

Отсутствие центра контроля и подтверждения транзакций на первый взгляд подталкивает к выводу о том, что при осуществлении транзакций в системе блокчейн отсутствует третье лицо как посредник для верификации, подтверждения транзакций. Однако такое утверждение не вполне верно: такой третьей стороной является сама система блокчейн и пользователи – владельцы устройств, входящих в сеть блокчейн.

Особенностью технологии блокчейн ошибочно считают анонимность транзакций[3].

---

[1] Отсюда и название технологии – блокчейн – цепь блоков.

[2] *Andreas M.* Antonopoulos. Mastering Bitcoin. O'Reily Media, 2015. С. 170.

[3] *Олиндер Н.В.* Криминалистическая характеристика электронных платежных средств и систем // Lex russica. 2015. № 10. С. 128–138.

Действительно, для использования криптовалюты биткоин по общему правилу нет необходимости регистрироваться или идентифицировать себя иным образом, достаточно лишь указать адрес электронной почты и желаемый пароль. Для использования системы используется пара публичный ключ – частный ключ, с помощью которых и осуществляются транзакции в системе без раскрытия личности отправителя и получателя. Однако, по справедливому утверждению зарубежных исследователей, такую систему следует называть псевдоанонимной, нежели анонимной[1]. Это связано с несколькими обстоятельствами.

Во-первых, как уже отмечалось, все транзакции в каждой конкретной системе блокчейн, кроме закрытых систем, заносятся в публичную книгу транзакций, с которой может ознакомиться любой желающий.

Во-вторых, в истории транзакций можно увидеть *IP*-адрес, который использовался при осуществлении транзакции. Безусловно, с использованием современных технологий можно добиться практически полной анонимности при использовании технологии блокчейн. Но, как показывает практика, в частности, на примере ареста Росса Ульбрихта по делу «Шелкового Пути», отследить как отправителя, так и получателя вполне возможно.

В связи с псевдоанонимной природой блокчейн невозможно согласиться с утверждением А.И. Савельева о том, что данная технология позволяет «достоверно фиксировать достоверные данные о принадлежности существующего в цифровой форме актива определенному **лицу** (выделено мной. – *А.Ч.*)»[2]. Дело в том, что пара публичный ключ – частный ключ определяет не конкретное лицо, а скорее конкретный IP-адрес или электронную почту, при этом не обязательно владельца частного ключа, который обеспечивает доступ к виртуальным единицам сети блокчейн. Следовательно, о достоверности принадлежности актива можно говорить только применительно к публичному ключу, но не к какому-то конкретному лицу, поскольку оно по общему правилу неизвестно.

---

[1] См., например: *Marcin Szczepanski*. Bitcoin Market, economic and regulation. EPRS Briefing, 2014 (URL: http://www.europarl.europa.eu/RegData/bibliotheque/briefing/2014/140793/LDM_BRI(2014)140793_REV1_EN.pdf (дата обращения: 25.01.2017)); *Malte Möser*. Anonymity of Bitcoin Transactions: An Analysis of Mixing Services // Münster Bitcoin Conference, 2013.

[2] *Савельев А.И.* Договорное право 2.0: «умные» контракты как начало конца классического договорного права // Вестник гражданского права. 2016. № 3. С. 32–60.

В связи с популяризацией технологии блокчейн в мире выделяют два поколения развития этой технологии – блокчейн 1.0, символизирующей только криптовалюту, и блокчейн 2.0, которая включает в себя иные способы применения, такие как «умные контракты», «умная собственность», распределенное хранение информации[1].

Таким образом, в настоящее время технология блокчейн используется двумя основными способами: 1) в качестве платежной системы для создания и осуществления транзакций с криптовалютой и 2) иные виды использования, включая «умные» контракты.

Использование технологии блокчейн в качестве платежной системы

Поскольку наиболее популярной криптовалютой в настоящее время является биткоин, анализ использования технологии блокчейн с точки зрения осуществления функций платежной системы будет проведен на примере биткоина.

Подчеркну, что биткоин нельзя относить к деньгам (валюте) в классическом понимании этих явлений экономической теорией[2]. Однако в силу сложившейся традиции называть криптовалюту, а равно и виртуальную валюту валютой и во избежание терминологической путаницы в дальнейшем в работе будут использоваться понятия виртуальной валюты и криптовалюты, но не в смысле денег (валюты) как законного средства платежа.

Биткоин как криптовалюта является разновидностью виртуальной валюты. Первое официальное определение виртуальной валюты было дано Европейским центральным банком в 2012 г.: виртуальная валюта представляет собой вид неурегулированных электронных денежных средств, выпуск и оборот которых контролируется создателем, используемых и принимаемых среди членов определенного виртуального сообщества[3]. В Нью-Йорке виртуальная валюта определяется как электронная денежная единица, используемая в качестве средства обмена либо в качестве средства сохранения стоимости[4].

[1] Blockchain and Beyond. Cellabz, 2015.

[2] *Чурилов А.Ю.* К вопросу о правовой природе криптовалюты // Хозяйство и право. 2016. № 9. С. 93–99.

[3] Virtual Currency Schemes. European Central Bank, 2012. С.13.

[4] New York Codes, Rules and Regulations. Title 23. Department of Financial Services. Chapter 1 – regulations of the superintendent of financial services. Part 200 – virtual currencies.

Таким образом, виртуальная валюта представляет собой цифровое выражение стоимости, не являющееся законным средством платежа, но принимаемое в качестве оплаты за товары и услуги в определенном кругу субъектов права.

Основным неудобством использования биткоина в качестве средства платежа является его неопределенный правовой статус.

Так, налоговая служба США признает биткоин имуществом[1]. Среди судов Соединенных Штатов нет единой позиции по вопросу правовой природы криптовалюты – некоторые судьи считают биткоин деньгами[2], некоторые не признают криптовалюту в качестве денег[3]. Комиссия по торговле товарными фьючерсами рассматривает биткоин в качестве цифрового биржевого товара (*digital commodity*)[4]. В Германии биткоин считается «частными деньгами». В Китае оборот биткоинов полностью запрещен для использования финансовыми и платежными организациями, в частности запрещается: определять цены в биткоинах, продавать и покупать биткоины, обменивать биткоин на национальные или иностранные валюты, оказывать любые иные связанные с биткоинами услуги клиентам и т.д.[5]. Европейский суд справедливости вынес решение, согласно которому операции с биткоином освобождены от налога на добавленную стоимостью (VAT) в соответствии с законодательными положениями о валюте, банкнотах и монетах, используемых в качестве законного средства платежа[6]. Однако во многих странах, в том числе и в Российской Федерации, правовой режим биткоинов, так и не попавших в поле зрения государства, не определен.

Центробанк России в 2014 г. предупредил, что предоставление услуг по обмену криптовалют на рубли и иностранную валюту, а также на товары (работы, услуги) будет расцениваться в соответствии с законодательством о противодействии легализации (отмыванию)

[1] Internal Revenue Service. Virtual Currency Guidance, section 4 (April 2014). Internal Revenue Bulletin: 2014-16.

[2] Case 1:14-cr-00243-JSR. Document 43 (URL: 08/19/14http://www.internetlawcommentary.com/materials/faiella_order.pdf (дата обращения: 21.11.2016)).

[3] Case F14-2923 (URL: http://www.miamiherald.com/news/local/crime/article91785802.ece/BINARY/Read%20the%20ruling%20(.PDF) (дата обращения: 25.01.2017)).

[4] Houman B. Shadab. Regulating Bitcoin and Block Chain Derivatives. Written statement to the Commodity Futures Trading Commission Global Markets Advisory Committee Digital Currency Introduction – Bitcoin, 2014.

[5] English summary of the Notice on Precautions Against the Risks of Bitcoins (URL: https://vip.btcchina.com/page/bocnotice2013 (дата обращения: 25.01.2017)).

[6] Skatteverket v David Hedqvist. Case C-264/14.

преступных доходов и финансированию терроризма как участие в осуществлении сомнительных операций. Поводом для данного заявления стало выявление случаев осуществления российскими нефинансовыми организациями операций с криптовалютой. ЦБ России отметил, что согласно ст. 27 ФЗ от 10.07.2002 № 86-ФЗ «О Центральном банке Российской Федерации (Банке России)» выпуск на территории Российской Федерации денежных суррогатов запрещается[1].

Вместе с тем в Российской Федерации не выработано легального определения денежного суррогата. Более того, в доктрине ведется дискуссия об определении денежного суррогата, его признаках и месте в гражданском обороте[2]. Однако, поскольку биткоин не является денежной единицей, он не может признаваться, вопреки мнению ряда исследователей[3], и денежным суррогатом.

Биткоин является объектом гражданских прав особого рода, не имеющим материального воплощения. По указанным выше причинам биткоин не может быть признан наличными деньгами. Он также не является вещью, поскольку вещами признаются материальные и физические, осязаемые объекты. Не являются биткоины и безналичными денежными средствами, поскольку они не находятся на банковских счетах, представляя собой лишь запись в публичной учетной книге об их принадлежности тому или иному публичному ключу. Невозможно рассматривать биткоин и в качестве обязательственного имущественного права (права требования), поскольку, во-первых, отсутствует субъект (эмитент, оператор), к которому такое требование обращено, и, во-вторых, отношения по обращению и созданию биткоинов не имеют обязательственного характера, поскольку технология блокчейн позволяет передавать биткоины от одного пользования к другому непосредственно[4].

На первый взгляд биткоины напоминают электронные денежные средства в том смысле, который придает им ФЗ от 27.06.2011 № 161-ФЗ

---

[1] Информация Банка России от 27.01.2014 «Об использовании при совершении сделок «виртуальных валют», в частности, Биткойн» // Вестник Банка России. 2014. № 11. 05.02.

[2] Обзор точек зрения см.: *Крылов О.М.* К вопросу о правовой категории «денежный суррогат» // Административное и муниципальное право. 2011. № 8. С. 56–61.

[3] *Мюттер Г.* Правовая неопределенность криптовалюты // эж-Юрист. 2016. № 16. С. 2.

[4] *Савельев А.И.* Договорное право 2.0: «умные» контракты как начало конца классического договорного права // Вестник гражданского права. 2016. № 3. С. 32–60.

«О национальной платежной системе», однако таковыми не являются. Оборот электронных денежных средств, исходя из толкования указанного Закона, всегда предполагает наличие посредника в лице оператора при использовании традиционных денежных средств. Платежная система биткоин не подразумевает наличие посредника при транзакции биткоинов от пользователя к пользователю.

Более того, биткоин не может считаться платежной системой в том смысле, который определен в п. 20 ст. 3 Закона о национальной платежной системе. Во-первых, в платежной системе биткоин нет вышестоящих организаций и операторов, поскольку пользователи взаимодействуют только между собой в одноранговой (пиринговой) сети. Во-вторых, эта система не регулируется правилами платежной системы, установленными российским или иным законодательством.

Не является биткоин и иностранной валютой по смыслу ФЗ от 10.12.2003 № 173-ФЗ «О валютном регулировании и валютном контроле», поскольку не является законным средством платежа ни в одном иностранном государстве.

Биткоин не может быть признан объектом права собственности в строгом смысле этого понятия. Фактически «владение» биткоином означает лишь то, что на «кошельке» владельца публичного и частного ключей есть записи о совершении определенного количества транзакций криптовалюты в отношении этого «кошелька», сумма которых составляет баланс «кошелька» – публичного ключа.

Попытки втиснуть криптовалюту в рамки существующего перечня объектов гражданских прав, в частности, в иное имущество[1], представляются не соответствующими природе криптовалюты. Криптовалюта является объектом прав особого рода, не имеющим материального воплощения.

В настоящее время ни биткоин, ни любая другая криптовалюта не могут быть отнесены к какому-либо виду объектов гражданских прав, в связи с чем представляется целесообразным внести соответствующие изменения в ГК РФ с целью включения в положения об объектах гражданских прав такого объекта гражданского права, как «криптовалюта». В рамках действующего отечественного законодательства процесс обмена биткоинов на товары следует рассматривать как заключение между сторонами договора мены, а на услуги – смешанного договора с элементами купли-продажи и возмездного оказания услуг.

[1] *Лейба А.* Реальная жизнь виртуальных денег // эж-Юрист. 2014. № 23.

Несмотря на правовую неопределенность, криптовалюта используется как гражданами, так и юридическими лицами, в том числе в предпринимательской деятельности. Рассмотрим те особенности криптовалюты, которые влияют на правовое регулирование криптовалюты как в настоящее время, так и в перспективе.

Исходя из особенностей технологии, лежащей в основе криптовалюты, ее невозможно подделать, в частности невозможна так называемая двойная трата одной и той же виртуальной единицы. Это связано с тем, что информация обо всех когда-либо совершенных транзакциях размещена в публичной книге транзакций, в случае противоречия которой транзакция не будет подтверждена и, как следствие, не будет совершена. Из этого вытекает два следствия. Первое – транзакции криптовалюты являются окончательными, и их нельзя оспорить во внесудебном порядке в отличие от транзакций с использованием классических платежных систем, таких как *Visa, PayPal*. Второе – при использовании в качестве средства платежа криптовалюты продавец защищен от мошенничества с возвратным платежом (*chargeback*).

Идентификация сторон транзакции и, следовательно, договора может быть затруднительна в связи с псевдоанонимной природой криптовалюты. Это обстоятельство создает множество трудностей, в том числе при неправомерных действиях сторон договора. Более того, фактическим обладателем криптовалюты является лицо, которое владеет частным ключом, дающим доступ к совершению транзакций. В случае неправомерного доступа к частному ключу утраченные единицы криптовалюты восстановить будет невозможно ввиду необратимости транзакций.

Отсутствие посредника в лице банка или платежной организации при осуществлении транзакций хотя и позволяет сократить операционные издержки, несет в себе определенные правовые риски. Поскольку запись о принадлежности криптовалюты не является вкладом, не гарантируется банком, невозможно застраховать факт обладания криптовалютой, к примеру, от ее утраты или неправомерного перевода иному лицу. Использование криптовалюты в настоящее время не требует ведения какой-либо отчетной документации, что может стать проблемой в налоговых правоотношениях. Невозможно арестовать «счет» криптовалюты или каким-либо иным способом воздействовать на операции в системе ввиду отсутствия администратора. Единственным возможным способом воздействия на владельца «кошелька» является изъятие его частного ключа.

Максимальное количество единиц криптовалюты, которые могут создать пользователи, ограничено и определяется особенностями протоколов, лежащих в основе криптовалюты. К примеру, максимально возможное количество биткоинов, которые могут быть созданы, – 21 млн[1]. То обстоятельство, что пользователи сами создают криптовалюту, хотя на первый взгляд это и является безусловным преимуществом, составляет непреодолимое препятствие на пути признания децентрализованной криптовалюты законным средством платежа в любом государстве. Это связано с тем, что правом на эмиссию денег обладает исключительно государство.

Так, в Российской Федерации исключительным правом осуществлять эмиссию обладает Банк России. Признание в качестве законного средства платежа какой-либо криптовалюты означает для государства утрату как монополии на эмиссию денежных средств, так и, как следствие, утрату контроля за эмиссией. Более того, невозможно принимать криптовалюту по ее нарицательной стоимости в связи с отсутствием таковой – она сама является товаром особого рода и обладает определенной, зависящей от спроса и предложения ценой.

Другие способы использования технологии блокчейн

Поколение блокчейн 1.0 не в полной мере раскрывало возможности этой технологии, в связи с чем постепенно эволюционировало в блокчейн 2.0.

Помимо платежных систем, существует множество вариантов использования систем, основанных на технологии блокчейн. Для этого в большинстве случаев создаются так называемые *MetaChain* или *Altchain*, представляющие собой дополнительный «слой» программного кода, встраиваемого в технологию, которую использует биткоин. Используя биткоины для создания собственных виртуальных единиц, создатели преследуют цель упростить верификацию обращения таких единиц, представляющих собой не криптовалюту как средство обмена и платежа, а, к примеру, сертификаты, купоны, голоса.

«Умные» контракты. Наиболее противоречивым применением технологии блокчейн являются так называемые умные контракты, представляющие собой договоры, которые автоматически исполняются

[1] *Степанченко А.В.* Иностранная валюта как объект современного гражданского оборота // Бизнес, Менеджмент и Право. 2013. № 2. С. 36–42.

компьютером[1]. Такой контракт состоит из трех основных частей – «ядра» (программного кода), в котором содержатся условия будущего договора; файла договора, находящегося в системе блокчейн; баланса счета пользователя.

Существует множество сервисов, с помощью которых можно воспользоваться технологией «умных» контрактов – *Etherium*, *BlockStream* и т.д.

Первоначально необходимо определить, можно ли рассматривать «умный» контракт как договор, т.е. соглашение двух и более лиц об установлении, изменении или прекращении гражданских прав и обязанностей.

В пользу признания «умного» контракта договором говорит, во-первых, то, что в результате его заключения действительно возникают права и обязанности в соответствии с условиями, на которых этот договор заключен. Во-вторых, совершая действия, направленные на заключение «много» контракта и соответственно договора, стороны выражают свою волю на достижение соглашения, что свидетельствует о волевом характере этих действий.

Проблемной применительно к признанию «умного» контракта договором в соответствии с отечественным законодательством является форма такого договора. В соответствии с ГК РФ договор может быть заключен в том числе путем обмена письмами, телеграммами, телексами, телефаксами и иными документами, включая электронные документы, передаваемые по каналам связи, позволяющим достоверно установить, что документ исходит от стороны по договору. В связи с этим наиболее серьезную проблему, как уже отмечалось не раз, составляет идентификация сторон. В связи с этим возникает вопрос: можно ли рассматривать использование частного ключа для заключения договора в качестве электронной подписи?

В соответствии с ФЗ от 06.04.2011 № 63-ФЗ «Об электронной подписи» электронная подпись – 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. По общему правилу участники блокчейн-систем не раскрывают свою личность, но возможно включить

[1] BBVA research. Smart contracts: the ultimate automation of trust? Digital Economy Outlook (October 2015) // (URL: https://www.bbvaresearch.com/wp-content/uploads/2015/10/Digital_Economy_Outlook_Oct15_Cap1.pdf).

информацию о договаривающихся сторонах в код «умного» контракта. Следовательно, при соблюдении условия идентификации сторон использование частного ключа можно рассматривать в качестве электронной подписи.

Таким образом, условно можно признать «умный» контракт договором[1], обладающим рядом признаков, которые позволяют выявить его существенные недостатки.

1. Существование исключительно в электронной форме. Этот признак, безусловно, не является квалифицирующим, поскольку договоры могут заключаться посредством обмена электронными письмами и не существовать на бумаге. Его существование лишь в электронной форме исключает его применение для заключения некоторых договоров. Примером может служить договор аренды недвижимого имущества, заключаемый на срок более года и подлежащий государственной регистрации. В настоящее время законодательством не предусмотрена процедура регистрации договора иного, нежели составленного на бумаге и подписанного сторонами.

2. Условия такого договора закрепляются с помощью языков программирования и формулируются по модели договора присоединения[2]. В связи с этим можно выделить ряд правовых проблем. Действительно, «ядро» «умного» контракта не может быть изменено после его создания, что вызовет проблемы при существенном изменении обстоятельств или необходимости изменения отдельных его условий, к примеру адреса доставки товара или в случае перемены сторон в обязательстве. Также при текущем уровне развития этой технологии невозможно урегулирование преддоговорных споров с использованием системы «умных» контрактов, что приводит к неприменимости такой формы договора в поставочных отношениях, за редкими исключениями.

3. Невозможно согласиться с мнением, что характерной чертой является повышенная степень определенности договора[3]. Невозможно включить все необходимые, а применительно к некоторым договорам и существенные условия в программный код, что на практике может привести к длительным судебным тяжбам.

---

[1] Необходимо отметить, что судебными инстанциями, в том числе зарубежными, не рассматривались споры в связи с заключением «умных» контрактов, что не позволяет сделать вывод о признании или непризнании законности таких договоров.

[2] См.: *Савельев А.И.* Договорное право 2.0: «умные» контракты как начало конца классического договорного права // Вестник гражданского права. 2016. № 3. С. 32–60.

[3] Там же.

4. Исходя из особенностей построения программного кода «умного» контракта по типу «если – то» (*if – then*) можно говорить о том, что такой договор всегда формирует встречное обязательство.

5. Следует согласиться с мнением о таком признаке «умных» контрактов, как их направленность на распоряжение цифровыми активами[1] ввиду практически полной непригодности для распоряжения реальными, а не цифровыми, активами.

Представляется спорным утверждение А.И. Савельева о невозможности нарушения «умного» контракта, об отсутствии необходимости посредников в виде судов, судебных приставов и прочих правоохранительных органов[2]. Существует множество обстоятельств, при которых такой договор может быть нарушен – нарушение сроков исполнения обязательства, поставка некачественного товара и т.д. В первую очередь это применимо к договорам по распоряжению реальными, а не цифровыми активами, но одно это ставит под сомнение вывод о ненарушаемости «умного» контракта. Более того, частным ключом лица может завладеть злоумышленник и заключить от его имени несколько договоров, которые в дальнейшем необходимо будет оспаривать в судебном порядке.

Подводя итог, следует признать маловероятным широкое распространение «умных» контрактов в ближайшее время в повседневной деятельности, особенно в предпринимательской, в связи, во-первых, с недостатком правового регулирования таких договоров и, во-вторых, с многочисленными проблемами как технологического, так и экономико-юридического характера. Безусловно, при дальнейшем развитии технологий будет появляться все больше и больше возможностей для заключения «умных» контрактов, их развитие повлияет на процесс законотворчества и правоприменительную практику.

Коллегиальное принятие решений. Теоретически интересным и возможным применением технологии блокчейн представляется децентрализованное принятие решений. Такой механизм можно было бы использовать в том числе и при принятии решений на общем собрании акционеров, если бы не неопределенность правового статуса такого голосования. Трудности применения такой процедуры в отечественном правопорядке можно рассмотреть на примере проведения общего собрания акционерного общества.

---

[1] См.: *Савельев А.И.* Договорное право 2.0: «умные» контракты как начало конца классического договорного права // Вестник гражданского права. 2016. № 3. С. 32–60.

[2] Там же.

Безусловно, голосование с применением технологии блокчейн необходимо рассматривать как заочное, которое может осуществляться в том числе и путем заполнения электронной формы бюллетеней в сети Интернет (ФЗ от 26.12.1995 № 208-ФЗ «Об акционерных обществах» (ред. от 03.07.2016)). Теоретически можно сформировать программный код голосования акционеров таким образом, чтобы он соответствовал требованиям, предъявляемым к бюллетеням для голосования. Однако в дальнейшем возникают определенные сложности как правового, так и технического характера.

Во-первых, идентификация голосующего акционера представляется затруднительной, поскольку исходя из самой сути технологии блокчейн голосует не лицо, а его ключ, установление принадлежности которого составляет отдельную проблему.

Во-вторых, при голосовании акционеров необходимо использовать закрытые блокчейн-системы, подразумевающие допуск каждого голосующего и предоставление ему пары публичный ключ – частный ключ, что представляется затруднительным в обществах с количеством участников свыше 500 тыс., для которых предусмотрены куда более удобные механизмы проведения заочного голосования.

В-третьих, применительно к публичным акционерным обществам в связи с постоянным движением акций проблематично отслеживать новых акционеров и исчезновение старых, используя технологию блокчейн.

В-четвертых, при использовании технологии блокчейн действует общее правило – один голос – один ключ, что не соответствует правилам голосования в акционерных обществах.

Следует заключить, что применительно к крупным компаниям в настоящее время использование технологии блокчейн для осуществления голосования не выглядит перспективным.

Хранение информации. В настоящее время существуют сервисы, предоставляющие услуги по децентрализованному хранению информации, используя для этого технологию блокчейн, – это позволяет снизить издержки при сохранении защищенности данных.

Так, стоимость хранения одного гигабайта данных на сервисе *Storj* стоит всего 0.015 долл. в месяц. Однако такое распределенное хранение информации влечет ряд рисков. К примеру, в случае обнаружения незаконного контента в системе блокировке могут подвергнуться все пользователи этой системы.

Иные способы использования технологии блокчейн. Принципы, лежащие в основе блокчейн, могут использоваться для построения систем распределенного хранения данных о собственности, нотариальных документах, данных о залоге недвижимости, долговых обязательствах. Кроме того, блокчейн можно использовать для хранения и доступа к базе данных клиентов, которая гораздо более защищена от воздействий третьих лиц, чем используемые в настоящее время базы данных. В этом случае необходимо использовать закрытые системы, чтобы предотвратить доступ к базам широкого круга лиц.

Вместе с тем «неприступность» данных в системе блокчейн напрямую зависит от надежности хранения частных ключей пользователями, в случае их утери восстановить доступ к базе можно будет только путем создания нового ключа, если и вовсе возможно.

Таким образом, технология блокчейн, безусловно, является перспективной и в дальнейшем будет только развиваться, однако технологические особенности приводят к проблемам и пробелам правового регулирования. Так, криптовалюту невозможно отнести ни к одному из ныне существующих объектов права, что затрудняет ее использование в обороте. Так называемые умные контракты порождают больше правовых проблем, чем решают их – их неприменимость к большей части отношений реального сектора экономики ставит под сомнение целесообразность дальнейшей разработки этого направления использования технологии блокчейн. Основными достоинствами технологии блокчейн являются защищенность от неправомерного воздействия со стороны третьих лиц или участников сети; низкие издержки при использовании в качестве платежной системы; снижение стоимости хранения информации.

Пристатейный библиографический список:

1. *Satoshi Nakamoto*. Bitcoin: A Peer-to-Peer Electronic Cash System (URL: https:// bitcoin.org/bitcoin.pdf (дата обращения: 25.01.2017)).

2. *Andreas M*. Antonopoulos. Mastering Bitcoin. O'Reily Media, 2015.

3. *Олиндер Н.В*. Криминалистическая характеристика электронных платежных средств и систем // Lex russica. 2015. № 10.

4. *Marcin Szczepanski*. Bitcoin Market, economic and regulation. EPRS Briefing, 2014 (URL: http://www.europarl.europa.eu/RegData/biblio-

theque/briefing/2014/140793/LDM_BRI(2014)140793_REV1_EN.pdf (дата обращения: 25.01.2017)).

5. *Malte Möser.* Anonymity of Bitcoin Transactions: An Analysis of Mixing Services // Münster Bitcoin Conference, 2013.

6. *Савельев А.И.* Договорное право 2.0: «умные» контракты как начало конца классического договорного права // Вестник гражданского права. 2016. № 3.

7. Blockchain and Beyond. Cellabz, 2015.

8. *Чурилов А.Ю.* К вопросу о правовой природе криптовалюты // Хозяйство и право. 2016. № 9.

9. Virtual Currency Schemes. European Central Bank, 2012.

10. Internal Revenue Service. Virtual Currency Guidance, section 4 (April 2014). Internal Revenue Bulletin, 2014–2016.

11. *Houman B.* Shadab. Regulating Bitcoin and Block Chain Derivatives. Written statement to the Commodity Futures Trading Commission Global Markets Advisory Committee Digital Currency Introduction – Bitcoin, 2014.

12. English summary of the Notice on Precautions Against the Risks of Bitcoins (URL: https://vip.btcchina.com/page/bocnotice2013 (дата обращения: 25.01.2017)).

13. *Крылов О.М.* К вопросу о правовой категории «денежный суррогат» // Административное и муниципальное право. 2011. № 8.

14. *Мюттер Г.* Правовая неопределенность криптовалюты // эж-Юрист. 2016. № 16.

15. *Лейба А.* Реальная жизнь виртуальных денег // эж-Юрист. 2014. № 23.

16. *Степанченко А.В.* Иностранная валюта как объект современного гражданского оборота // Бизнес, Менеджмент и Право. 2013. № 2.

17. BBVA research. Smart contracts: the ultimate automation of trust? Digital Economy Outlook (October 2015) (URL: https://www.bbvaresearch.com/wp-content/uploads/2015/10/Digital_Economy_Outlook_Oct15_Cap1.pdf).

И.А. Румянцев

БЛОКЧЕЙН И ПРАВО[1]

Аннотация. *Данная статья описывает технологию блокчейн. Автор рассматривает ее технические характеристики, а также правовые проблемы, возникающие при внедрении данной технологии. Также в работе рассматриваются другие технологии, связанные с блокчейном: смарт-контракты, криптовалюты.*

Ключевые слова: *биткоин, блокчейн, смарт-контракты, криптовалюты.*

Появление технологии блокчейн стало одним из ключевых событий в современной технологической сфере. На базе блокчейна функционирует значительное количество криптовалют, а его применение становится востребованным для целей оптимизации бизнес-процессов.

Блокчейн рассматривается А.И. Савельевым как «децентрализованная распределенная база данных, «учетная книга» всех подтвержденных транзакций, совершенная в отношении определенного актива, в основе функционирования которой лежат криптографические алгоритмы»[2]. Думается, что более точным было бы такое определение: блокчейн – это децентрализованный распределенный реестр транзакций, защищенный криптографическими средствами от взлома. В ходе исследования будет произведен разбор понятий, используемых в этом определении.

Блокчейн «родился» вместе с биткоином – как решение проблемы децентрализованной валюты и оказался гораздо перспективнее самой криптовалюты. Из известных успешных примеров реального использования блокчейна можно назвать: криптовалюту *Bitcoin*[3], ставшую

[1] Статья победителя конкурса IP & IT LAW – 2017.

[2] *Савельев А.И.* Договорное право 2.0: «Умные» контракты как начало конца классического договорного права // Вестник гражданского права. 2016. № 3. С. 32–59.

[3] *Satoshi Nakamoto*. Bitcoin: A Peer-to-Peer Electronic Cash System. P. 3 (URL: www.bitcoin.org).

предтечей всех блокчейн-технологий; проект *Ethereum*[1] – платформу, позволяющую создавать собственные блокчейны использованием гораздо более сложных алгоритмов – смарт-контрактов и различных цифровых активов – «токенов». Революционность решения, а также стремительный рост популярности стали препятствиями для планомерного и вдумчивого анализа природы блокчейна и существенно замедлили встраивание блокчейна в существующее правовое регулирование.

К проблемам, которые возникают при исследовании блокчейна, следует отнести отсутствие единообразного и семантически верного употребления терминов. В связи с этим необходимо дать следующие пояснения:

– термин «блокчейн» является транслитерацией английского слова *Blockchain*, с тем же смыслом.

– смарт-контракт и «умный» договор (контракт) – суть одно и то же. В настоящей работе будет использоваться термин «смарт-контракт» (англ. *smart* – умный), так как перевод термина позволяет воспринимать его неправильно. Кроме того, далее в статье сделана оговорка и относительно использования слова «договор» при описании смарт-контракта.

Блокчейн является перспективным решением, однако значимость этой технологии сильно переоценена. Слова Г. Грефа «Блокчейн – новый Интернет»[2] большинством были поняты неправильно – он абсолютно справедливо замечает несоизмеримые выгоды использования блокчейн вместо альтернативных расчетных технологий в оптимизации банковских расчетных процессов. Даже с исторической точки зрения блокчейн задумывался как платформа для криптовалюты *Bitcoin*, а значит, архитектура этой технологии особенно перспективна именно в финансовой сфере, так как существенно снижает издержки и увеличивает доверие в определенной (в том числе и банковской) экосистеме.

Автором настоящей работы будут рассмотрены минусы технологии блокчейн, проблемы регулирования данной технологии, а также определенные сферы, где блокчейн будет неэффективен.

[1] Информация с официального сайта проекта Ethereum (URL: https://www.ethereum.org/).

[2] См.: https://lenta.ru/news/2016/05/21/blockchain/ (дата обращения: 30.01.2017).

Классификация блокчейна

В связи со стремительным развитием технологии блокчейн имеет смысл рассмотреть возможные варианты реализации технологии блокчейн. Это связано с тем, что на разных уровнях регулирование блокчейна может осуществляться с учетом его технических возможностей.

На текущий момент в отечественной литературе описано несколько классификаций блокчейн-проектов.

Так, И.Т. Булгаков[1] указывает на дихотомическое деление по критерию использования криптовалют: финансовые и нефинансовые.

Представляется, что подобная характеристика не может быть полной, поскольку в ней не учитываются особенности применения криптовалют на основе блокчейна. Криптовалюты используются в трех целях: «сама по себе, то есть как аналог фиатным валютам» (*Bitcoin, Zcash, Darkcoin*); в качестве расчета за услуги, предоставленные использованием блокчейна как сервиса (*Namecoin, Ethereum*); в качестве *ICO*[2] как инновационного способа краудфандинга. Причем применение в одних целях не исключает использование в других[3].

Таким образом, наличие или отсутствие криптовалюты не позволит нам сделать правильный выбор относительно природы блокчейн-проекта, следовательно, критерий не может быть правильным с точки зрения классификации.

Сложно согласиться и с другим утверждением того же автора о том, что в нефинансовых проектах блокчейн представляет собой «лишь инфраструктуру для хранения, распространения и передачи информации»[4].

Блокчейн независимо от сферы применения всегда является лишь вспомогательной технологией: способом хранения и обработки информации. И.Т. Булгаков был бы прав, если бы у криптовалют было

---

[1] *Булгаков И.Т.* Правовые вопросы использования технологии блокчейн // Закон. 2016. № 12. С. 80–88.

[2] *ICO* подразумевает выпуск криптовалюты с предложением обменять новую криптовалюту на уже существующие криптовалюты. Подобная сделка может быть мотивирована высокой перспективностью, а как следствие, и окупаемостью проекта, авторы которого прибегли к *ICO*. Проект получает финансирование, а лица, обменявшие свою валюту, получают прибыль на увеличении курса криптовалюты в связи с развитием проекта.

[3] Например, *Ethereum*: проект собрал с помощью краудфандинга 20 млн долл. и использует эту валюту в качестве расчетной единицы за пользование ресурсом.

[4] *Булгаков И.Т.* Правовые вопросы использования технологии блокчейн. С. 84

одноцелевое использование. А так как криптовалюты в разных блокчейн-технологиях применяются для достижения различных целей (от расчетной единицы до привлечения капитала (*ICO*)) и имеют разный вид и способ использования, то нельзя применять столь неустойчивый критерий для классификации видов блокчейна.

Для понимания эволюции блокчейна самым верным будет опираться на характеристику, предложенную Мелани Свон, которая выделяет несколько уровней развития блокчейна по критерию технических возможностей[1], выделяя блокчейн 1.0, Блокчейн 2.0, Блокчейн 3.0.

Блокчейн 1.0 – «как валюта» представляет собой платформу для реализации платежных систем, основанных на простейшем цифровом активе – криптовалюте. Первым и наиболее популярным примером реализации этой технологии стал биткоин. Со временем появились другие криптовалюты, основанные на схожих алгоритмах. Их стали называть альткоины (альтернативы биткоину). Функционал этого блокчейна ограничен сценарным языком, который, как правило, не обладает полнотой по Тьюрингу[2], поэтому лишен возможности осуществлять сложные действия.

Блокчейн 2.0 – «как контракт» явился закономерным следствием развития блокчейна 1.0. Эпоха блокчейна 2.0 неразрывно связана с проектом *Ethereum*. Основатель проекта Виталик Бутерин обратил внимание на недостатки предыдущей модели и усовершенствовал ее. Главным новшеством стало появление цифрового актива – «токена», который не определен заранее и может быть изменен в зависимости от конкретных предпочтений пользователя. Также протокол блокчейна *Ethereum* написан на языке *Solidity*, который является тьюринг-полным. Эти модификации ознаменовали появление такого феномена, как смарт-контракты, использование которых позволяет обменивать согласованный сторонами цифровой актив, привязанный к токену, на определенную криптовалюту.

[1] *Свон Мелани.* Блокчейн. Схема новой экономики / пер. с англ. М.: Олимп-Бизнес, 2017.

[2] Тьюринг-полнота – в теории вычислимости, тьюринг-полным называется исполнитель, если он может вычислить любую вычислимую функцию. Простыми словами, тьюринг-полнота подразумевает способность к выполнению всех действий, предусмотренных математической логикой. Сценарный язык биткоина способен на проведение лишь самых примитивных операций, язык *Solidity* (видоизмененный *Javascript*) позволяет вводить сложные циклы и т.д., существенно увеличивая возможности данной технологией. Подробнее: *T. Neary*, *D. Woods*. Four small universal Turing machines. Fundamenta Informaticae, 91(1):123–144, 2009.

Блокчейн 3.0 – «как децентрализованное приложение» представляет собой абсолютно новую веху в технологиях. Мелани Свон дает интригующее определение: «децентрализованное приложение – это приложение, которое работает в сети распределенным образом при этом информация об участниках надежно защищена, а выполнение операций децентрализовано в разных узлах сети»[1]. В качестве рабочих экземпляров уже действуют *OpenBazaar*[2] (децентрализованный *Craiglist*), *LaZooz*[3] (децентрализованный *Uber*).

Исторически блокчейн был неразрывно связан с биткоином и рассматривался как его уникальное свойство. Действительно, основы блокчейна и биткоина были впервые описаны в знаменитой публикации Сатоши Накомото. Однако возможное применение блокчейна гораздо перспективнее, чем биткоин. Биткоин – одна из многих криптовалют, хотя и самая популярная из них. Блокчейн, в свою очередь, представляет собой основу функционирования биткоина, но не ограничивается им. Следовательно, биткоин – это ответ на вопрос «что?», блокчейн – «как?».

Функционирование блокчейна (на примере биткоина)

Для начала работы с биткоином необходимо установить биткоин-кошелек. Существует огромное количество способов, как это сделать: от скачивания самого блокчейна биткоина, содержащего все транзакции (весом около 100 ГБ на момент написания настоящей статьи), до подключения к биткоин-приложению[4], в котором память устройства не используется для сохранения транзакций. Сам биткоин-кошелек генерируется путем создания пары ключей: публичного (открытого) и приватного (закрытого).

Публичный ключ является идентификационным (уникальным) номером. Размещение его в открытом пространстве неспособно повлечь какие-либо угрозы для пользователя. Ситуация во многом аналогична

[1] *Свон Мелани*. Схема новой экономики / пер. с англ. М.: Олимп-Бизнес, 2017.

[2] *OpenBazaar* – платформа децентрализованной торговли, позволяющая заключать сделки купли-продажи без посредников, т.е. напрямую с продавцами, и поощряющая торговлю под псевдонимами (подробнее: URL: https://openbazaar.org/).

[3] *LaZooz* – платформа децентрализованного поиска и предложения услуг по перевозке «децентрализованное такси» (подробнее URL: http://lazooz.org/).

[4] На данном сайте можно выбрать удобный биткоин-кошелек (URL https://bitcoin.org/ru/choose-your-wallet).

сбору средств на счет, когда другие участники системы имеют возможность пополнить счет, но не взломать. Уникальность публичного ключа позволяет выдвигать смелые предположения относительно его использования. Ряд ученых Принстонского университета предлагают в будущем приравнять публичный ключ к личности человека (*identities*) в возможных децентрализованных системах[1].

Публичный ключ не работает без приватного ключа. Размещение приватного ключа в общем доступе приведет к немедленному списанию средств с кошелька, что было проверено автором настоящей статьи на собственном опыте. Потеря приватного ключа является потерей доступа к счету, нет никаких способов восстановить приватный ключ. Это можно считать одним из недостатков системы.

Транзакцией в биткоине принято называть запись о том, что с конкретного счета списано и на другой публичный ключ записано определенное количество биткоинов. И эта транзакция валидна только после подписи данной записи приватным ключом передающего. Без подписи приватным ключом любые транзакции не будут одобрены вычислительной частью системы – майнерами (англ. *Mining* – добыча) и, соответственно, не попадут в блокчейн.

После совершения транзакции сама транзакция транслируется на всю одноранговую сеть биткоина, позволяя другим узлам «увидеть» транзакцию, и именно эта «публичность» сводит риск атаки двойной траты к нулю.

Транзакции объединяются узлами в блоки, после чего посредством распределенного консенсуса[2] достигается соглашение насчет валидности транзакции, и блок вписывается в цепочку – в блокчейн. Атака «двойной траты», т.е. одновременная отправка биткоинов на два адреса не представляет угрозы. Это объясняется тем, что, поскольку одна из транзакций, которая «вписана» в блокчейн, станет валидной, то следующая за ней транзакция злоумышленника не подтвердится консенсусом, так как будут отсутствовать данные

[1] Биткоин и криптовалютные технологии: лекции Пристонского университета (http://forklog.com/opublikovan-perevod-lektsij-prinstona-o-kriptografii-tsifrovyh-valyut/).

[2] Распределенный консенсус представляет собой соглашение, принятое всеми участниками сети по поводу одного конкретного события. Распределенный консенсус вносит в блокчейн «демократический» элемент, так как без него невозможно принятие решения о внесении в сам блокчейн определенного блока. Благодаря распределенному консенсусу технология блокчейн пользуется доверием среди пользователей, которые не знают друг друга.

о наличии денег на счете, которые уже были списаны в результате первой транзакции.

Блокчейн представляет собой цепочку блоков. Ключевая ценность этой цепочки в том, что каждый блок неразрывно связан со следующим блоком. Сам блок состоит из подтвержденных транзакций и криптографической подписи (хеш-указатель), которая содержит в себе данные предыдущего блока. Если злоумышленник захочет изменить или удалить транзакцию, ему придется менять все остальные блоки в системе, что практически невозможно ввиду огромной вычислительной мощности компьютеров, обслуживающих систему. Образно говоря, блокчейн похож на прошитые ниткой пронумерованные листы бумаги: невозможно незаметно выдернуть или подменить лист, не порвав нитку.

Вычислительная мощность блокчейна представляет собой «ноды» (минимальные компьютерные единицы). Пользователей, которые предоставляют свою вычислительную мощность, называют «майнеры». Их деятельность система поощряет биткоинами, что можно назвать «эмиссией» биткоинов, так как они возникают впервые.

Майнинг в биткоине осуществляется децентрализованно. В его основе лежит принцип *proof-of-work* (*PoW* – доказательство работы)[1], который приводит к тому, что ноды конкурируют за то, чтобы обрабатывать транзакции и вписывать их в блокчейн. Этим обеспечивается достаточно высокая скорость работы, стабильность и достоверность системы. Для того чтобы вычислительной работой занимались не только энтузиасты, система биткоина предоставляет определенные блага: от награды (определенного актива) за блок до процентов с подтвержденных и закрепленных в блокчейне транзакций.

В связи с этим сейчас майнинг превратился в профессиональную деятельность, которая осуществляется либо путем установки огромных вычислительных мощностей в районах с дешевым электричеством (майнинг фермы), либо организацией сообщества майнеров, которые

[1] *Proof-of-work* не является единственным принципом защиты распределенных систем от злоупотребления. Его конкурентом является принцип *proof-of-stake* (*PoS* – доказательство доли), который подразумевает, что будет вписан в блокчейн не тот блок, учетная запись которого будет располагать бóльшими вычислительными мощностями (*proof-of-work*), а блок, учетная запись которого будет содержать бóльшее количество средств на счету. Стоит отметить, что в настоящий момент популярные криптовалюты (*EmerCoin*, *NovaCoin*, *YaCoin*, *PeerCoin* и *Reddcoin*) используют *PoS* и *PoW* одновременно.

объединяют мощности своих компьютеров, а потом пропорционально этой мощности распределяют награды за блок (майнинг-пул). Непрофессиональные (одиночные) майнеры уже достаточно редки, так как убытки, понесенные из-за майнинга (время, электроэнергия) становятся больше возможного вознаграждения.

Можно выделить следующие основные характеристики блокчейна.

1. Децентрализованный характер

Блокчейн представляет собой структуру, в которой нет единицы управления. Причем децентрализованность присутствует на всех этапах совершения транзакции. На этапе совершения транзакций невозможно внутрисетевое принуждение к совершению транзакции, а также отмена транзакции другим участником сети. На этапе подтверждения и внесения транзакции в блокчейн майнеры на абсолютно равных условиях конкурируют друг с другом, что лишает их какой-либо власти в отношении пользователей. Распределенный консенсус[1] с философской точки зрения представляет собой реализованный принцип абсолютной демократии, который предполагает принятие ключевых вопросов относительно самой системы только при одобрении абсолютным большинством пользователей.

2. Криптографические алгоритмы как основа доверия между участниками системы

С помощью хеш-функций, *proof-of-work*, ассиметричного шифрования уровень доверия между участниками системы достигает своего предела. Возможность взлома блокчейна сведена к минимуму, хотя такие разновидности хакерских угроз, как «Атака 51 процента»[2] или «Атака Сивиллы»[3], остаются потенциальной угрозой для блокчейна. Распределенный консенсус является в данном случае наиболее приоритетной целью для атакующих.

3. Автономность

Основы функционирования блокчейна заложены в его программном коде, который представляет собой программное обеспечение с открытым кодом. Данное качество позволяет существенно повысить уровень доверия, так как каждый участник может ознакомиться

[1] *Савельев А.И.* Договорное право 2.0: «Умные» контракты как начало конца классического договорного права // Вестник гражданского права. 2016. № 3. С. 32–59.

[2] При контроле более половины вычислительной мощности одним злоумышленником нарушается принцип распределенного консенсуса.

[3] Создание большого количества личностей (*identities*) для искажения распределенного консенсуса.

с «конституцией» блокчейна и быть уверенным, что она будет изменена только при достижении консенсуса между большинством участников этой системы. Нельзя не заметить, что подобное ознакомление требует высокой профессиональной подготовки в области программирования и криптографии, однако само наличие этой возможности можно считать прорывом в сфере развития высоких технологий[1].

Общие проблемы в блокчейне

При поверхностном рассмотрении практически любого правового явления возникает желание назвать предмет исследования вещью своего, особого рода (*sui generis*). Однако при более детальном анализе можно рассмотреть пример аналогичных технологий, к которым уже выработано техническое регулирование и определенное понимание.

Как можно было понять из технического описания блокчейна, сам блокчейн – это всегда производная технология. Она может быть использована в платежных системах, реестрах, банковских расчетах. Однако она не является самодостаточной технологией: с точки зрения права интерес имеет цифровой актив, который подлежит обмену в блокчейне, а сам блокчейн лишь задает определенные технические свойства, которые нужны юристам для разграничения блокчейна и сходных технологий.

Обмен данными в блокчейне невозможен без сети: для совершения транзакции необходимо взаимодействие двух устройств, наличие двух встречных сигналов, т.е. коммуникации, поэтому мы можем смело констатировать: блокчейн всегда работает при помощи компьютерных сетей, которые можно определить как информационную связь между двумя компьютерами[2].

Логически верным, на взгляд автора, является рассмотрение всех особенностей блокчейна внутри всех возможных компьютерных сетей, но стоит отметить низкую эффективность подобного анализа.

Использование компьютерных сетей обусловлено решением различного рода задач. Локальные сети, такие как *BAN* (*Body Area Net-*

[1] *Савельев А.И.* Лицензирование программного обеспечения в России. Законодательство и практика. М.: Инфотропик Медиа, 2012. С. 335.

[2] *Олифер В., Олифер Н.* Компьютерные сети. Принципы, технологии, протоколы: учебник для вузов. СПб.: Питер, 2016. С. 44.

work), *PAN* (*Personal Area Network*), *LAN* (ЛВС, *Local Area Network*), *CAN* (*Campus Area Network*), *MAN* (*Metropolitan Area Network*) подразумевают наличие определенной хозяйственной цели. Именно эта цель обусловливает их архитектуру, доступ, а также взаимоотношения пользователей сети. Поэтому в данном случае уместна аналогия с моделями обслуживания облачных сервисов: платформа как услуга (*Platform-as-a-Service*), инфраструктура как услуга (*Infrastructure-as-a-Service; IaaS*). Облачные технологии и блокчейн в данных моделях призваны решать определенные узкоцелевые задачи, такие как развертывание разработанных приложений на платформе, предоставленной провайдером (*PaaS*), или организация документооборота на предприятии[1]. Поэтому блокчейн, используемый в подобных компьютерных сетях, является технологическим свойством уже существующих и определенных отношений между пользователями, взаимодействующими внутри этой сети. В связи с этим использованию блокчейна в данных сетях будет уделено меньше внимания.

Особый интерес вызывает использование блокчейна внутри глобальных сетей, таких как Интернет.

И.М. Рассолов из решения Верхового суда США от 11.07.1996 приводит следующее: «Интернет – глобальное объединение компьютерных сетей и информационных ресурсов, не имеющих четко определенного собственника и служащих для интерактивного соединения (коммуникации) физических и юридических лиц»[2]. Регулирование отношений внутри сети Интернет является наиболее интересным, перспективным и неизученным с точки зрения правовой науки.

В.В. Архипов указывает, что в случае с любыми правоотношениями, возникающими в информационно-телекоммуникационных сетях, возникают три общие правовые проблемы. К ним он относят: 1) проблему идентификации пользователей, 2) проблему информационных посредников, 3) проблему определения юрисдикции[3].

Помимо названных проблем, В.В. Архипов выделяет ряд частных проблем, которые присутствуют не во всех отношениях, опосредуемых сетью Интернет. Применительно к блокчейну актуальными признаются две частные проблемы – проблема пиринговых технологий

[1] *Савельев А.И.* Правовая природа «облачных» сервисов: свобода договора, авторское право и высокие технологии // Вестник гражданского права. 2015. № 5.

[2] *Рассолов И.М.* Право и Интернет. Теоретические проблемы. М.: Норма, 2009.

[3] *Архипов В.В.* Интернет-право: учебник и практикум для бакалавриата и магистратуры. М.: Юрайт, 2016. С. 48.

и проблема автоматизированных действий. Эти проблемы обусловлены технологическими особенностями блокчейна.

Обозначенные проблемы можно прокомментировать следующим образом.

1. Проблема определения юрисдикции. Блокчейн является платформой с открытым исходным кодом: для его успешного использования необходимо лишь «запустить» этот код. Транзакции, совершенные в блокчейне, находятся внутри цепочки блоков, которая распределена между всеми участниками блокчейна, т.е. сам блокчейн трансграничен – границы блокчейна простираются до границ Интернета. Проблема определения юрисдикции заключается не в отсутствии нормативного материала, а, напротив, в том, что «Интернет является не архаичным пространством, а самым «зарегулированным местом в мире»[1]. При наличии большого количества нормативного материала вопрос об определении юрисдикции в блокчейне не является особо проблемным, а скорее подлежит осмыслению в контексте применения различных, уже выработанных доктрин, например, в рамках доктрины минимальных контактов[2].

2. Проблема ответственности информационных посредников также может представлять особый интерес в рамках блокчейна. В сочетании с упоминаемой выше проблемой пиринговых технологий ответственность проявляется наиболее остро. Однако неясно, о каких информационных посредниках идет речь при *P2P-* (*peer-to-peer* – от равного к равному (англ.)) технологии. Информационным посредником в блокчейне (поскольку блокчейн – одноранговая сеть) будет по сути каждый пользователь, на компьютере которого будет содержаться блокчейн. В связи с этим, как справедливо отмечает В.В. Архипов, подобное утверждение может вызвать огромные затруднения на практике. По мнению автора настоящей статьи, по этому вопросу современная отечественная система регулирования отношений в сети Интернет довольствуется отдельными и недостаточно эффективными[3] запретами, а также единичными случаями привлечения к ответственности[4].

[1] *Савельев А.И.* Электронная коммерция в России и за рубежом: правовое регулирование. М.: Статут, 2016.

[2] *Барнашов А.М.* Экстерриториальная юрисдикция в США: доктрина «минимальных контактов» // Российская юстиция. 2000, май.

[3] Lenta.ru. 2016. 17 февр. (URL: https://lenta.ru/news/2016/02/17/medvedrutracker/ (дата обращения: 30.01.2017)).

[4] Решение № 1-226/13–15.10.2013. Тимирязевский районный суд г. Москвы.

В ситуации с блокчейном, в котором соотнести личность пользователя и публичный ключ нельзя с абсолютной уверенностью, проблема приобретает больший масштаб.

Самостоятельной проблемой становится ситуация, когда в блокчейн включается запрещенный актив (например, объект, распространение которого нарушает авторские права другого лица, хотя есть и более курьезные реальные примеры злоупотреблений[1]). Одним из наиболее эффективных способов решения данной проблемы может стать повышенная ответственность майнеров. В пользу этого вывода можно выдвинуть следующие аргументы.

Во-первых, майнеры – профессионалы в сфере обработки транзакций и поддержания функционирования блокчейна. Ситуацию, когда сами пользователи являются майнерами, рассматривать нет оснований, поскольку здесь налицо признаки исполнителя противоправного деяния. Наибольший интерес вызывает ситуация (а в блокчейне статистически это наиболее частый случай), когда майнеры и пользователи блокчейна разделены. Это обусловлено профессионализмом работы, а также определенными имущественными затратами на майнинг, вследствие чего майнинг становится невыгодным самим пользователям. При этом в зависимости от характера майнинга и статуса майнеров (профессиональный или непрофессиональный) можно будет устанавливать стандарт осмотрительности, а также дифференцировать ответственность для майнера на виновную или безвиновную. При этом природа ответственности будет коррелировать с природой правонарушения (при нарушении гражданских прав – гражданская ответственность, уголовных норм – уголовная и т.д.).

Во-вторых, майнеры имеют наиболее четкое представление относительно актива в блокчейне, который они поддерживают. Именно выбором актива обусловлена их деятельность и предпочтение поддержки именно этого блокчейна, а не другого. В ситуации аренды у одного юридического лица серверов для майнинга ответственность в случае правонарушении для арендатора будет устанавливаться в соответствии с принципами добросовестности, осмотрительности и др.

[1] Была попытка создать «биржу убийств» (подробнее: URL: https://cryptochan.org/birzha-ubijstv-assassination-market-prinimaet-zakazy-za-bitcoin/) – аукцион, на котором пользователи собирают в порядке свободного волеизъявления сумму на убийство какого-либо лица. Как только сумма становится приемлемой для киллера, тот делает ставку. Если в течение какого-либо времени распределенным консенсусом подтверждается смерть этого лица, на указанный киллером кошелек приходит скопленная сумма.

В-третьих, при привлечении к ответственности майнеров обработка блокчейна будет усложнена, поэтому попытки пресечь дальнейшие действия в блокчейне станут эффективными. Напротив, при привлечении к ответственности пользователей, количество обрабатываемого материала сокращается и блокчейн начинает функционировать еще лучше. Если в случаях с торрентами объекты, нарушающие авторские права, размещаются на конкретных компьютерах пользователей и их распространение может быть пресечено удалением, то применительно к блокчейну пресечение правонарушения возможно только при привлечении к ответственности майнера.

В-четвертых, стоит отметить, что на сегодняшний день существуют возможности борьбы с распространением нелегального контента. Видами этой борьбы может являться перезапись блока, содержащего запрещенные к распространению данные, или внутриблокчейновая верификация контента. Таким образом, у добросовестных майнеров есть возможности для пресечения правонарушений в блокчейне. А так как они еще в большей части являются профессионалами, осуществление подобных мер можно возлагать на них.

Несомненно, если у правоохранительных органов появятся возможности привлечения именно исполнителей преступления и правонарушителей к ответственности, это будет наиболее оптимальным решением. Но на сегодняшнем этапе можно исходить из презумпции, что именно майнер имеет наибольшие возможности в блокчейне, порождающие и сопоставимую ответственность. Эти обстоятельства могут учитываться при разработке правовой регламентации деятельности майнеров.

3. Проблема идентификации пользователей характерна для всего виртуального мира, и блокчейн не стал исключением. Однако наличие и сочетание двух ключей публичного и приватного – может стать презумпцией идентичности личности, владеющей двумя ключами (владеть – иметь информационный доступ) в реальной жизни, и лица, использующего эти ключи при совершении транзакции.

4. Проблема автоматизированных действий будет рассмотрена далее – при разборе смарт-контрактов в контексте договорного права.

Смарт-контракт в договорном праве

Прежде всего следует сделать оговорку: понятия смарт-контракта и договора пересекаются лишь частично. Смарт-контракт – это

программный код, управляющий определенным активом. Квалификация отношений, опосредуемых смарт-контрактом, невозможна без понимания актива, используемого в этом смарт-контракте. Поэтому определение, данное А.И. Савельевым, согласно которому смарт-контракт – это «договор, существующий в форме программного кода»[1], верно лишь отчасти.

В качестве иллюстрации допустимо сослаться на смарт-контракт, с помощью которого производится голосование в блокчейне между пользователями. Активом данного смарт-контракта будет являться голос – *vote*.

Так как, приоритетным с позиций исследования является рассмотрение смарт-контракта с точки зрения гражданского права, то автор будет рассматривать и приводить примеры исключительно из гражданско-правовой сферы.

Рассмотрим основные аспекты смарт-контракта как договора.

Смарт-контракт представляет собой протокол, написанный на каком-либо языке программирования, функционирующий в блокчейне, который обеспечивает автономность и самоисполнимость условий такого договора по наступлении заранее определенных в нем обстоятельств[2].

Главные тезисы о смарт-контракте в договорном праве:

1. Невозможно удалить или изменить смарт-контракт с момента загрузки в блокчейн. При активации смарт-контракта в блокчейн-клиенте код закрепляется внутри блока и становится внутри структуры блокчейна.

2. Автоматизированность исполнения: смарт-контракт будет заключен не только при согласовании воль, но по своей природе он будет заключен только в том случае, если у пользователей, достигших соглашения, будет возможность одновременного исполнения смарт-контракта. В соответствии с этим можно сделать вывод, что на сегодняшний день с помощью смарт-контрактов возможен лишь оборот тех объектов, в рамках которых компьютер может «оценить» наличие их исполнения. Необязательно, чтобы исполнение происходило в рамках блокчейна, важно, чтобы программа могла проверить исполнение (например, передача вещи и установ-

[1] *Савельев А.И.* Договорное право 2.0: «Умные» контракты как начало конца классического договорного права // Вестник гражданского права. 2016. № 3. С. 32–59.

[2] Там же.

ка факта прибытия в место исполнения с помощью меток). Таким образом, автор делает вывод – все, что способна «принять» в качестве исполнения вычислительная машина, может быть предметом смарт-контракта.

3. Сохранение и применение большинства выработанных по отношению к договорному праву подходов по отношению к смарт-контракту. А.И. Савельев указывает, что большинство концепций договорного права, таких как обязательство, неисполнение или ненадлежащее исполнение, по отношению к смарт-контрактам неприменимо. Он пишет: «Поскольку одним из ключевых элементов обязательства является его направленность в будущее и последующие волевые действия (бездействие) обязанного лица по его исполнению, в ситуации, когда соответствующие условия исполняются самим компьютером, утрачивает значение и само понятие «обязательство». В «умном» контракте имеют значение операции компьютера, а не поведение должника, которое является ядром понятия «обязательство»[1]. А.И. Савельев также утверждает, что «любое исполнение, произведенное программным кодом, будет считаться «надлежащим», в связи с чем данное понятие само по себе утрачивает смысл, поскольку ненадлежащего исполнения в рамках «умного» контракта быть не может»[2].

Такой подход представляется неверным. Смарт-контракт есть лишь способ реализации гражданских прав, а гражданские права, как и право в целом, живут своей жизнью и представляют вид и меру должного поведения людей. Смарт-контракт – способ осуществления гражданских прав. И если хозяйственная цель, которую ставило лицо при вступлении в смарт-контракт, не была достигнута ввиду, например, умышленных действий контрагента, то такое лицо имеет право на защиту гражданских прав. Условно говоря, если посредством смарт-контракта был передан «битый» (не поддающийся расшифровке) файл, разве обязательство передать файл можно признать исполненным? Разве только смарт-контракт должен определять, исполнено или не исполнено обязательство? Или это работа судьи?

Можно привести сравнение смарт-контракта с морским кораблем. Если должник кому-либо обязался передать товар, а в качестве

[1] *Савельев А.И.* Договорное право 2.0: «Умные» контракты как начало конца классического договорного права // Вестник гражданского права. 2016. № 3. С. 32–59.

[2] Там же.

способа перевозки должник выбрал отправление по морю. С точки зрения факта должник никак не способен повлиять на исполнение с момента поднятия кораблем якоря, и его у контрагента не будет фактической возможности потребовать надлежащего исполнения непосредственно при передаче товара. Однако если исполнение, предложенное должником, будет ненадлежащим, то кредитор будет иметь весь арсенал прав, чтобы потребовать защиты своих нарушенных прав в суде.

4. С позицией А.И. Савельева можно согласиться только в одном случае: если при привязке актива к токену блокчейн верифицирует актив как валидный, то можно рассматривать смарт-контракт как способ исполнения обязательств, выбранный сторонами. При таком понимании смарт-контракта появляются достаточно перспективные и интересные возможности для внедрения технологии в юридическую практику. Например, включение в ГК РФ параграфа про автоматизированное исполнение обязательств было бы не менее интересным, чем другая недавняя законодательная инициатива о роботах[1].

5. Знаковым для правового регулирования в электронной коммерции является понятие «электронный агент»[2], применительно к которому уже выработаны законодательные правила и сложилась некоторая практика. Смарт-контракт является видовым понятием электронного агента, из чего следует, что подавляющее число норм, подлежащее применению в электронной коммерции, распространяется и на смарт-контракты.

6. Ответственность за неисполнение условий. В данном случае уместно не придумывать новые подходы, а ограничиваться существующим. Если одно из встречных предоставлений происходит посредством совершения транзакции в блокчейне, то ответственность за неисполнение или просрочку несет сторона, выбравшая совершение транзакций в блокчейне как способ исполнения. По мнению автора настоящей статьи, взлом и подмена транзакций будут считаться непреодолимой силой в соответствии с положениями ст. 401 ГК РФ, поскольку архитектура блокчейна подразумевает невозможность совершения подобных действий. А иные обстоятельства («Атака 51%»

[1] См.: http://www.dentons.com/ru/insights/alerts/2017/january/27/dentons-develops-first-robotics-draft-law-in-russia

[2] *Савельев А.И.* Электронная коммерция в России и за рубежом: правовое регулирование. М.: Статут, 2016.

или сбой самого смарт-контракта) не могут рассматриваться как чрезвычайные и непредотвратимые обстоятельства.

Заключение

Блокчейн, бесспорно, обладает рядом неоспоримых достоинств. Однако у него есть и недостатки, которые со временем станут препятствием для масштабного распространения блокчейна. Недостатки – это оборотная сторона достоинств блогчейна, поэтому можно говорить о том, что сила блокчейна есть его слабость.

Среди недостатков блокчейна автор настоящей статьи выделяет следующие:

Пиринговая система. Именно отсутствие единицы, наделенной административно-распорядительными или организационными полномочиями в блокчейне, станет основным препятствием для его внедрения. Невозможность отменить совершенную транзакцию или, наоборот, заставить принудительно совершить ее может отпугнуть большую часть рынка в связи с тем, что выработанное законодательство относительно недействительности сделок предоставляет какую-либо защиту слабым сторонам. В блокчейне нет слабых сторон – там все равны, а это означает, что пользователь блокчейна принимает на себя повышенные риски. Это позволяет скептически отнестись к возможному будущему «децентрализованному правительству», упоминаемому в книге Мелани Свон[1].

Использование блокчейна для реестров также вызывает сомнение. Любой реестр должен быть приспособлен к принудительному изменению, но пиринговые технологии не позволяют совершение подобных действий.

Таким образом, в любых отношениях, в которых присутствует необходимость в элементе управления, применение блокчейна вызовет большие трудности. Высказанная А.И. Савельевым идея о «суперпользователе», под которым он понимает лицо, обладающее «особыми полномочиями по пересмотру содержимого реестра *Blockchain*»[2], является решением проблемы, но одновременно с этим разрушает ценность блокчейна как децентрализованной системы.

---

[1] *Свон Мелани*. Блокчейн. Схема новой экономики / пер. с англ. С. 113.

[2] *Савельев А.И.* Договорное право 2.0: «Умные» контракты как начало конца классического договорного права // Вестник гражданского права. 2016. № 3. С. 38.

Технология блокчейна как программного кода может создать условия для различного рода злоупотреблений. Не стоит забывать и вопиющие случаи провалов блокчейн-проектов, связанных с ошибкой в коде (например, проект *TheDAO*). Невозможность предусмотреть все в процессе подготовки смарт-контракта в сочетании с его дальнейшей неизменностью вызывает отторжение, так как подобная «негибкость» скорее вредит, усложняет оборот. Поэтому перспектива создания масштабных приложений эпохи *Blockchain* 3.0 выглядит довольно туманной.

Доверие к блокчейну, а не к его пользователям. Благодаря математическим алгоритмам блокчейн увеличивает доверие к системе. Однако если блокчейн будет предназначен для обработки какого-либо актива, то, если один из пользователей будет скомпрометирован, будет скомпрометирован весь реестр. Например, если в реестр кредитных историй, который ведут все банки, один из банков будет вносить ложные данные, то скомпрометированным окажется весь реестр, что невозможно исправить.

Среди сфер, в которых использование блокчейна является наиболее эффективным, является оптимизация бизнес-процессов внутри предприятия или внутри бизнес-экосистемы. Например, банкам выгодно создание децентрализованного реестра, так как они склонны доверять друг другу (да и с точки зрения правового режима находятся в равном положении).

Невозможно предсказать все последствия применения и распространения блокчейна, но одно можно сказать точно: эта технология имеет право быть объектом исследования и имеет право быть предметом законодательного регулирования. Попытки регулирования отношений с использованием технологии блокчейн предпринимались уже неоднократно. Например, принят закон о «битлицензиях» (*BitLicense*) в Нью-Йорке, который фактически приравнял операции с биткоином к финансовым переводам, установил правила для компаний, которые используют биткоин для расчетных операций[1].

В то же время в Европейском союзе было запрещено проведение нерегулируемых *ICO*[2]. Инициатива связана с большим риском злоупо-

[1] См.: http://www.dfs.ny.gov/legal/regulations/adoptions/dfsp200t.pdf

[2] См.: http://forklog.com/evrosoyuz-zakryvaet-vozmozhnost-provedeniya-nereguliruemyh-kriptovalyutnyh-ico/

треблений при проведении, а также борьбой с отмыванием денежных средств или финансированием терроризма.

Это неполный список уже реализованных попыток законодателя урегулировать отношения по использованию блокчейна, но чаще всего они связаны с превентивными мерами по недопущению нарушений закона (в основном уголовного) или применению ответственности. Между тем необходимо регламентировать использование блокчейна, поскольку существует высокая вероятность того, что будет представлять собой очень востребованный продукт.

Пристатейный библиографический список:

1. *Satoshi Nakamoto*. Bitcoin: A Peer-to-Peer Electronic Cash System (URL: www.bitcoin.org).

2. *Архипов В.В.* Интернет-право: учебник и практикум для бакалавриата и магистратуры / В.В. Архипов. М.: Юрайт, 2016.

3. *Архипов В.В.* Публикация в информационном портале «Закон.ру» (URL: https://zakon.ru/blog/2014/1/13/bitcoin_osnovnye_principy_i_otdelnye_yuridicheskiznachimye_osobennosti (дата обращения: 31.01.2017)).

4. Биткоин и криптовалютные технологии: лекции Пристонского университета (URL: «http://forklog.com/opublikovan-perevod-lektsij-prinstona-o-kriptografii-tsifrovyh-valyut).

5. *Булгаков И.Т.* Правовые вопросы использования технологии блокчейн // Закон. 2016 № 12. С. 80–88.

6. *Олифер В., Олифер Н.* Компьютерные сети. Принципы, технологии, протоколы: учебник для вузов. 5-е изд. СПб.: Питер, 2016.

7. *Рассолов И.М.* Право и Интернет. Теоретические проблемы. 2-е изд., доп. М.: Норма, 2009.

8. *Савельев А.И.* Договорное право 2.0: «Умные» контракты как начало конца классического договорного права // Вестник гражданского права. 2016. № 3.

9. *Савельев А.И.* Электронная коммерция в России и за рубежом: правовое регулирование. М.: Статут, 2016.

10. *Савельев А.И.* Правовая природа «облачных» сервисов: свобода договора, авторское право и высокие технологии // Вестник гражданского права. 2015. № 5.

11. *Савельев А.И.* Лицензирование программного обеспечения в России. Законодательство и практика. М.: Инфотропик Медиа, 2012.

12. *Свон Мелани*. Блокчейн. Схема новой экономики / пер. с англ. М.: Олимп-Бизнес, 2017.

К.В. Нам

ПРАВОВОЕ РЕГУЛИРОВАНИЕ РЕГИСТРАЦИИ И ИСПОЛЬЗОВАНИЯ ДОМЕННОГО ИМЕНИ В ГЕРМАНИИ

Аннотация. *Право Германии не содержит специальных кодифицированных норм, призванных регулировать отношения в сфере доменных имен. Правовое регулирование осуществляется с помощью общих норм, регулирующих схожие отношения. Большое значение для регулирования соответствующих вопросов имеет судебная практика. В статье помимо положений немецкого законодательства рассматриваются правовые подходы в регулировании доменных имен, сформированные судебной практикой.*

Ключевые слова: *Интернет, доменные имена, правовое регулирование, право Германии.*

Деятельность пользователей Интернета может быть как пассивной, так и активной с точки зрения пользования только чужими сайтами и платформами или же создания собственных сайтов или порталов.

Для активных пользователей Интернета, создающих свой сайт, одним из первых встает вопрос выбора правильного доменного имени. Здесь возникают разнообразные правовые вопросы, связанные с учетом прав на уже существующие наименования и обозначения, защитой собственного доменного имени от регистрации третьими лицами схожих до степени смешения обозначений, а также многие другие. В связи с этим вопросы правового регулирования регистрации и использования доменного имени для так называемых активных пользователей Интернета являются весьма актуальными, представляют для них практический интерес.

В настоящей статье будут рассмотрены подходы немецкого права к вопросам регулирования регистрации и использования доменных имен. Данное направление права в Германии, как и в других странах, имеет большое значение в силу бурного развития Интернета[1] и возникающих в связи с этим правовых вопросов.

[1] Согласно статистическим данным число пользователей Интернета в Германии выросло с 2001 по 2016 г. с 37 до 79% от общего числа населения (https://de.statista.

Правовое регулирование вопросов, связанных с доменными именами, в Германии, как и во многих других странах, не кодифицировано в отдельном специальном законодательном акте, а осуществляется в соответствии с общими нормами, регулирующими права на имя, наименование (§12 *BGB*), права на обозначения (§ 14, 15 *MarkenG*), вопросы недобросовестной конкуренции (§ 3–5 *UWG*), а также деликтным правом (§ 823, 826 *BGB*).

Значительная роль в регулировании вопросов, связанных с доменными именами, в Германии признается за судебной практикой. Как подчеркивается в литературе, доменные споры уже стали в немецких судах рутинным делом[1]. После длительной фазы правовой неопределенности в начальной стадии развития Интернета многие проблемы в сфере обозначений и недобросовестной конкуренции были решены именно на уровне судов. В настоящее время имеются уже десятки решений Верховного суда Германии и сотни решений нижних инстанций.

Понятие и правовая природа доменного имени

Все интернет-ресурсы (сайты, домашние страницы, порталы, социальные сети и т.д.) упорядочены в сети под своими доменами – это необходимо для того, чтобы они были технически и фактически доступны. Чтобы загрузить тот или иной интернет-сайт, необходимо набрать доменное имя (ввести определенный *URL*-адрес). Поэтому можно говорить о том, что домен выполняет те же задачи, что домашний адрес, почтовый адрес при почтовом отправлении или телефонный номер при телефонном разговоре[2].

Помимо функции адресации, являющейся в большей степени технической функцией доменного имени, выделяют еще идентификационную функцию. Доменные имена могут быть сформированы не только из набора различных знаков, но и из имен, слов и даже целых выражений, тем самым они могут быть легче использованы в рекламных целях. Восприятие ключевых слов или запоминающихся выражений в доменных именах позволяет говорить об идентификационных

com/statistik/daten/studie/13070/umfrage/entwicklung-der-internetnutzung-in-deutschland-seit-2001/).

[1] *Bettinger Torsten*. Handbuch des Domainrechts. Nationale Schutzsysteme und internationale Streitbeilegung. München, 2008. S. 71.

[2] *Haug Volker*. Internetrecht, 2. Auflage. Stuttgart, 2010. S. 231.

возможностях доменных имен. Идентификационная функция определяется как возможность идентификации владельца домена и, соответственно, отграничение его от других лиц[1]. В силу данной функции доменные имена обладают значительной экономической ценностью и имеют свою реальную цену, могут продаваться и покупаться.

В Германии существуют целые так называемые биржи доменных имен (см., например, *www.sedo.de*). Стоимость некоторых доменных имен составляет миллионы долларов. Например, домен *business.com* был продан в 1999 г. за 7,5 млн долл. США, а домен *vodka.com* в 2006 г. – за 3 млн долл. США[2].

Экономическую ценность домена увеличивает такая техническая особенность, как его единственность и уникальность. Факт того, что кто-то является владельцем определенного домена, означает одновременно, что никто другой не может иметь этот же домен.

Как это обычно бывает, экономическая ценность того или иного явления обусловливает необходимость как правовой защиты вовлеченных лиц, так и необходимость правового регулирования экономического оборота такого явления. В начальный период развития Интернета немецкий правоприменитель сталкивался с определенными юридическими трудностями. Если в техническом смысле домен представляет собой лишь компьютерную адресацию, то в юридическом смысле квалификация домена вызывала в Германии до недавнего времени значительные трудности, в первую очередь в силу «неовеществленности» домена[3].

Вместе с тем уже многие годы судебная практика исходит из применения к доменам принципов, взятых из права наименований, обозначений[4]. Так, в своем решении от 12.04.2000 Верховный суд земли Бранденбург указал следующее: «Так называемое доменное имя представляет собой схожее с наименованием обозначение, которому посредством простой регистрации придается также функция идентификации, так как обычный интернет-пользователь при загрузке определенного сайта ожидает получить предложения определенного продавца. При нарушении права на наименование пострадавший имеет право требования, основанное на § 12 BGB»[5].

[1] *Haug Volker*. Internetrecht, 2. Auflage. Stuttgart, 2010. S. 232.

[2] http://www.towave.ru/pub/25-samykh-dorogikh-domennykh-imen-v-istorii.html

[3] *Haug, Volker*. Grundwissen Internetrecht, 3. Auflage, Stuttgart, 2016. S. 204.

[4] Одними из первых было решение LGMannheim, NJW 1996, 2736 (heidelberg.de).

[5] OLG Brandenburg, Urteil 12.04.00 Az.1 U 25/99.

Но куда большие споры вызывал в немецком праве и судебной практике вопрос о правовой природе права на доменное имя.

Домены обладают определенной экономической ценностью, имеют измеримую в деньгах стоимость, отчуждаемы и могут быть предметом различных договорных обязательств[1]. Та особенность доменного имени, что оно является в силу технических особенностей единственным в своем роде, наделяет его владельца неким **фактическим** абсолютным правом владения доменом. Если кто-то владеет доменом, то другой им владеть уже не может[2]. Вопрос заключался в том, является ли такое фактическое владение абсолютным самостоятельным правом в юридическом смысле.

Если бы право на домен являлось абсолютным правом, его «владелец мог бы держать любого другого на расстоянии от домена не только фактически, но и юридически»[3]. Обосновать этот вывод можно ссылками на схожесть доменного имени с наименованием или обозначением и применением к доменам норм права, регулирующего вопросы наименований и обозначений. Однако в итоге право на домен не признано абсолютным правом, аналогичным праву на наименование, на товарный знак. Аргументом против этого стало то обстоятельство, что наименования и товарные знаки могут использоваться и иметь правовую защиту отдельно от доменов, что домены в большей степени представляют собой лишь форму использования независимых от них наименований и товарных знаков[4]. Кроме того, признание права на домен абсолютным правом стало и отсутствие специального указания на это в законе[5].

В итоге немецкий правопорядок квалифицировал право на доменное имя в качестве обязательственного права, а не абсолютного.

В известном решении Федерального конституционного суда Германии по делу *ad-acta.de*[6] было указано, что право на использование доменного имени представляет собой относительное договорное право пользования. В данном деле ответчику – фирме, которая занималась массовой регистрацией доменных имен с целью их дальнейшей продажи, в соответствии с решениями нижестоящих судов было предпи-

[1] *Härting Niko*. Internetrecht, 5.Auflage. Köln, 2014. S. 444.

[2] *Haug.* Internetrecht. S. 232.

[3] *Haug.* Grundwissen Internetrecht. S. 204.

[4] Ibid. S. 204, 205.

[5] *Härting.* Internetrecht. S. 444.

[6] BVerfG Beschluss vom 24.11.2004, Az.:1 BvR 1306/02.

сано воздержаться от использования домена *ad-acta.de*, а регистрация самого этого домена подлежала отмене. Истцом выступала фирма *Ad-acta Datenschutz und Recycling GmbH*, которая посчитала, что нарушены ее права на фирменное наименование, товарный знак. Судами иск был удовлетворен. Ответчик ставил перед конституционным судом вопрос о нарушении ее конституционного права на защиту права собственности в связи с тем, что право на доменное имя представляет собой право, аналогичное праву собственности. Конституционный суд в своем постановлении указал, что, несмотря на отдельные противоположные мнения в юридической литературе, владелец доменного имени не получает ни права собственности на интернет-адрес, ни иного абсолютного права на доменное имя, которое могло быть схожим или аналогичным исключительному праву (на средство индивидуализации). Конституционный суд пояснил, что владелец доменного имени в результате заключения договора с регистратором доменных имен *DENIC*[1] взамен уплачиваемого вознаграждения получает право использования определенного домена, которое представляет собой относительное договорное право пользования. При этом заключение договора на неопределенный срок с одновременно предусмотренными возможностями его расторжения характеризуют данное правоотношение как длящееся обязательство.

Несмотря на то что право на доменное имя является не абсолютным, а обязательственным правом, оно пользуется в Германии наряду с иными относительными имущественными правами конституционной защитой.

Конституционным судом указывалось, что право пользования доменом представляет собой охраняемую правом имущественную ценность, и правовая защита предоставлена владельцу домена в той же степени, в какой предоставлена и собственнику материальной вещи. И право *DENIC* как стороны договора расторгнуть договор в определенных случаях не находится в противоречии с наличием у договорного по своей природе права пользования доменом конституционно-правовой защиты, предусмотренной для права собственности, а лишь ограничивает объем прав владельца домена.

Основанием для придания обязательственно-правовому требованию такой же правовой защиты, как и праву собственности, является ст. 14 Конституции Германии и многолетняя судебная практика при-

[1] Deutsches Network Information Center.

менения данной статьи Федеральным конституционным судом Германии, согласно которой под понятие «собственность» по смыслу ст. 14 Конституции Германии подпадают также основанные на заключении договора обязательственно-правовые требования. Такие требования хотя и направлены только на соответствующего контрагента по договору, однако являются такой же имущественной ценностью, как и право собственности на материальную вещь[1].

Регистрация доменных имен

Главной организацией, отвечающей за организацию и координацию регистрации доменных имен и контролирующей данный процесс, является международная некоммерческая организация *ICANN*[2], находящаяся в штате Калифорния в США. Права на выдачу и управление адресами в Европе переданы ею *Réseaux Européens Network Coordination Center* (*RIPE-NCC*)[3]. Вопросами регистрации доменов в зоне *.eu* ведает непосредственно *EURid*[4], а доменов в зоне *.de* – *DENIC*[5].

Как правило, доменное имя состоит из двух частей – из домена верхнего уровня и из стоящего перед ним домена второго уровня. Например, в доменном имени *berlin.de* доменом верхнего уровня является *.de*, а *berlin* – доменом второго уровня. *.de*, являющийся доменом верхнего уровня, представляет собой национальный домен Германии.

Организацией, отвечающей за регистрацию доменных имен второго уровня в зоне домена *.de*, является некоммерческое товарищество *DENIC* на основании переданных ICANN полномочий. Первоначально регистрацией доменных имен занимался отдел информатики университета г. Дортмунда, но впоследствии в связи с бурным развитием Интернета отдел перестал справляться с этой задачей. Тогда крупнейшими немецкими провайдерами было создано некоммерческое товарищество *Deutsches Network Information Center* (*DENIC*). При этом техническое обеспечение процесса регистрации было поручено компьютерному центру университета г. Карлсруэ.

DENIC осуществляет свои задачи на гражданско-правовой основе, оно не является ни государственным органом, ни уполномоченной го-

[1] См., например, BVerfG Beschluss vom 08.06.1977, Az.:2 BvR 499/74 und 1042/75.

[2] https://www.icann.org/ru

[3] *Hetmank Sven.* Internetrecht, Wiesbaden 2016. S. 29.

[4] http://eurid.eu.

[5] https://www.denic.de/

сударством организацией[1]. При этом отмечается, что доменные имена в Интернете представляют собой общественное достояние и что в силу этого большого общественного, а также экономического значения доменов встает вопрос о легитимности *DENIC*, являющегося некоммерческим товариществом, выполнять эти по сути публичные функции[2].

С одной стороны, регистрационные правомочия *DENIC* получены им через *RIPE* от *ICANN*, которая является организацией, находящейся в юрисдикции США и подчиняющейся правопорядку Соединенных Штатов Америки. С другой стороны, *DENIC* осуществляет свою деятельность по отношению к населению Германии, так как подавляющее большинство владельцев доменных имен в зоне *.de* имеют свое место жительства или место нахождение в Германии. Здесь возникает вопрос относительно гарантий соблюдения интересов Германии как суверенного государства и ее прав и обязанностей по обеспечению действия собственных правовых основополагающих принципов.

Проблемы легитимности *DENIC* как организации, ответственной за регистрацию доменных имен, поднимались не только в юридической литературе, но также и депутатами немецкого парламента. В ответе на один из депутатских запросов о легитимности *DENIC* федеральное правительство Германии указало следующее: «*Регистрация доменных имен осуществляется в разных странах на основании различных принципов. При этом диапазон регистраторов простирается от полностью частных коммерческих организаций до государственных органов, подчиненных министерствам связи. В Германии этот процесс начинался в научной сфере, далее привел к образованию некоммерческого товарищества DENIC. Согласно данным федерального правительства, деятельность DENIC полностью удовлетворяет интернет-сообщество. Регистрационный процесс при этом осуществляется честно по отношению ко всем заявителям. Поэтому нет никакого основания переводить процесс регистрации доменных имен в иные правовые и организационные формы*»[3].

Таким образом, правительство Германии посчитало, что в настоящий момент, несмотря на большое общественное и экономическое значение процесса регистрации доменных имен, нет необходимости создания специальной публично-правовой базы для легитимации данного процесса. Во всяком случае до тех пор, пока деятельность *DENIC*

[1] *Hetmank*. Internetrecht. S. 29.

[2] *Haug*. Grundwissen Internetrecht. S. 224.

[3] BT-Drs. 14/3956.

полностью удовлетворяет интересам как немецкого государства, так и пользователей Интернета на территории страны.

При регистрации домена действует строгий принцип приоритетности, согласно которому домен получает тот, кто подал соответствующую заявку первым[1]. Сама регистрация происходит посредством заключения соответствующего договора. Содержание договора определяется общими условиями договора[2], разработанными *DENIC*.

Предметом регистрационного договора между *DENIC* и заявителем является обязательство первого зарегистрировать домен второго уровня на имя заявителя и осуществлять его соединение в сети Интернет с доменом верхнего уровня *.de* (§ 2 *DDB*[3]). В качестве встречного удовлетворения заявитель обязан оплачивать эти услуги *DENIC* в соответствии с устанавливаемыми *DENIC* и публикуемыми им расценками (§ 4 *DDB*).

Заявитель отвечает за верность предоставленных данных, а также за то, что он обладает правом на регистрацию и пользование соответствующим доменом и что при этом не будут нарушены ни права третьих лиц, ни нормы действующего законодательства (п. 1 § 3, п. 3 § 5 *DDB*). Заявитель также обязуется отвечать за все требования, включая возмещение всех убытков и расходов, которые могут быть предъявлены к *DENIC* третьим лицом на том основании, что права такого лица были нарушены регистрацией и использованием заявителем соответствующего домена (п. 4 § 5 *DDB*).

DENIC со своей стороны отвечает за допущенные им умышленно или вследствие грубой неосторожности нарушения существенных условий договора (п. 1 § 5 *DDB*). Если же нарушение условий договора произошло вследствие простой неосторожности, то ответственность *DENIC* ограничивается «обычно предвидимыми» убытками. При этом указывается, что «как правило, такие предвидимые убытки не должны превышать размер ежегодной платы за домен» (п. 1 § 5 *DDB*).

Договор заключается на определенный срок с правом владельца домена расторгнуть его в любой момент без предварительного уведомления (п. 1 § 7 *DDB*). В отличие от владельца домена право *DENIC* на одностороннее расторжение договора предусмотрено лишь при

[1] *Hetmank*. Internetrecht. S. 30; BT-Drs. 14/3956.

[2] Общие условия договора (*allgemeine Geschäftsbedingungen*) являются согласно § 305 BGB предварительно сформулированными типовыми условиями, предназначенными для большего числа договоров, которые одна сторона договора представляет другой стороне в качестве условий заключаемого между ними договора.

[3] DENIC-Domainbedingungen. https://www.denic.de/domainbedingungen/

наличии на то веских оснований (п. 2 § 7 *DDB*). В качестве примера таких веских оснований называются случаи, когда домен как таковой содержит противоправные высказывания, когда регистрация домена явно нарушает права третьих лиц или иным образом является противоправным, когда владелец домена не производит оплату, предусмотренную договором, и др. (подп. (а) – (к) п. 2 § 7 *DDB*).

Оборотоспособность прав на доменные имена обеспечивается правом владельца домена уступки своих прав третьему лицу. Уступка прав на домен производится посредством расторжения договора правообладателем и указанием на то лицо, которое вправе зарегистрировать домен на себя (§ 6 *DDB*).

Своего рода ограничением по кругу заявителей на регистрацию домена в зоне *.de* можно назвать условие, согласно которому заявитель должен иметь свое место нахождения в Германии или же в противном случае определить находящееся на территории Германии контактное лицо, которое одновременно уполномочено от имени заявителя получать деловую и судебную корреспонденцию (п. 1 § 3 *DDB*).

Ответственность регистратора DENIC

DENIC с начала коммерческого использования доменных имен придерживается либеральной политики при регистрации доменов, согласно которой не предусматриваются ни ограничения по отношению к кругу лиц, являющихся потенциальными заявителями, ни иные ограничения содержательного, материального характера. Регистрация производится в отличие от товарных знаков без проверки на возможное нарушение прав третьих лиц[1].

Как указывало правительство Германии, следует учитывать, что регистрационное учреждение, такое как *DENIC*, производит не «выдачу», а лишь «регистрацию» доменных имен. Различие состоит в том, что *DENIC*, за исключением отдельных случаев явных нарушений, не проводит правовой экспертизы, а лишь проверяет, не был ли заявленный домен зарегистрирован ранее, осуществляет свою деятельность не на основании каких-либо определенных критериев, а на основании принципа приоритетности *firstcome, firstserved*[2].

[1] *Bettinger.* Handbuch des Domainrechts. Nationale Schutzsysteme und internationale Streitbeilegung. S. 76.

[2] BT-Drs. 14/3956.

В этом же направлении складывается и судебная практика.

Если владелец доменного имени посредством его регистрации и неправомочного использования нарушает права третьих лиц на средства индивидуализации или его действия могут рассматриваться в качестве нарушения норм о добросовестной конкуренции, то регистратор может быть привлечен в качестве ответчика только в двух случаях:

1) регистратор умышленно желал и содействовал нарушению прав третьих лиц;

2) он зарегистрировал доменное имя, несмотря на то, что он мог и должен был распознать нарушение прав третьих лиц на средства индивидуализации или нарушение прав в сфере добросовестной конкуренции. Такое явное нарушение предполагается тогда, когда схожесть доменного имени с известным брендом легко распознаваема, в том числе и для регистратора, а недобросовестный заявитель в нарушение прав правообладателя известного бренда преследовал цель зарегистрировать соответствующее доменное имя на себя[1].

Подобные действия недобросовестных лиц признаются в литературе и судебной практике как противоречащие принципу «добрых нравов»[2]. В качестве примера явно неправомерного использования известного наименования приводится ситуация, когда зарегистрированная в Панаме фирма регистрирует доменное имя *regierung-oberfranken.de*[3], которое по сути означает официальное наименование органа управления одного из немецких территориальных округов[4].

В остальном, как подчеркивалось Федеральным Верховным судом Германии, проверка допустимости регистрации и использования доменного имени лежит в зоне ответственности заявителя, так как задачей регистратора в первую очередь является быстрое, надежное и незатратное для заявителей администрирование доменных имен и в особенности, их регистрация. В задачи регистратора не входит проведение полноценной проверки всех требований и претензий в конфликтных случаях в отношении спорных наименований.

Регистратор, который обладает лишь ограниченным количеством сотрудников, обеспечивает эффективность своей работы таким

[1] BGH. Urteil vom 17.05.2001, Az.: I ZR 251/99.

[2] *Härting.* Internetrecht. S.448; OLGFrankfurta.M. Beschluss vom 12.02.2000 Az.: 6W33/00.

[3] *Regierung Oberfranken* означает наименование правительства одного из немецких территориальных округов – Верхняя Франкония.

[4] *Hetmank*. Internetrecht. S.30; BGH, GRUR 2012, 651.

образом, чтобы организовать по возможности быструю и незатратную регистрацию доменных имен на основании принципа приоритетности в автоматизированном режиме, не проводя при этом правовой проверки заявленных имен на предмет нарушения прав третьих лиц. Лишь только таким образом регистратор в состоянии выполнять задачи по регистрации огромного количества доменных имен. При таком автоматизированном процессе проведение проверки при каждой регистрации является фактически невозможным[1].

Примечательно сравнение немецкими судьями объема обязанностей регистратора с обязанностями средства массовой информации, которое размещает у себя объявления третьих лиц: ограниченные обязанности регистратора по проверке наименований сопоставимы с ограниченными обязанностями СМИ по проверке размещаемых им объявлений третьих лиц на предмет нарушения прав третьих лиц.

Таким образом, в соответствии с подходом, сложившимся в немецкой судебной практике, требование к регистратору об отмене регистрации доменного имени лишь тогда является обоснованным и подлежит удовлетворению, когда такая регистрация имела очевидно противоправный характер и владелец доменного имени действовал явно незаконно.

Нарушения прав на имя, наименование и прав на обозначения

Правило о недопустимости неправомерного использования чужого имени, чужого наименования в ущерб интересам правообладателя, которое закреплено в § 12 *BGB*[2], применяется в Германии в силу сложившейся судебной практики и к доменным именам.

Неправомочным будет использование чужого имени, если оно вызывает у третьих лиц заблуждение при идентификации владельца имени и лица, которое использует чужое имя, если при этом нарушаются права и законные интересы владельца имени, имеет место и при использовании домена его владельцем, который при этом не является носителем имени или наименования.

[1] BGH. Urteil vom 17.05.2001, Az.: I ZR 251/99.

[2] В праве Германии под правовую охрану права на имя подпадают не только имена и фамилии граждан, а также наименования организаций, не являющихся активными участниками коммерческого оборота, таких как некоммерческие организации, органы власти.

Так, в одном из судебных решений[1] было признано неправомерным использование частным лицом домена *verteidigungsministerium.de*[2]. Суд указал, что использование такого домена вводит в заблуждение пользователей Интернета, которые ожидают, что они попадают на страницу немецкого Министерства обороны. При этом подчеркивалось важное значение, которое имеет Министерство обороны для государства и для общества в целом и то, что в такой ситуации индивидуальное мнение владельца домена не должно восприниматься третьими лицами как мнение оборонного ведомства. Кроме того, суд обратил внимание на то, что публиковавшаяся на этом сайте информация прямо противоречила задачам и интересам немецкого Министерства обороны.

Не является нарушением права на имя использование домена, в котором содержится название родовых вещей, хотя оно и является идентичным чьему-то имени или фамилии.

Так, в одном из судебных дел[3] гражданин по фамилии *Säugling* (на русский переводится как «младенец») безуспешно предъявлял претензии к владельцу доменного имени *saegling.de*, который занимался продажей товаров для младенцев.

Наряду с правом на имя и наименование в сфере использования доменов правовой защите подлежат также так называемые права на обозначения. К этой группе относятся товарные знаки и знаки обслуживания (§ 3 MarkenG), фирменные наименования и коммерческие обозначения (§ 5 MarkenG), наименования мест происхождения товаров и услуг (§ 126 MarkenG).

Права на обозначения относятся к категории абсолютных прав[4], что исключает неправомочное использование в деловом обороте соответствующих обозначений третьими лицами. Также не допускается использование обозначений, схожих до степени смешения.

В основе большинства споров в сфере использования доменов лежат требования, основанные на нарушении прав на имя, наименование или на обозначение. Для удовлетворения требований по таким спорам необходимо доказать наличие следующих обстоятельств: 1) отсутствие у владельца спорного домена правомочий на использование соответст-

[1] LG Hannover. Urteil vom 12.09.2001, Az.:7O349/01.

[2] Verteidigungsministerium – Министерство обороны в ФРГ.

[3] LG München I. Urteil vom 08.03.2001, Az.: 4HK0200/01.

[4] *Haug.* Grundwissen Internetrecht. S. 268.

вующего наименования или обозначения; 2) нарушение прав и законных интересов правообладателя имени или обозначения, которое, как правило, выражается в наличии риска заблуждения третьими лицами при идентификации правообладателя. В случае признания требования обоснованным возможны различные правовые последствия, предполагающие как материальное возмещение, так и удовлетворение нематериально-правовых требований.

Основным интересом и желанием правообладателя, чье право было нарушено, является устранение такого нарушения, что достигается посредством обязывания нарушителя воздерживаться от незаконного использования наименования или обозначения, принадлежащих правообладателю (§ 12, 1004 *BGB*, § 14, 15 *MarkenG*). В спорах по использованию доменных имен ответчику предписывается воздержаться от использования соответствующего спорного домена, что подразумевает обязанность *DENIC* аннулировать регистрацию домена[1].

Также не менее важным, а в некоторых случаях и более приоритетным интересом для лица, чье право было нарушено, является возмещение убытков, которые оно понесло вследствие нарушения его прав на имя или на обозначение. Основанием для предъявления требования о возмещении убытков из-за нарушения права на имя, наименование (§ 12 *BGB*) являются общие положения деликтного права, основанные на § 823 *BGB*. Регулирование возмещения убытков вследствие нарушения прав на обозначения основаны также на специальных нормах § 14, 15 *MarkenG*.

Одно время дискуссионным являлся вопрос, имеет ли пострадавшее лицо право требования передачи, перерегистрации спорного домена на себя. Но так как ни нормы, регулирующие право на имя, наименование, ни нормы о правах на обозначения не содержат правовых оснований для подобной передачи доменного имени, судебная практика ответила на этот вопрос отрицательно.

В итоге вопрос защиты прав лица, которое имеет право и намерение самостоятельно использовать и зарегистрировать на себя спорный домен, решается с помощью положений Общих условий *DENIC*. Так, согласно § 2 абз. 3 *DDB* в случае обоснованного заявления лица, которое оспаривает или собирается оспорить регистрацию домена за его владельцем, *DENIC* может обременить соответствующий домен запретом на его отчуждение третьим лицам. Таким образом, достигается

[1] *Haug.* Grundwissen Internetrecht. S. 251.

цель защиты прав лица, которое имеет потенциальное право на домен и намеревается в дальнейшем самостоятельно его использовать и соответственно зарегистрировать его на свое имя.

Правонарушения в области конкурентного права

Факты регистрации и использования доменных имен могут приводить также и к нарушениям норм о добросовестной конкуренции. Основополагающей в немецком праве нормой в этой области является § 3 *UWG*, в соответствии с которой не допускается нарушение правовых норм, направленных на обеспечение прав и интересов всех участников рынка и обеспечение добросовестной конкуренции, если при этом нарушаются права участников рынка, а также права потребителей. Применительно к сфере доменных имен применяются также § 4, 5 *UWG*, которые указывают конкретные нарушения конкурентного права.

Параграф 4 *UWG* запрещает создание препятствий в осуществлении и развитии деятельности участников рынка. Немецкая доктрина и судебная практика относят к соответствующим нарушениям следующие случаи недобросовестной конкуренции: недобросовестная регистрация большого количества доменных имен (*Domain Grabbing*), регистрация доменных имен, близких по написанию к адресам популярных сайтов в расчете на ошибку части пользователей (*Typosquatting*), регистрация доменных имен, отражающих наименование родовых понятий, вещей.

Сама по себе регистрация доменных имен не является противоправной и не нарушает норм о добросовестной конкуренции, тем более, если при регистрации был соблюден принцип приоритетности. К владельцу доменных имен не может быть никаких претензий, если только не будет установлено, что целью резервирования доменных имен было не собственное их использование, а препятствование регистрации этих доменов другими, с тем чтобы в дальнейшем продать их заинтересованным лицам[1].

Квалифицирующим признаком при определении таких правонарушений являются факты регистрации большого количества доменных имен, содержащих чужие наименования, торговые знаки, коммерческие обозначения[2]. Нарушение норм о добросовестной конкуренции,

[1] BGH. Urteil vom 24.4.2008, Az.: I ZR 159/05.

[2] OLGFrankfurta. M., Beschluss vom 12.02.2000 Az.: 6W33/00.

называемое тайпсквоттингом, имеет место при регистрации домена, близкого по написанию с доменным именем популярных сайтов, с той целью, чтобы пользователи, ищущие сайт конкурента, попадали на сайт тайпсквоттера[1]. Регистрация доменов, содержащих в себе наименование родовых вещей, в принципе, является легитимной и признается нарушением норм о добросовестной конкуренции лишь в тех случаях, когда заявитель регистрирует на себя большое количество созвучных или по-разному пишущихся обозначений одного понятия или вещи с целью воспрепятствовать использование таких доменов другими лицами[2].

Параграф 5 *UWG*, который запрещает недобросовестную конкуренцию посредством введения в заблуждение, применяется судебной практикой также в отношении недобросовестного использования доменных имен. Введение в заблуждение в соответствии с § 5 *UWG* имеет место тогда, когда недобросовестное лицо либо посредством использования недостоверных данных, либо иным образом стремится ввести в заблуждение, обмануть потребителя или иных заинтересованных лиц[3]. В случае с недобросовестным использованием доменных имен нарушение § 5 *UWG* имеет место тогда, когда содержание интернет-сайта и деятельность владельца домена не соответствуют наименованию доменного имени.

Например, сайт *www.rechtsanwalt.com* (*rechtsanwalt* переводится как «адвокат, защитник») ассоциируется у пользователей с лицами, осуществляющими соответствующую профессию. В одном из судебных решений было признано неправомерным и нарушающим § 5 *UWG* использование данного домена лицом, не осуществляющим адвокатскую деятельность[4].

В качестве правовых последствий нарушения правил добросовестной конкуренции при использовании доменных имен могут быть заявлены требования о запрете использования соответствующих доменных имен, о возмещении убытков, а также публично-правовое требование о наложении на нарушителя штрафа, взыскиваемого в федеральный бюджет (§ 8–10 *UWG*).

[1] BGH. Urteil vom 22.01.2014, Az.: I ZR 164/12.

[2] BGH. Urteil vom 16.12.2004, Az.: I ZR 69/02.

[3] *Hetmank*. Internetrecht. S. 63.

[4] OLG Hamburg Urteil vom 02.05.2002, Az.: 3U303/01.

Пристатейный библиографический список:

1. *Bettinger Torsten*. Handbuch des Domainrechts. Nationale Schutz systeme und internationale Streitbeilegung. München, 2008.
2. *Haug Volker*. Internetrecht, 2. Auflage. Stuttgart, 2010.
3. *Haug Volker*. Grundwissen Internetrecht, 3.Auflage, Stuttgart, 2016.
4. *Härting Niko*. Internetrecht, 5.Auflage. Köln, 2014.
5. *Hetmank Sven*. Internetrecht, Wiesbaden, 2016.

М.А. Рожкова

ПРАВА НА ДОМЕННОЕ ИМЯ

Аннотация. *Анализ отечественной юридической литературы позволил автору сделать вывод о том, что сложности с пониманием сущности доменных имен и, как следствие, правоприменительные проблемы во многом связаны с тем, что отечественные юристы не разграничивают техническую и идентификационную функции доменных имен. В предлагаемой статье предпринимается попытка исправить это упущение, для чего автор обращается к прецедентной практике Европейского суда по правам человека, актам Конституционного Суда РФ и практике отечественных арбитражных судов* (*включая Суд по интеллектуальным правам*), *учитывая при этом технические аспекты процесса переадресации.*

Ключевые слова: *доменное имя, доменные споры.*

Проблематика доменных имен сегодня ничуть не утратила актуальность: отсутствие подробного законодательного урегулирования большинства вопросов, связанных с использованием доменных имен, порождает немало споров, которые передаются на рассмотрение судов и арбитражей. В настоящей статье предпринята попытка разобрать некоторые из вопросов, значимых для правильного разрешения доменных споров.

Доменное имя: функция переадресации

В п. 15 ст. 2 Закона об информации дано определение **доменного имени** (англ. *Domain Name*): под ним понимается *обозначение символами, предназначенное для адресации сайтов в сети Интернет в целях обеспечения доступа к информации, размещенной в сети Интернет*. Упрощая, можно говорить о том, что с помощью доменного имени пользовательское сетевое устройство (компьютер, планшет, смартфон и пр.) переадресуется на конкретный информационный ресурс – сайт, поисковик, портал, домашнюю страницу и пр. Весьма удачным является определение, в свое время использованное ФАС Московского округа в одном из своих постановлений: «Домен... – это набор символов,

позволяющий идентифицировать и найти в сети Интернет ресурс (веб-сайт) с определенным доменным именем»[1].

Доменное имя принципиально отличается от ***IP*-адреса** (сокр. от англ. *Internet Protocol Address*). *IP*-адрес присваивается каждому работающему в сети Интернет устройству (серверу, компьютеру, планшету, смартфону и пр.), позволяя идентифицировать его среди иных работающих в Интернете устройств, получать и передавать ту или иную информацию. В п. 16 ст. 2 Закона об информации под **сетевым адресом** (*IP*-адресом) понимается «идентификатор в сети передачи данных, определяющий при оказании телематических услуг связи абонентский терминал или иные средства связи, входящие в информационную систему». Иными словами, *IP*-адрес – это набор символов, позволяющий идентифицировать в сети Интернет компьютер или иное устройство.

Таким образом, совершенно неправильно говорить о том, что «доменное имя соответствует уникальному *IP*-адресу». Напротив, доменное имя и *IP*-адрес принципиально различаются: первое предназначено для переадресации устройства на информационный ресурс, второй – для идентификации устройства, выходящего в сеть.

Важно заметить при этом, что на одном устройстве – сервере, имеющем соответствующий *IP*-адрес, могут размещаться одновременно тысячи разных информационных ресурсов (сайтов, порталов, домашних страниц и т.д.), имеющих разные доменные имена. И в то же время сайт (информационный ресурс), имеющий одно доменное имя, может быть размещен сразу на нескольких серверах и соответствовать одновременно нескольким *IP*-адресам (например, для распределения нагрузки на серверы).

Вследствие сказанного понятия «доменное имя» и «сетевой адрес» (*IP*-адрес) следует четко разграничивать. Неразграничение этих понятий может стать как причиной нарушения прав заинтересованных лиц, так и препятствием к их защите.

Ярким примером этого тезиса является дело «*Харитонов против России*»[2], которое в настоящее время рассматривается ЕСПЧ.

Заявитель – директор Ассоциации интернет-издателей Владимир Харитонов является правообладателем сайта интернет-библиотеки и администратором доменного имени *digital-books.ru*, на котором эта библиотека размещалась. Сайт заявителя находился на одном *IP*-адресе (на

[1] Постановление ФАС Московского округа от 02.06.2003 № КГ-А41/3503-03.

[2] *Kharitonov v. Russia, application no. 10795/14.*

одном сервере) с другим сайтом – «Растаманские сказки» (размещенном на домене *rastamantales.ru*), в отношении которого Роскомнадзором было принято решение о блокировании вследствие выявления информации, запрещенной к распространению. Однако на основании решения был заблокирован не отдельный сайт (по доменному имени), а весь *IP-адрес* (весь сервер). Таким образом, был ограничен доступ не только к сайту-нарушителю, но и к «добросовестным» сайтам, размещенным на том же сервере (на том же *IP*-адресе) и не содержащим никакой запрещенной информации, включая сайт заявителя *digital-books.ru*

Владимир Харитонов обжаловал в судебном порядке решение Роскомнадзора, ограничивающее доступ к его сайту, не содержащему незаконной информации, но суды нескольких инстанций признали блокировку *IP*-адреса соответствующей закону.

С учетом этого Владимир Харитонов обратился в КС РФ с жалобой, в которой оспаривал конституционность п. 2 ч. 2 ст. 15[1] Закона об информации. Статья 15[1] Закона посвящена «Единому реестру доменных имен, указателей страниц сайтов в сети «Интернет» и сетевых адресов, позволяющих идентифицировать сайты в сети «Интернет», содержащие информацию, распространение которой в Российской Федерации запрещено» (далее – Единый реестр), созданного в целях ограничения доступа к сайтам, содержащим запрещенную к распространению информацию. В оспариваемом п. 2 ч. 2 ст. 15[1] предусмотрено, что в Единый реестр включаются не только доменные имена и (или) указатели страниц сайтов[1] в сети Интернет, но и сетевые адреса (*IP*-адреса) без уточнения применения этой нормы в различных ситуациях.

Таким образом, оспариваемая норма, как указывал В. Харитонов, не исключает возможность блокирования *IP*-адреса, на котором размещен информационный ресурс, содержащий запрещенную к распространению информацию, что в итоге может повлечь блокировку не одного сайта, содержащего запрещенную информацию, а целого сервера, на котором, как отмечалось, могут располагаться тысячи сайтов, причем сайтов «добросовестных». По мнению заявителя жалобы, в подобных случаях «владельцы сайтов, не содержащих запрещенной информации, лишаются права распространять незапрещенную информацию законным способом и фактически подвергаются мерам юридической ответственности при отсутствии правонарушения».

[1] Речь идет о едином указателе ресурса – *URL* (сокр. от англ. *Uniform Resource Locator* – единый указатель местонахождения ресурса).

КС РФ не нашел оснований для принятия данной жалобы к рассмотрению, отметив при этом следующее: «Что же касается владельцев сайтов, не содержащих запрещенной к распространению в Российской Федерации информации, но доступ к которым оказался ограничен в связи с включением в реестр сетевого адреса, то их права на распространение информации, по существу, оказываются затронуты не решением о включении сетевого адреса в Единый реестр и принятыми в связи с этим мерами, а ненадлежащими действиями (бездействием) обслуживающего их провайдера хостинга. Соответственно, защита их права на распространение информации должна осуществляться, прежде всего, в рамках правоотношений с обслуживающим их провайдером хостинга»[1].

Таким образом, КС РФ, по сути, уклонился от оценки нарушения прав владельцев информационных ресурсов, не содержащих запрещенной информации, доступ к которым был заблокирован при применении мер ответственности к владельцам других информационных ресурсов.

Между тем ЕСПЧ в схожей ситуации признавал права владельцев информационных ресурсов нарушенными[2].

Так, при рассмотрении дела «*Ахмет Йилдырым против Турции*»[3] ЕСПЧ было установлено, что заявитель являлся владельцем информационного ресурса (созданного с помощью сервиса *Google Sites* (*sites.google.com*)), на котором им публиковались собственные научные труды и материалы, отражающие его взгляды по различным вопросам. В июне 2009 г. национальный суд в рамках борьбы с преступлениями в Интернете принял решение о применении предварительной меры в виде блокирования сайта, принадлежащего другому владельцу (далее – сайт нарушителя), но затем решение было изменено и принято решение о блокировании доступа ко всем сайтам, созданным на *Google Sites*. Вследствие этого заявитель был лишен доступа к собственному сайту. Ходатайство об отмене распоряжения в отношении сайта заявителя было отклонено национальным судом. По состоянию на апрель 2012 г. заявитель по-прежнему не мог пользоваться своим сайтом, хотя уголовное дело в отношении владельца другого сайта

[1] Определение КС РФ от 17.07.2014 № 1759-О.

[2] См. об этом: *Рожкова М.А.* Доменные имена как идентификаторы и средства коммуникации // Хозяйство и право. 2015. № 3. С. 55–70.

[3] Постановление ЕСПЧ от 18.12.2012 по делу «Ахмет Йилдырым против Турции» (*Ahmet Yildirim v. Turkey*; *application no.* 3111/10).

(сайта нарушителя с незаконным содержанием) было прекращено в марте 2011 г.

ЕСПЧ признал подобное блокирование ограничением права заявителя на свободу выражения мнения (ст. 10 Конвенции по правам человека). Это объяснялось тем, что сервис *Google Sites* предназначен для облегчения создания и совместного использования сайтов в сети Интернет, вследствие чего он является средством осуществления свободы слова. Кроме того, ЕСПЧ сослался на то, что блокирование доступа ко всем сайтам на *Google Sites* представляет собой ограничение права пользователей сети Интернет на получение информации, поскольку Интернет в настоящее время стал одним из главных средств, с помощью которых люди реализуют право на выражение мнения, а также получение и распространение информации, гарантированное ст. 10 Конвенции. Причем в постановлении ЕСПЧ отмечалось, что *Google Sites* содержит столь значительное количество данных и информации, что он по своему объему сопоставим с онлайн-архивами крупных газет или традиционных библиотек. В то же время национальный суд из-за единственного сайта нарушителя вынес решение о блокировании доступа ко всем ресурсам *Google Sites*, закрыв доступ к такому большому количеству информации на неопределенный срок.

ЕСПЧ указал, что, вынося решение о блокировании *Google Sites* в качестве предварительной меры, национальный суд исходил из того, что это единственно возможный способ блокирования сайта нарушителя. Между тем названная мера в данном случае не может рассматриваться в качестве единственно возможной – блокирование доступа ко всем сайтам на *Google Sites* из-за единственного сайта нарушителя представляет собой ограничение свобод, гарантированных ст. 10 Конвенции по правам человека.

Вследствие сказанного не удивительно, что жалоба Владимира Харитонова на блокирование его сайта при блокировке по *IP*-адресу сайта нарушителя была принята к рассмотрению ЕСПЧ, который в мае 2017 г. коммуницировал ее российскому государству.

Новое назначение доменных имен и различия в целях их регистрации и использования

Система доменных имен, упрощающая и ускоряющая переадресацию в сети Интернет, начала создаваться в 80-е гг. прошлого столетия. Но достаточно быстро к пользователям Интернета пришло понимание

того, что помимо чисто технической функции переадресации доменные имена из-за их простой для запоминания формы могут использоваться и в иных целях.

В связи с этим в п. 10 доклада Всемирной организации интеллектуальной собственности (далее – ВОИС) по доменным именам уже в 1999 г. отмечалось: «Доменные имена были предназначены для выполнения технической функции способом, удобным для пользователей Интернета. Они предназначались для предоставления компьютерам легко запоминающейся и идентифицирующей адресации без необходимости прибегать к идентифицирующему цифровому *IP*-адресу. Именно потому, что они легко запоминаются и идентифицируются, доменные имена, кроме того, приобрели дополнительное предназначение в качестве идентификаторов бизнеса или частных лиц... в то время как телефонные и факсимильные номера состоят из анонимного набора цифр, не несущих какого-либо дополнительного смысла, доменные имена, вследствие своего предназначения быть легко запоминаемыми и идентифицирующими, часто несут в себе дополнительное значение, связанное с наименованием или обозначением бизнеса, либо его продуктами или услугами»[1]. С учетом этого в Отчете ВОИС 2002 г. подчеркивалось: «Большинство организаций, вне зависимости от того, относятся ли они к электронной коммерции или нет, рекламируют свои доменные имена для обозначения своего присутствия в Интернете. Таким образом, хотя они, как таковые, и не являются объектом интеллектуальной собственности, доменные имена в настоящее время выполняют функцию идентификации, подобную той, что несут в себе товарные знаки»[2].

Эта позиция находила подтверждение и в отечественной судебной практике.

Так, еще в 2001 г. при рассмотрении доменного спора относительно использования товарного знака *kodak* в доменном имени *kodak.ru* Президиум ВАС РФ отметил следующее: «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 то-

[1] Final Report of the WIPO Internet Domain Name Process "The Management of Internet Names and Addresses" 30.04.1999 (http://www.wipo.int/amc/en/processes/process1/report/index.html).

[2] Интеллектуальная собственность в Интернете: обзор проблем. Женева: ВОИС, 2002. С. 24.

варов и услуг других юридических или физических лиц. Кроме того, доменные имена, содержащие товарные знаки или торговые наименования, имеют коммерческую стоимость»[1].

Таким образом, доменные имена с определенного момента помимо *технической функции переадресации в сети* Интернет стали использоваться для *выделения* (*идентификации*) *товаров, работ, услуг или бизнеса* одних производителей, продавцов и исполнителей среди аналогичных товаров, работ, услуг. Поэтому, отвлекшись от технической функции доменных имен, необходимо изучить назначение доменного имени в качестве **идентификатора**[2].

Функция доменного имени, на которую обращается внимание в большинстве работ зарубежных исследователей, – это *функция идентификации бизнеса или частных лиц*[3]. И этот момент требует специального комментария.

Если цель использования доменного имени не предполагает получения выгоды, носит *некоммерческий характер*, то оно выступает **уникальным идентификатором владельца информационного ресурса.** Так, доменное имя *rozhkova.com* идентифицирует автора настоящей работы. Доменное имя может использоваться для сайта (или любого иного информационного ресурса), отражающего, например, кулинарные пристрастия, тягу к путешествиям, любовь к животным либо любые другие некоммерческие интересы владельца этого ресурса.

Если доменное имя регистрируется для целей достижения *коммерческих целей*, и сайт, размещенный на этом доменном имени, используется, например, для продвижения на рынке товаров, работ услуг, предложения к продаже и т.д., то ситуация принципиально меняется. В этом случае доменное имя становится **родовым идентификатором**

[1] Постановление Президиума ВАС РФ от 16.01.2001 № 1192/00 по делу № А40-25314/99-15-271.

[2] См. об этом подробнее: *Рожкова М.* Идентификаторы: все ли надо относить к объектам интеллектуальной собственности? // Хозяйство и право. 2015. № 2. С. 82–86; *Она же.* Идентификаторы // https://zakon.ru/blog/2017/01/18/identifikatory; *Она же.* Средства индивидуализации и средства индивидуализации товаров, работ, услуг – почувствуй разницу // https://zakon.ru/blog/2017/09/18/sredstva_individualizacii_i_sredstva_individualizacii_tovarov_rabot_uslug__pochuvstvuj_raznicu

[3] В настоящей работе не используется выражение «средства индивидуализации товаров, работ, услуг» вследствие его неправильности (подробнее об этом см.: Защита деловой репутации в случаях ее диффамации или неправомерного использования (в сфере коммерческих отношений) / авт. колл. Рожкова М.А., Афанасьев Д.В., Глазкова М.Е. и др.; под общ. ред. М.А. Рожковой. М.: Статут, 2015. С. 161–189 (автор параграфа – М.А. Рожкова).

товаров (работ, услуг) – подобно товарному знаку, указанию места производства/происхождения продукции, универсальному штрих-коду (*barcode*) и т.д.

Причем идентифицирующая роль доменного имени весьма скромна, когда речь идет не об интернет-пространстве, а о реальном мире.

Например, на лицевой стороне коробки конфет «*Merci*» доминирующим является товарный знак «*merci*» (зарегистрированный на имя производителя продукции – *August Storck KG*[1]), тогда как иные родовые идентификаторы – обозначение места производства конфет, *barcode*, знаки сертификации (в том числе добровольной), принадлежащее производителю доменное имя *storck.com* и т.п. – наносятся на обороте коробки. То есть при покупке этих конфет потребитель ориентируется на известный товарный знак «*merci*», но не на указанное на упаковке доменное имя *storck.com*

В виртуальном пространстве роль доменного имени возрастает в разы: потребитель склонен искать в сети Интернет товары, работы, услуги определенных производителей и продавцов, основываясь прежде всего (а иногда и только) на идентификации по доменному имени.

К сожалению, возможность доменного имени выступать идентификатором была воспринята отечественной судебной практикой не сразу. Вначале российские суды игнорировали необходимость установления **цели использования** доменного имени, что приводило к судебным ошибкам при рассмотрении дел в отношении доменных имен. Самым известным в этом смысле («хрестоматийным») стало дело о доменном имени *mumm.ru*.

Компания *G.H. Mumm&Cie*, в 1986 г. зарегистрировавшая товарный знак «*MUMM*» в отношении газированных напитков, французских вин, в том числе шампанского (и производящая шампанское под маркой «*MUMM*»), в 2010 г. обратилась с иском к гражданину Ю., требуя запретить использование товарного знака «*MUMM*» в доменном имени *mumm.ru* (права на которое с 2009 г. принадлежали данному гражданину) – имени, служащем обозначением сайта о египетских мумиях[2]. Это требование было основано на нормах п. 1 и 2 ст. 1484 ГК РФ, закрепляющих за лицом, на имя которого зарегистрирован товарный знак, исключительное право использования этого знака любым

[1] См., например: http://www.trademarkia.com/company-august-storck-kg-107714-page-1-2

[2] Постановление Президиума ВАС РФ от 18.05.2011 № 18012/10 по делу № А40-47499/10-27-380.

не противоречащим закону способом, включая использование в сети Интернет посредством «размещения» в доменном имени.

Арбитражные суды различных инстанций выносили противоречивые решения. По результатам рассмотрения дела в порядке надзора Президиум ВАС РФ поддержал решение о запрещении гражданину Ю. использовать спорное доменное имя. Обосновывая свою позицию, Президиум ВАС РФ указал: Ю. не имеет отношения к бизнесу компании *G.H. Mumm&Cie* и не получил согласия на использование товарного знака компании; у Ю. не было каких-либо законных прав и интересов в отношении доменного имени *mumm.ru*, так как он не является обладателем прав на одноименный товарный знак «и доменное имя не отражает его имени или фирменного наименования его компании». И в качестве заключения был сформулировал следующий вывод: Ю. недобросовестно использовал товарный знак «*MUMM*», принадлежащий компании *G.H. Mumm&Cie*, своими действиями создал препятствия компании для размещения информации о ней и ее товарах с использованием ее товарного знака на названном домене российской зоны сети Интернет, что привело к опасности введения потребителей продукции в заблуждение.

Бесспорно, этот вывод вызывает немало вопросов. Первый из них такой: каким образом сайт, посвященный египетским мумиям, может породить опасность введения потребителей в заблуждение в отношении шампанского и иных вин, производимых компанией *G.H. Mumm&Cie*? Допустимо ли говорить об использовании в доменном имени товарного знака, если доменное имя обозначает некоммерческий сайт, вообще не предназначенный для продвижения на рынке/предложения к продаже/рекламы товаров? Должно ли частное лицо, приобретающее право на доменное имя для обозначения информационного ресурса, не имеющего коммерческих целей, быть ограничено в выборе доменного имени в связи с тем, что схожее доменное имя (но в иной доменной зоне) принадлежит крупной коммерческой компании?

Схожими вопросами задавались и другие юристы. Например, А. Куликова, оспаривая корректность обоснования названного Постановления, весьма эмоционально пишет: «Домен «*mumm.ru*» не отражает имени владельца, его фирменного наименования или товарного знака, а потому у него нет прав и интересов в отношении спорного доменного имени. Значит ли это, что любой владелец домена должен регистрировать фирму или товарный знак? Данный довод ставит под угрозу существование

миллионов доменов с некоммерческим наполнением: личные блоги, кулинарные странички, профессиональные форумы и т.п.»[1].

Думается, что непонимание различий между доменными именами, используемыми в коммерческих целях, и доменными именами, не имеющими таковой цели, повлекло вынесение указанного неверного судебного решения. К сожалению, российские суды с упорством продолжают следовать позиции, заложенной в указанном Постановлении Президиума ВАС РФ, притом что она является очевидно неправильной.

В ситуации, когда чужие фирменное наименование, товарный знак или коммерческое обозначение «включаются» в доменное имя, используемое в *коммерческих целях*, речь, конечно, должна идти о недобросовестной (паразитирующей) конкуренции, ведь налицо использование одним лицом деловой репутации, заработанной другим лицом, с целью получения дополнительной выгоды[2].

Но будет ли аналогичной ситуация, когда в доменное имя, предназначенное для решения исключительно некоммерческих задач, включается (умышленно или по незнанию) чье-то фирменное наименование или товарный знак? По всей видимости, ответ на этот вопрос должен быть отрицательным: включение в доменное имя, не предназначенное для использования в коммерческих целях, фирменного наименования какой-либо компании, товарного знака или коммерческого обозначения не может быть актом недобросовестной конкуренции хотя бы потому, что *владелец такого доменного имени осуществляет его использование* **вне конкурентной среды**. Поэтому в таких случаях нет никаких оснований говорить о конкуренции.

Подобное понимание находило отражение в зарубежной практике. Например, в деле *Bell Expressvu Limited Partnership v. Tedmonds & Co* истец (являющийся правообладателем доменного имени *expressvu.com*) требовал передачи ему доменного имени *expressvu.org* (принадлежащего ответчику), ссылаясь на то, что использование этого доменного имени ответчиком нарушает права истца на товарный знак «*ExpressVu*»[3].

---

[1] *Куликова А.Ю.* Кто в доме хозяин? Современные походы к разрешению споров о столкновении доменного имени и товарного знака // Правовая защита интеллектуальной собственности: проблемы теории и практики: сб. материалов II Международного юридического форума. М., 2014. С. 325.

[2] См. об этом: Защита деловой репутации в случаях ее диффамации или неправомерного использования (в сфере коммерческих отношений) / под общ. ред. М.А. Рожковой.

[3] Bell Expressvu Limited Partnership v. Tedmonds & Co, Reasons for Decision 27/03/2001.

Проанализировав ситуацию, канадский суд учел некоммерческий характер сайта ответчиков, а также наличие на первой странице сайта специального указания на то, что ответчик не связан ни с *Bell Canada Enterprises*, ни с другими его аффилированными лицами: *Bell Expressvu, BCE Media, Bell Canada, Bell Mobility, Bell Canada International*. Суд отметил, что ответчик не продвигает на сайте товары или услуги в качестве конкурента истца, а пропагандирует критику истца как коммерческого производства. Вследствие этого функционально этот сайт реализует свободу слова, которая защищается в силу ст. 2(b) Канадской хартии прав и свобод[1].

Канадский суд подчеркнул, что рассматриваемое им дело существенно отличается от дел *Marks & Spencer plc v. One in a Million* и *Panavision International LP v. Toeppen*, в которых ответчики регистрировали доменные имена с использованием товарного знака другой компании с целью последующей перепродажи доменного имени правообладателю этого товарного знака.

При этом канадский суд обратил внимание на сходство разбираемого им дела с делом № D2000-0190, рассмотренном Центром ВОИС по арбитражу и посредничеству (см. о нем далее). В этом деле предметом третейского разбирательства стала ситуация, когда бывший сотрудник компании *Bridgestone-Firestone* зарегистрировал на себя доменное имя *bridgestone-firestone.net* и разместил на нем сайт, на котором выкладывал документы, посвященные спору с бывшим работодателем. Арбитр по этому делу обращал внимание на то, что основная цель использования доменного имени здесь не коммерческая и состоит в реализации права критиковать истца (бывшего работодателя). Бывший работник не вводит пользователей в заблуждение на своем сайте и его действия не направлены на то, чтобы очернить или запятнать товарный знак бывшего работодателя.

Регистрация домена не с коммерческой целью: нестабильность российской судебной практики

В начале своей деятельности Суд по интеллектуальным правам (далее – СИП) продемонстрировал готовность при рассмотрении доменных споров учитывать цель использования доменного имени. Эта позиция нашла подтверждение в одном из его постановлений.

[1] Образует первую часть Конституционного акта 1982 г.

Установив, что сайт, размещенный на доменном имени *goldstar.ru*, используется его правообладателем С. в личных, научных и образовательных целях, суд отказал компании «Фьюжн Текникс Ко Лимитед» и компании «Голдстар Электроникс Компани Лимитед» в удовлетворении иска о запрете С. использования в доменном имени *goldstar.ru* обозначения «*goldstar*» (сходного до степени смешения с товарными знаками, принадлежащими истцам). При этом суд подчеркнул: «...ответчик не осуществляет какую-либо предпринимательскую или иную экономическую деятельность посредством администрирования доменного имени «www.goldstar.ru». Доказательство обратного суду представлено не было, при этом суд указал, что протокол осмотра указанного сайта в сети Интернет не опровергает доводов ответчика об использовании сайта в личных, некоммерческих целях, в том числе получения и переадресации личной почты»[1].

Но не так давно СИП при рассмотрении конкретного дела неожиданно сделал, в общем, перечеркивающий прежние начинания вывод.

СИП вынес постановление, подтверждающее правильность судебных актов нижестоящих судов, которыми с индивидуального предпринимателя (далее – ИП) в пользу иностранной компании была взыскана компенсация за нарушение исключительных прав – ответчик использовал в доменном имени товарный знак истца[2]. Материалами дела подтверждалось, что истец (иностранная компания) является правообладателем товарного знака «*RIHO*», а ответчик (ИП), зарегистрировавший на свое имя доменное имя *riho.ru*, разместил на этом домене сайт, на котором предлагает к продаже ту же сантехническую продукцию, что и та, для которой зарегистрирован указанный товарный знак истца. При этом, как подчеркивается в постановлении СИП, «ответчик утверждает, что спорное доменное имя, воспроизводящее товарную марку компании, было зарегистрировано предпринимателем и с момента регистрации и по настоящее время используется для продвижения и реализации легально произведенной продукции под товарным знаком истца».

В подобных обстоятельствах нет оснований оспаривать правильность вынесенных по делу решений, в которых суды трех инстанций признали ответчика нарушившим исключительные права истца на товарный знак (подп. 5 п. 2 ст. 1484 ГК РФ).

[1] Постановлении СИП от 01.10.2014 № С01-709/2014 по делу № А40-92932/2013.

[2] Постановление СИП от 06.04.2017 № С01-107/2017 по делу № А41-29186/2016.

Возражения в этом деле вызывают лишь несколько утверждений, пóходя сделанных судом кассационной инстанции безотносительно к рассматриваемому делу.

СИП сформулировал в своем постановлении *общее положение, которое распространяется не только на лиц, осуществляющих предпринимательскую деятельность* (*к числу которых относились истец и ответчик*), *но и вообще всех лиц, коммерческую деятельность не осуществляющих.*

Так, суд указал: «Сам факт размещения в доменном имени обозначения, сходного до степени смешения с принадлежащим истцу товарным знаком, уже свидетельствует о нарушении исключительных прав истца, противоречит требованиям статьи 10-bis Парижской конвенции, согласно которой актом недобросовестной конкуренции считается всякий акт конкуренции, противоречащий честным обычаям в промышленных и торговых делах». И исходя из сказанного заключил: «Согласно закону обычай распространяется не только на сферу предпринимательской деятельности, а также учитывая, что участниками споров в сети Интернет согласно обычаям международной торговли являются лица, не участвующие в предпринимательской деятельности, **акт недобросовестной конкуренции** по использованию доменного имени (регистрации, администрированию, делегированию и другим действиям), тождественного или сходного до степени смешения с товарным знаком или иным средством индивидуализации юридических лиц, товаров, работ, услуг и предприятий, **может быть осуществлен** лицом, не являющимся непосредственным конкурентом на товарном рынке, а также **лицом, не осуществляющим предпринимательской деятельности** (выделено мной. – *М.Р.*)».

Процитированные утверждения представляют собой свободное, «авторское» изложение п. 2 Справки по вопросам, возникающим при рассмотрении доменных споров, утвержденной Постановлением президиума СИП от 28.03.2014 № СП-21/4[1] (далее – Справка № СП-21/4), хотя упоминание самой Справки в постановлении почему-то опущено. Своеобразный вывод СИП, согласно которому *недобросовестную конкуренцию можно ожидать и от лица, не осуществляющего предпринимательскую деятельность и вовсе не выходящего на товарный рынок* (!), позволила сформироваться следующему правилу: «Для размещения

[1] См.: http://ipcmagazine.ru/official-cronicle/the-questions-that-arise-when-considering-domain-disputes

в доменном имени чужого товарного знака нужно согласие правообладателя независимо от цели использования сайта»[1].

Не останавливаясь на самом привнесенном правиле – с учетом предыдущей части настоящей работы он может получить только негативную оценку – нельзя оставить без внимания, возникающие вслед за ним вопросы. Кассационной инстанции, по всей видимости, следовало пойти дальше и дополнительно разъяснить, что делать администраторам доменных имен – физическим лицам, которые не ведут никакой коммерческой деятельности, используют доменное имя для размещения на нем личной страницы (сайта) и лишены всякой возможности зарегистрировать товарный знак, совпадающий с их доменом. Следование правилу, вытекающему из названного постановления СИП, приведет к тому, что они не смогут защитить свое доменное имя от недобросовестного захвата в случае, если оно случайно совпало с товарным знаком коммерческой компании. По сути, для администраторов – физических лиц вероятность защитить свои права на доменное имя стала весьма призрачной, притом что *необоснованное лишение администратора домена доменного имени по сути представляет собой лишение его части принадлежащего ему имущества*.

Права на доменное имя – имущественные права

Доменное имя, рассматриваемое в контексте его функции **средства адресации** в сети Интернет, не может признаваться самостоятельным объектом гражданских прав. Аналогию здесь можно провести с рекламой, которая также является всего лишь средством – средством маркетинга и, вне сомнений, в таком качестве не может выступать объектом гражданских прав[2].

Но если рассматривать доменное имя как упомянутый выше «**идентификатор бизнеса или частных лиц**», то здесь ситуация меняется на прямо противоположную – использование этого идентификатора вполне «способно» принести имущественную выгоду, поэтому его экономи-

[1] См.: http://ipcmagazine.ru/news/3908-news2695

[2] Рекламой определяется как «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» (ст. 3 ФЗ от 13.03.2006 № 38-ФЗ «О рекламе»).

ческая ценность не оспаривается. Подтверждение этому можно найти в практике ЕСПЧ – в деле «*Паеффген против Германии*»[1].

Компания-заявитель (*Paeffgen GmbH*), занимающаяся электронной коммерцией, зарегистрировала на себя несколько тысяч доменных имен. По условиям соглашений, которые компания заключала с национальной регистратурой доменных имен DENIC[2] при регистрации доменов, регистратура не принимала на себя обязанность проверять, не нарушает ли регистрация и использование доменного имени права третьих лиц. Впоследствии несколько лиц обратились в суды с требованиями о запрещении *Paeffgen GmbH* использовать доменные имена, совпадающие с их товарными знаками и коммерческими обозначениями, а также распоряжаться этими доменами. Поскольку ряд судебных разбирательств закончился не в пользу *Paeffgen GmbH*, компания обратилась в ЕСПЧ с жалобой, в которой ссылалась на непропорциональное вмешательство этими судебными решениями в ее право на имущество.

Анализируя факты данного дела, ЕСПЧ прямо указал на то, что права на использование доменов имеют экономическую ценность, и сделал вывод о том, что эти права подпадают под действие ст. 1 Протокола № 1 к Конвенции по правам человека. Иными словами, ЕСПЧ признал права на использование домена в качестве нематериального актива, обладающего бесспорной имущественной значимостью. То есть *права на доменное имя отнесены Судом к имущественным правам*, которые российским законодательством прямо **признаются разновидностью имущества** (ст. 128 ГК РФ).

К сожалению, исходя из того в наименовании и тексте ст. 1 Протокола № 1 к Конвенции по правам человека в переводе ее на русский язык используется слово «собственность»[3], отечественные юристы делают вывод о том, что право на доменное имя следует понимать как право собственности. Такая позиция не учитывает того, что ЕСПЧ

[1] Постановление ЕСПЧ от 18.09.2007 по делу «Паеффген против Германии» (*Paeffgen GMBH v. Germany*; *application no.* 25379/04, 21688/05, 21722/05, 21770/5).

[2] Deutsches Network Information Center.

[3] Так, ст. 1 Протокола № 1 к Конвенции получила название «*Protection of property*», что переведено как «Защита собственности». При этом перевод абз. 1 выглядит следующим образом: «Каждое физическое или юридическое лицо имеет право на уважение своей собственности. Никто не может быть лишен своего имущества, иначе как в интересах общества и на условиях, предусмотренных законом и общими принципами международного права» (официальный перевод текста Протокола № 1 к Конвенции на русский язык был опубликован в: СЗ РФ. 2001. № 2. Ст. 163).

разработана *собственная концепция категории possessions* (упоминаемая в аутентичном тексте ст. 1 Протокола № 1 к Конвенции на английском языке), о чем Суд неустанно напоминает в постановлениях по делам, где рассматриваются вопросы прав на имущество, включая упомянутое дело «Паеффген против Германии».

Концепция имущества (а именно так должен переводиться термин *possessions*), разработанная ЕСПЧ, является новаторской – в ней обобщены передовые тенденции, иногда только намечающиеся в национальных правовых системах европейских стран. Следование этой концепции позволяет ЕСПЧ распространять положения ст. 1 Протокола № 1 к Конвенции на все активы, обладающие экономической ценностью (включая те, которые прямо не признаются объектами гражданских прав в большинстве национальных правовых систем)[1]. Именно об этой концепции упоминается, например, в Постановлении ЕСПЧ «*Васильев и Ковтун против России*»[2] (перевод О.Л. Ветровой): «Концепция «имущества», отраженная в первом абзаце статьи 1 Протокола № 1 к Конвенции, имеет автономное значение, которое не ограничивается правом собственности в отношении материальных вещей и не зависит от формальной классификации по национальному законодательству: некоторые иные права и интересы, представляющие собой активы, могут также рассматриваться как «имущественные права» и, следовательно, как «имущество» по смыслу данного положения. В каждом деле необходимо исследовать вопрос о том, был ли заявитель наделен при обстоятельствах дела, взятых в целом, титулом на действительный интерес, защищенный статьей 1 Протокола № 1 к Конвенции»[3].

Как известно, вещные права (включая право собственности) могут возникать только *в отношении материальных вещей*, тогда как доменное имя со всей очевидностью относится к нематериальным объектам. В подтверждение того, что права на доменное имя нельзя рассматривать в качестве разновидности права собственности, является также, в частности, и *срочный характер регистрации этих прав*.

[1] См.: *Афанасьев Д.В.* Подача жалобы в Европейский Суд по правам человека. М.: Статут, 2012 (СПС «КонсультантПлюс»); *Рожкова М.А.* Понятие «имущество» в правоположениях Европейского Суда по правам человека // Объекты гражданского оборота: сб. ст. / отв. ред. М.А. Рожкова. М.: Статут, 2007. С. 95–112.

[2] Постановление ЕСПЧ от 13.12.2011 по делу «Васильев и Ковтун против России» (*Vasilyev and Kovtun v. Russia*; *application no.* 13703/04) (СПС «КонсультантПлюс»).

[3] СПС «КонсультантПлюс».

Регистрация доменного имени, которая допускается обычно на срок не более 1–2 лет (с правом неоднократного продления), может прекратиться по истечении указанного срока при отсутствии оплаты за продление регистрации – в этом случае информация о доменном имени исключается из реестра, что, в свою очередь, прекращает права на домен.

Недопустимо относить доменное имя к объектам интеллектуальной собственности – на это неоднократно указывала ВОИС[1] (исключительные права предусматривают действие в течение определенного законом срока и на определенной территории, права на доменное имя, в отличие от регистрации доменного имени, не ограничиваются сроком и имеют трансграничный характер). Вследствие сказанного сложно поддержать как разработчиков части четвертой ГК РФ, которые пытались внедрить доменные имена в отечественную систему интеллектуальной собственности[2], так и адептов этой идеи, снова предлагающих включить доменные имена в число объектов интеллектуальной собственности[3].

Отвергая возможность рассмотрения прав на доменное имя в качестве права собственности или исключительных прав, казалось бы, следует согласиться с классификацией этих прав как относительных. Но и признание их относительными правами также имеет возражения.

Право на доменные имена возникает вследствие регистрации домена на имя заинтересованного лица, осуществляемой регистраторами, аккредитованными *Корпорацией по присвоению имен и номеров*

[1] См., например: Интеллектуальная собственность в Интернет: обзор проблем. Женева: ВОИС, 2002. С. 24.

[2] Параграф 5 «Право на доменное имя», который предлагалось ввести в главу ГК РФ, посвященную средствам индивидуализации, содержал ст. 1542 «Доменное имя», в которой закреплялись следующие положения: «1. На доменное имя, то есть символьное обозначение, предназначенное для идентификации информационных ресурсов и адресации запросов в сети Интернет и зарегистрированное в реестре доменных имен в соответствии с общепринятым порядком и обычаями делового оборота (Статья 5), закрепляется исключительное право. 2. Доменное имя состоит из иерархической последовательности наименований доменов, которые являются областями адресного пространства. Каждый из доменов занимает определенный уровень такой иерархической последовательности, причем домен первого уровня включает в себя домены второго уровня, домен второго уровня – домены третьего уровня и т.д. Доменом первого уровня считается домен, наименование которого указано в доменном имени крайним справа».

[3] Такие предложения направлялись, например, на рассмотрение рабочей группы по интеллектуальной собственности Центра компетенций по нормативному регулированию цифровой экономики Сколково.

в Интернете[1] (англ. *Internet Corporation for Assigned Names and Number* (далее – *ICANN*)) или *национальной регистратурой* (см. о ней далее). Иными словами, частное лицо, за которым регистратором зарегистрировано уникальное доменное имя[2], с момента внесения соответствующих сведений в реестр становится обладателем прав на доменное имя (правообладателем доменного имени). При этом на всех третьих лиц накладывается обязанность не препятствовать этому лицу в реализации прав на доменное имя, что позволяет говорить об абсолютном (а не относительном) характере этого права.

Вследствие сказанного правовая природа прав на доменное имя нуждается в дальнейших исследованиях. А на сегодняшний день можно выделить следующие его особенности.

Доменное имя представляет собой нематериальный объект, поэтому **сам домен** – *вследствие естественных свойств – не допускает его передачу* (по той же причине в соответствии с положениями п. 4 ст. 129 ГК РФ исключен оборот объектов интеллектуальной собственности, свойством оборотоспособности обладают лишь права на такие объекты). Таким образом, переход (передача) от одного лица к другому возможен только в отношении (имущественных) **прав на доменное имя**. То же можно сказать относительно возможности обращения взыскания – взыскание может быть обращено лишь на **права** на доменное имя, относящиеся к имущественным правам (что предусматривает ст. 75 ФЗ «Об исполнительном производстве»), но никак не на само доменное имя.

К сожалению, для отечественной практики нередки случаи ошибочного подхода к решению обозначенного вопроса. Так, имел место арест судебным приставом-исполнителем нескольких доменных имен, права на которые принадлежали должнику по исполнительному производству. В дальнейшем судебному приставу-исполнителю удалось добиться того, что арестованные доменные имена были «переданы на реализацию на комиссионных началах, и реализованы». Причем

[1] Некоммерческая организация, зарегистрированная в 1998 г. в Калифорнии, деятельность которой нацелена на обеспечение непрерывного и стабильного функционирования глобальной сети Интернет (https://www.icann.org/).

[2] Зарегистрировать можно только то имя, которое отсутствует в реестре, – регистрация идентичных имен исключена в отличие от товарных знаков, которые могут визуально различаться, притом что буквенное обозначение их будет идентично (см. дело о доменном имени *naturino.ru* – Постановление СИП от 24.09.2014 № С01-246/2014 по делу № А40-149236/2012).

в качестве предмета договора купли-продажи указывалось: продавец (территориальное управление Госимущества) обязуется передать в собственность (!), а покупатель (гражданин) обязуется оплатить и надлежащим образом принять несколько доменных имен; приложением к договору стал акт приема-передачи доменных имен. Проблемы обнаружились тогда, когда приобретатель выяснил, что доменные имена не нуждаются в государственной регистрации, не могут быть «изъяты» и переданы ему в собственность.

Проведенный анализ позволил сделать вывод о том, что права на доменное имя, возникающие и прекращающиеся соответственно в момент внесения соответствующей записи в реестр доменных имен или исключения информации из реестра, включают в свой состав ряд правомочий:

1) **правомочие обладания правами на доменное имя**, означающее наличие этих прав в распоряжении конкретного лица. Именно это правомочие и позволяет реализовывать все называемые далее правомочия – правомочие использования и правомочие распоряжения доменом;

2) **правомочие использования доменного имени**, что подразумевает, в частности, возможность создания поддоменов; создания почтовых ящиков, связанных с доменом или его поддоменами; размещения на домене или поддоменах сайтов; размещения рекламы на доменах, не используемых под сайты; парковки доменов и т.д.

Характеризуя юридическое содержание правомочия использования домена, необходимо отметить, что в отличие от объектов интеллектуальной собственности, которые допускают их одновременное *использование неопределенным кругом лиц*, уникальное доменное имя технически может быть *использовано только одним лицом* – либо самим обладателем прав на доменное имя (уполномоченным им лицом (лицами)), либо лицом, которому право на использование доменного имени предоставлено по договору (уполномоченным им лицом (лицами)).

Все иные лица, осуществляющие, например, поиск информационного ресурса по доменному имени в сети Интернет, не используют домен – они являются *пользователями,* или, иначе, потребителями. Другими словами, речь в этом случае идет не об использовании домена, а об обычном потребительском пользовании сетевыми инструментами. Этот вывод подтверждает следующая цитата: «*О пользовании* можно говорить не только применительно к вещам, но и в отношении нематериальных объектов: это чтение книги, наслаждение музыкой, созерцание картины, поиск нужных сведений в базе данных и т.д.,

и т.п. Пользование – это потребление, освоение, восприятие существа и свойств нематериального продукта, это то, что представляет интерес в первую очередь для потребителя»[1];

3) **правомочие распоряжения правами на доменное имя**. Оно может быть реализовано путем:

– во-первых, *отказа от прав* на доменное имя, которое влечет исключение из соответствующего реестра доменных имен сведений об обладателе прав на конкретное доменное имя и прекращение у него прав на этот домен;

– во-вторых, *отчуждения прав* (*уступки прав*) на доменное имя, предполагающее заключение обладателем прав на доменное имя с другим лицом соглашения, которое становится основанием для внесения в реестр доменных имен изменений и влечет за собой переход прав на доменное имя от первого лица ко второму;

– в-третьих, *предоставления иному лицу права использовать доменное имя* на условиях, предусмотренных соответствующим договором, что не предполагает переход (передачу) прав на доменное имя от одного лица к другому.

Здесь же следует обратить внимание на недопустимость заключения в отношении доменных имен таких договоров, как, например, «*договор купли-продажи доменного имени*» или «*договор аренды доменного имени*» – в силу нематериальной природы доменного имени (исключающей возможность владения и пользования им самим, но только правами на доменное имя). Эта позиция уже находила поддержку в судебной практике. Так, суд апелляционной инстанции в одном из своих решений указал: «...домен не является вещью или средством индивидуализации, не имеет собственников, не может быть передан во временное владение и (или) пользование по договору аренды, в связи с чем договор аренды доменного имени, заключенный между Абрамовым В.В. и ООО «Древ-Град»..., в силу положений ст. 168 ГК РФ является ничтожной сделкой, не порождающей юридических последствий»[2].

Завершая данную часть, надо отметить еще один момент. Лицо, зарегистрировавшее на себя доменное имя, не только обладает правами на зарегистрированный домен, но и несет **соответствующее этому бремя**. Прежде всего речь идет о *необходимых расходах*, которые пред-

[1] *Маковский А.Л.* О кодификации гражданского права (1922–2006). М.: Статут, 2010. С. 617.

[2] Постановление 9ААС Постановление от 26.09.2014 по делу № А40-169281/2013.

стоит понести этому лицу: плата за продление регистрации доменного имени, оплата хостинговых услуг и т.д. К бремени можно отнести и *усилия по администрированию домена*, что подразумевает под собой определение порядка использования доменного имени, а также осуществление организационной и технической поддержки функционирования домена.

Проблема обозначений: *registrar* (аккредитованный регистратор доменных имен) и *registrant* (правообладатель доменного имени)

Как уже указывалось, права на доменное имя возникают у лица только после включения соответствующих сведений в реестр доменных имен. Такая запись вносится *аккредитованным регистратором* (англ. ***registrar***) на основании заключенного с упомянутым лицом договора об оказании услуг, связанных с регистрацией конкретного доменного имени (доменных имен). Но не договор, заключенный регистратором и названным лицом, а только лишь внесение соответствующей информации о доменном имени в реестр порождает права на домен – именно с этого момента данное лицо становится *обладателем прав на зарегистрированное доменное имя* (англ. ***registrant***).

В аутентичном тексте Единой политики рассмотрения споров о доменных именах[1] (англ. *Uniform Domain Name Dispute Resolution Policy* (далее – *UDRP*)) на английском языке лицо, на имя которого зарегистрировано доменное имя, в обобщенном виде обозначается как потребитель (англ. *customer*). Под потребителем предлагается понимать «*владельца доменного имени*», или, иначе, «*регистранта*» (англ. *the domain-name holder or registrant*)[2].

С позиции отечественной доктрины лицо, на имя которого зарегистрирован домен, не может именоваться как «владелец» доменного имени или (тем более) как «владелец регистрации». Это обусловлено тем, что под «владельцем» традиционно понимается лицо, осуществляющее соответствующее правомочие в отношении *вещей материальных*, тогда как в отношении *нематериальных объектов* (к которым как раз

[1] Принята *ICANN* 26.08.1999.

[2] Надо отметить, при переводе *UDRP* на русский язык была допущена серьезная ошибка: в представленном *ICANN* русскоязычном варианте упоминался «*владелец доменного имени* или *регистра**тор***». Неправильный перевод создал предпосылки для ситуаций, когда исковые требования предъявлялись не к лицу, на имя которого зарегистрирован домен (*registrant*), а к самому регистратору (*registrar*).

и относится доменное имя) речь может идти лишь *об обладании* правами, на что уже указывалось выше.

В отечественной практике сложилось так, что *лицо, на которое зарегистрировано доменное имя*, обычно обозначают как «**администратор доменного имени**» («**администратор домена**»). Прямое подтверждение этого можно найти и в судебной практике.

Так, абз. 1 п. 1.2 Справки № СП-21/4, предусмотрено, что требование о пресечении действий, нарушающих права на товарный знак и выражающихся в незаконном использовании доменного имени, может быть предъявлено к *администратору соответствующего доменного имени*. Следующим абзацем того же пункта Справки № СП-21/4 закреплено, что требование о возмещении убытков за незаконное использование в доменном имени товарного знака, равно как и требование о взыскании компенсации, может быть предъявлено как *администратору соответствующего доменного имени*, так и лицу, фактически использовавшему это доменное имя (например, так называемому арендатору домена), – эти лица отвечают солидарно.

Является ли верным наименование, избранное для обозначения лица, на чье имя зарегистрирован домен? Думается, что ответ будет отрицательным в силу следующего.

Если, воспользовавшись сервисом *WHOIS* (от англ. *Who is*? – Кто это?), ввести в строку запроса конкретное доменное имя, то можно получить из реестра доменных имен сведения об этом домене. В частности, в реестре в обязательном порядке содержится информация об именах и наименованиях таких субъектов, как:

– *Registrar* – лицо, включившее данное доменное имя в реестр, т.е. аккредитованный регистратор. Регистратор обязательно указывается в реестре и не подлежит сокрытию настройками приватности (см. о нем далее);

– *Registrant* – лицо, на чье имя зарегистрировано данное доменное имя[1]. То есть речь идет об *обладателе прав на доменное имя* или, иными словами, **правообладателе доменного имени** – именно это понятие и будет использоваться далее в настоящей статье. При включенной настройке приватности нередко вместо *registrant* указывается *Person* (для граждан) и *Org* (для организаций);

– *Admin* (сокр. от *administrator*) – администратор (со стороны правообладателя доменного имени), т.е. контактное лицо по вопросам ад-

[1] В зарубежных литературных источниках он иногда именуется как *owner* (собственник, владелец), что недопустимо с позиций отечественной цивилистики.

министрирования домена, а также вопросов размещения информации и материалов на информационном ресурсе, размещенном на данном домене. В качестве админа, таким образом, могут выступать, например, веб-разработчик или команда копирайта, т.е. те, кто управляет контентом сайта, является лицом, ответственным перед правообладателем доменного имени, или это может быть лицо, с которым правообладатель заключил договор на использование доменного имени, и т.д.;

– *Tech* (сокр. от *technical administrator*) – лицо, отвечающее за техподдержку (со стороны правообладателя доменного имени), т.е. контактное лицо по техническим вопросам. Это может быть, например, сотрудник (подразделение) правообладателя – юридического лица или самостоятельная компания, осуществляющая техподдержку домена на основании договора.

Как показывает практика, в реестре доменных имен достаточно часто одно и то же лицо указывается и как *registrant* (правообладатель доменного имени), и как *admin*, и как *tech* одного домена. Это не запрещается правилами регистрации доменных имен и может быть продиктовано нежеланием правообладателя доменного имени изменять в реестре информацию в случаях смены контактных лиц по вопросам администрирования и техническим вопросам (*admin* и *tech*) или иными соображениями.

Но нередки и случаи, когда в соответствующих полях указаны реальные администраторы домена (*admin*) и техподдержка (*tech*). Для этих случаев следует специально подчеркнуть: *полномочия обладания правами на доменное имя, использования домена и распоряжения правами на доменное имя принадлежат только* **правообладателю доменного имени** (*registrant*). Упомянутые *admin* и *tech*, не обладая никакими правами в отношении самого домена, призваны лишь исполнять соответствующие функции; информация о них включается в реестр (а затем отображается в базе *WHOIS*) для целей контакта по вопросам администрирования и техническим вопросам.

Изложенное позволяет говорить о крайней неудачности широко распространенного в отечественной литературе и практике выражения «администратор доменного имени» для обозначения правообладателя доменного имени. Причем это вовсе не отвлеченная теоретическая проблема – результатом этого является непонимание судьями того, какими правами обладает такой «администратор», и отказ признавать за ним какие-либо субъективные гражданские права, кроме абстрактной возможности администрировать домен.

Кроме того, неудачность наименования правообладателя доменного имени не позволяет судьям разглядеть очевидные различия между владельцем сайта, «администратором доменного имени», хостинг-провайдером, регистратором доменных имен. В итоге судебные решения нередко изобилуют ссылками на нормы и положения, не подлежащие применению к случаям, по которым вынесены эти решения.

Так, на рассмотрение СИП в качестве суда кассационной инстанции поступило дело о запрете размещения сайтов на доменах *oaommk.ru* и *metallgoldline.ru*, взыскании 1 млн руб. компенсации за незаконное использование произведения, товарного знака и фирменного наименования истца, а также публикации судебного решения[1]. Акционерное общество – истец в обоснование своего иска ссылалось на факт создания двух сайтов-двойников его сайта, на которых были указаны контактные данные не истца, а других производителей продукции.

Суды первой и апелляционной инстанций не нашли оснований для удовлетворения иска. В обоснование указывалось, что администратором обоих доменов было физическое лицо (не привлеченное к участию в этом деле), тогда как в качестве ответчиков привлечены другие лица – общество с ограниченной ответственностью и аккредитованный регистратор доменных имен, не являющиеся в данном случае субъектами ответственности.

СИП отменил принятые судами первой и апелляционной инстанций судебные акты, а дело направил на новое рассмотрение, указав на неправильность вывода о том, что регистратор доменных имен в данном случае не является ненадлежащим ответчиком. Ссылаясь на положения ГК РФ об ответственности информационных посредников, СИП заметил: «Требование, направленное на запрет публикации сайта, предъявленное к обществу «РЕГ.РУ» (регистратору доменных имен. – *Прим. М.А.Р.*), по существу судами рассмотрено не было». И далее в постановлении отмечается: «...даже в случае, когда администратор доменного имени не предоставляет услуги хостинг-провайдера, а лишь осуществляет делегирование домена, он, в соответствии с пунктами 6.5, 6.6 Правил регистрации доменных имен в домене «.RU» и «.РФ», утвержденных решением Координационного центра национального домена в сети Интернет от 05.10.2011 № 2011-18/81, может такое делегирование приостановить или прекратить». Комментарии, очевидно, излишни.

[1] Постановление СИП от 09.12.2015 № С01-1000/2015 по делу № А40-52455/2015.

При этом имеют место и иные крайности. Встречаются решения, в которых исключительно «администратор доменного имени» полагается ответственным за действия иных лиц, что вовсе не соответствует логике абз. 2 п. 1.2 Справки № СП-21/4, согласно которому требования о возмещении убытков за незаконное использование в доменном имени товарного знака, требование о взыскании компенсации могут быть предъявлены как «администратору доменного имени», так и лицу, фактически использовавшему это доменное имя, – они отвечают солидарно.

Например, в деле, в рамках которого ИП предъявил к ООО иск о взыскании компенсации за незаконное использование на сайте товарных знаков истца, суды даже не стали исследовать вопрос о том, имел ли ответчик какое-либо отношение к сайту-нарушителю[1]. Суды первой, апелляционной, а затем и кассационной инстанций признали требование не подлежащим удовлетворению по причине предъявления к ненадлежащему ответчику: «Судами установлено, что ответчик не является администратором доменных имен *www.biozdrav.ru* и *www.fujik.ru*. Из справки регистратора следует, что администратором названных доменных имен является третье лицо – общество «Гранит»». И это при том, что из судебных решений не усматривалось, что ответчик каким-либо образом оспаривал свое участие в создании сайта и его использовании для достижения собственных коммерческих целей. Довод о ненадлежащем ответчике повторил и СИП, включивший в свое постановление следующий пассаж: «Поскольку фактическое использование ресурсов сайта невозможно без участия в той или иной форме администратора домена, являющегося лицом, создавшим соответствующие технические условия для посетителей своего интернет-ресурса, владелец домена несет ответственность за содержание размещенной на соответствующем сайте информации».

Сказанное подтверждает тезис о том, что трудности, с которыми приходится сталкиваться правообладателям доменных имен, во многом связаны с проблемой неправильного их обозначения.

Национальная регистратура и аккредитованные регистраторы

Разбор полномочий национальной регистратуры и аккредитованного регистратора (*registrar*) нужно предварить кратким обзором состава доменного имени.

[1] Постановление СИП от 10.02.2015 № С01-1379/2014 по делу № А40-177543/2013.

Как известно, полное доменное имя включает в себя имена нескольких доменов – начиная с доменов более высокого уровня (родительских доменов) и затем переходя к доменам последующих уровней, причем *состав доменных имен раскрывается справа налево*.

I. **Корневой домен** (англ. *root domain*), называемый иногда доменом нулевого уровня, который не имеет имени и обозначается в полном доменном имени точкой.

II. **Домены первого (верхнего) уровня** (англ. *Top-Level Domain*; далее – ***TLD***). Это:

– **национальные и региональные домены** (англ. *Country-Code Top-Level Domain*; далее – ***ccTLD***), которые создаются специально для стран и отдельных территорий и выражаются двухсимвольным кодом страны или соответствующей территории (региона): *.ru* (Россия); *.us* (США); *.de* (Германия); *.fr* (Франция); *.lt* (Литва); *.cc* (Кокосовые острова); *.aq* (Антарктида) и т.п.;

– **домены общего назначения** (англ. *Generic Top-Level Domain*; далее – ***gTLD***), которые были созданы для использования их какими-либо сообществами или определенного класса организациями. Это, например: *.com* (от англ. *commercial*; изначально – для коммерческих организаций); *.biz* (от англ. *business*; для коммерческих организаций); *.org* (от англ. *organization*; для некоммерческих организаций); *.net* (от англ. *network*; для сетевых структур) и т.п.[1];

– **новые домены общего назначения** (англ. *New Generic Top-Level Domain*; далее – ***New gTLD***) могут быть зарегистрированы за юридическим лицом (в частности, коммерческой компанией), некоммерческой организацией или органом власти государства по результатам аукциона. Это, например: *.cloud* (зона «облачных» сервисов); *.xxx* (зона ресурсов порнографического содержания); *.day* (домены для всех особенных дней); *.vodka* и т.д.

III. **Домены второго уровня** (англ. *Second-Level Domain*; далее – ***SLD***). Среди доменов второго уровня, входящих в доменную зону *.ru*, можно упомянуть, в частности, *yandex.ru*, *mail.ru*, *zakon.ru*, *pravo.ru*

IV. **Домены третьего уровня** (в качестве таковых можно назвать такие домены третьего уровня, как *news.yandex.ru* (Яндекс-новости), *torg.mail.ru* (товары на mail.ru), cases.pravo.ru (база судебных дел на *pravo.ru*) и т.п.

[1] Изначально было создано всего восемь *gTLD* (*.com, .net, .org, .int, .edu, .gov, .mil, .arpa*), затем в 2001 г. появилось еще семь (*.info, .biz, .name, .coop, .museum, .aero, .pro*).

Таким образом, например, полное доменное имя *ru.wikipedia.org*, обозначающее русскоязычную зону Википедии, включает в себя, во-первых, домен нулевого уровня (.), во-вторых, домен первого уровня (общего назначения) *.org*, в-третьих, домен второго уровня *wikipedia.org* и, наконец, в-четвертых, домен третьего уровня *ru.wikipedia.org*.

Важно подчеркнуть, что домены первого (верхнего) уровня распределяются (делегируются) *ICANN*, а регистрация осуществляется аккредитованными регистраторами в отношении доменов второго уровня (домены третьего и последующего уровней обычно не регистрируют, но встречаются и исключения из общего правила).

ICANN делегирует права по администрированию ***ccTLD*** соответствующим организациям (редко – гражданам), становящимся вследствие этого *администраторами национального либо регионального домена первого уровня*. В связи с этим на них возлагается обеспечение функционирования этих доменов.

Так, администратором национальных доменов *.ru* и *.рф* является Координационный центр национального домена сети Интернет[1]; домена *.su* – Фонд развития Интернет[2]; национального домена *.de* – некоммерческая организация *DENIC*[3]; национального домена *.lt* – Каунасский технологический университет[4]; домена *.aq* – Питер Мотт (Новая Зеландия). Осуществляя свои полномочия, администраторы национальных доменов разрабатывают необходимые регламентирующие правила (например, по регистрации в национальной доменной зоне доменов второго уровня (***SLD***)[5], об альтернативных способах урегулирования возникающих споров о доменных именах[6] и пр.), в которых учитывается общая политика *ICANN* в отношении ***ccTLD***.

Администратор национального домена исполняет функцию **национальной регистратуры**, осуществляя поддержку реестра, содержащего сведения о ***SLD,*** зарегистрированных в национальной доменной зоне, а также обеспечение функционирования этих имен в Интернете. При этом администратор национального или регионального домена, как

[1] См.: http://www.cctld.ru/

[2] См.: http://www.fid.su/

[3] *Domain Verwaltungs- und Betriebsgesellschaft eG* (http://www.denic.de/).

[4] http://www.domreg.lt/

[5] См., например: Правила регистрации доменных имен в доменах .RU и .РФ (http://www.cctld.ru/files/pdf/docs/rules_ru-rf.pdf?v=2).

[6] См., например: Положение «О процедурах, подлежащих применению при возникновении споров о доменных именах» (http://www.cctld.ru/files/pdf/docs/litigations.pdf).

правило, сам не является регистратором (прямая регистрация доменного имени через него невозможна), а предоставляет право регистрации ***SLD*** в реестре *регистраторам, получившим у него (администратора) соответствующую аккредитацию*.

Регистраторы, аккредитованные администратором национального или регионального домена, оказывают заинтересованным лицам услуги по регистрации ***SLD***[1]. Регистраторы, не имеющие аккредитацию администратора национального или регионального домена, есть лишь *посредники* между заинтересованным лицом и аккредитованным регистратором.

gTLD, как указывалось выше, создаются обычно для использования их какими-либо сообществами или определенного класса организациями и выражаются кодом, в котором используется три и более символов.

В июне 2011 г. *ICANN* запущена программа ***New gTLD***[2], в рамках которой новый домен общего назначения может быть зарегистрирован юридическим лицом (в частности, коммерческой компанией), некоммерческой организацией или органом власти государства.

Делегирование ***New gTLD*** осуществляется по результатам частного аукциона: с победителем аукциона *ICANN* подписывает соответствующее соглашение. Так, корпорация *Google* приобрела права на новый домен *.app* (от англ. *application* – приложение)[3]; американской компании *Amazon* был делегирован новый домен *.book*; итальянской компании *Aruba* – домен *.cloud*; отечественному Фонду содействия развитию технологий и инфраструктуры Интернета – домены *.moscow* и *.москва*. В соответствии с этим соглашением компания-победитель, как **оператор реестра нового домена общего назначения**, принимает на себя обязанности по поддержке реестра, содержащего сведения о зарегистрированных в этой доменной зоне доменов второго уровня, а также по обеспечению функционирования этого реестра. При этом оператор реестра ***New gTLD*** вправе предоставлять доступ к реестру только *регистраторам, получившим аккредитацию ICANN*.

Таким образом, в отличие от регистраторов, оказывающих услуги по регистрации ***SLD*** в *национальной доменной зоне* (для чего необходима

[1] Следует отметить, что некоторые администраторы национальных доменов разрешают такую регистрацию только гражданам соответствующей страны или местным предприятиям, обладающим созвучным товарным знаком.

[2] См.: http://newgtlds.icann.org/en/

[3] Как пишет The Business, Insider Google предложил на аукционе рекордную сумму в 25 млн долл. (см.: http://finance.yahoo.com/news/google-just-paid-25-million-234008295.html;_ylt=AwrBJR7LEPBUwD4AEjjQtDMD).

аккредитация администратора национального или регионального домена), регистраторы, оказывающие услуги по регистрации доменных имен второго уровня в зоне ***New gTLD,*** нуждаются в получении аккредитации самой *ICANN* (посредством заключения с *ICANN* Соглашения об аккредитации Регистратора). Здесь же следует добавить, что один и тот же регистратор может быть аккредитован как *администратором национального или регионального домена*, так и *ICANN*, что позволит ему осуществлять регистрацию доменных имен второго уровня как в национальной доменной зоне, так и в зоне доменов общего назначения.

Продолжение см. в статье: М.А. Рожкова, Д.В. Афанасьев «Доменные споры: избранные аспекты».

Пристатейный библиографический список:

1. Final Report of the WIPO Internet Domain Name Process «The Management of Internet Names and Addresses» 30.04.1999 (http://www.wipo.int/amc/en/processes/process1/report/index.html).

2. Интеллектуальная собственность в Интернет: обзор проблем. Женева: ВОИС, 2002.

3. *Рожкова М.* Идентификаторы: все ли надо относить к объектам интеллектуальной собственности? // Хозяйство и право. 2015. № 2.

4. Защита деловой репутации в случаях ее диффамации или неправомерного использования (в сфере коммерческих отношений) / авт. колл. Рожкова М.А., Афанасьев Д.В., Глазкова М.Е. и др.; под общ. ред. М.А. Рожковой. М.: Статут, 2015.

5. *Куликова А.Ю.* Кто в доме хозяин? Современные походы к разрешению споров о столкновении доменного имени и товарного знака // Правовая защита интеллектуальной собственности: проблемы теории и практики: сб. материалов II Международного юридического форума. М., 2014.

6. *Маковский А.Л.* О кодификации гражданского права (1922–2006). М.: Статут, 2010.

7. *Афанасьев Д.В.* Подача жалобы в Европейский Суд по правам человека. М.: Статут, 2012 (СПС «КонсультантПлюс»).

8. *Рожкова М.А.* Понятие «имущество» в правоположениях Европейского Суда по правам человека // Объекты гражданского оборота: сб. ст. / отв. ред. М.А. Рожкова. М.: Статут, 2007.

М.А. Рожкова,
Д.В. Афанасьев

ДОМЕННЫЕ СПОРЫ: ИЗБРАННЫЕ АСПЕКТЫ[1]

Аннотация. *Статья посвящена анализу альтернативного рассмотрения доменных споров. Авторы затрагивают вопросы правовой природы аккредитованных арбитражных центров, разрешающих этот особый вид дел, – споры в отношении доменных имен в соответствии с процедурой UDRP (Единая политика рассмотрения споров о доменных именах).*

Ключевые слова: *доменное имя, арбитражное соглашение, разрешение споров, процедура UDRP, арбитражный центр.*

Возможность по собственному усмотрению распорядиться правами на доменные имена создала условия для использования в коммерческой практике «грабительских и паразитических способов», под которыми понимается «преднамеренная, недобросовестная регистрация в качестве доменных имен знаменитых и других товарных знаков в надежде продать доменные имена владельцам этих знаков или недобросовестным образом воспользоваться преимуществами репутации, принадлежащей этим знакам» (п. 23 упоминавшегося доклада ВОИС по доменным именам[2]).

В связи с этим Й. Курбалийя отмечает следующее: «На заре Интернета регистрация доменных имен основывалась на принципе «первым пришел – первым обслужили», что в результате породило явление, известное как киберсквоттинг[3]: регистрация доменных имен с целью

[1] Статья является продолжением статьи М.А. Рожковой «Права на доменные имена.

[2] Final Report of the WIPO Internet Domain Name Process «The Management of Internet Names and Addresses» 30.04.1999 (http://www.wipo.int/amc/en/processes/process1/report/index.html).

[3] Киберсквоттинг (от англ. *cybersquatting* – киберзахват) – регистрация доменного имени, содержащего товарный знак, фирменное наименование или иное различительное обозначение, права на которые принадлежат другому лицу, с целью дальнейшей перепродажи этого доменного имени или его недобросовестного использования. Лица, осуществляющие киберсквоттинг, называются киберсквоттерами: это название произошло от англ. *squatter* – лицо, незаконно захватывающее чужую землю или поселяющееся в чужом доме.

их последующей перепродажи»[1]. Эта проблема нашла отражение и в документе ВОИС «Основы электронной коммерции и вопросы интеллектуальной собственности», где подчеркивается: «Конфликт (между системой имен и системой интеллектуальной собственности. – *Прим. М.Р., Д.А.*) усилился из-за отдельной практики, связанной с лицами, недобросовестно регистрирующими в качестве доменных имен различительные обозначения, особенно товарные знаки, с целью последующей продажи их владельцам идентификаторов, или просто используя нечестным образом преимущества доброго имени, ассоциированного с ними»[2].

В ситуациях, когда зарегистрированное доменное имя включает в себя чужое фирменное наименование, коммерческое обозначение, товарный знак или знак обслуживания, у правообладателей появляются основания требовать защиты их нарушенных исключительных прав. Дела, возникающие из требований правообладателя о пресечении неправомерного использования в доменном имени обозначения, совпадающего с фирменным наименованием, коммерческим обозначением, товарным знаком или знаком обслуживания, в отечественной юридической литературе принято именовать **доменными спорами**.

Но перечисленные дела – лишь одна из разновидностей дел о доменных именах. Круг дел, подпадающих под понятие «доменный спор» (дело по поводу доменного имени), гораздо шире. Причем в него попадают не только споры, возникающие из частных правоотношений, но и дела, возникающие из отношений публичных.

Так, доменные споры возникают, в частности, вследствие утраты «администратором доменного имени» (правообладателем доменного имени) права на доменное имя по причине несвоевременной оплаты им продления регистрации[3] или оспаривания сделки по передаче доменного имени от одного лица другому[4]. К делам по поводу доменных имен можно отнести и дела публично-правового толка, в рамках которых решается вопрос, например, о признании аккредитованного регистратора виновным в недобросовестной конкуренции при реги-

[1] *Курбалийя Й.* Управление Интернетом. М.: Координационный центр национального домена сети Интернет, 2010. С. 50.

[2] Интеллектуальная собственность в Интернет: обзор проблем. С. 99.

[3] См., например, постановление ФАС Московского округа от 17.12.2013 по делу № А40-98343/2012.

[4] См., например, постановления Девятого ААС от 22.07.2010 № А40-158243/09-83-1009, от 07.08.2008 по делу № А40-58671/07-67-480.

страции доменов[1] или об отмене решения национального регистратора о внесении изменений в положение о регистрации[2].

В рамках настоящей статьи будут рассматриваться доменные споры в узком их значении – как дела, возникающие по поводу доменных имен в связи с защитой правообладателями принадлежащей им интеллектуальной собственности.

UDRP, а также разработанные на ее основе Правила *UDRP* (англ. *Rules for Uniform Domain Name Dispute Resolutio Policy*)[3] определяют процедуру альтернативного рассмотрения дел, касающихся доменных имен и товарных знаков (знаков обслуживания). В соответствии с процедурой рассматриваются дела, в рамках которых по требованию правообладателя товарных знаков (знаков обслуживания) оспаривается регистрация ***gTLD***.

Следует специально обратить внимание на то, что процедура *UDRP* предназначена для разбирательства не всех дел. Например, эта процедура не предполагает использования при рассмотрении дел, связанных с хищением доменов.

Так, Центр ВОИС по арбитражу и посредничеству решил, что процедура *UDRP* не распространяется на дело, в рамках которого истцы заявляли о похищении у них 74 доменных имен (в частности, *bx111222.com*, *bx222333.com*, *bx333444.com*, *long33333.com*, *long44444.com*, *long55555.com* и т.д.), что было осуществлено путем взлома их учетной записи у регистратора[4]. Обосновывая свои требования, истцы ссылались на использование доменов в недобросовестных целях и отсутствие у ответчика законного интереса в отношении похищенных доменных имен. Центр ВОИС по арбитражу и посредничеству указал, что прежде всего необходимо установить, что доменное имя идентично или схоже с товарным знаком или знаком обслуживания истца. Но истцы не смогли подтвердить сходства с товарными знаками (ввиду отсутствия у них прав на какие-либо товарные знаки), а также приобре-

[1] Так, Федеральная антимонопольная служба России (ФАС России) установила, что регистратор доменных имен *Ru-Center* участвовал в сговоре с пятью компаниями, следствием чего стал раздел рынка регистрации доменов. По итогам данного дела ФАС России предписала регистратору уплатить штраф в размере около 240 млн руб. за недобросовестную конкуренцию.

[2] См., например: решение АС г. Москвы от 09.03.2011 по делу № Ф40-88153/1022-792.

[3] Утверждены Правлением *ICANN* 30.10.2009.

[4] http://www.wipo.int/amc/en/domains/search/text.jsp?case=D2017-0289

тения спорными доменными именами различительной способности в результате рекламы или использования доменных имен для продаж. В результате Центр ВОИС по арбитражу и посредничеству признал, что утверждения о хищении доменных имен находятся за пределами действия *UDRP* и за пределами компетенции самого Центра.

Вместе с тем альтернативное рассмотрение доменных споров регламентируется не только *UDRP* и разработанными на ее основе Правилами.

Так, споры в доменной зоне *.uk* (Соединенное Королевство) допускают их урегулирование на основании одной из процедур *DRS (Dispute Resolution Service*), разработанных организацией *Nominet,* являющейся администратором национального домена *.uk*. При этом на первом этапе *Nominet* выступает в качестве бесплатного медиатора в целях урегулирования доменного спора[1]. В случае, если дело не было урегулировано посредством медиации или правообладатель доменного имени не предоставил ответ в установленный срок, назначается один арбитр (именуемый экспертом), решение которого признается обязательным к исполнению в отношении доменного имени.

Споры в доменной зоне *.pl* (Польша) рассматриваются в соответствии с регламентами Польской торговой палаты или Польской палаты информационных технологий и телекоммуникаций при условии, что хотя бы один из участников доменного спора имеет местонахождение на территории Польши. Если ни одна из сторон спора не подпадает под это условие, спор может быть рассмотрен Центром ВОИС по арбитражу и посредничеству в соответствии с Регламентом ускоренного арбитража в целях разрешения споров о доменном имени *.pl.*

Следует отметить, что разбирательство доменных споров согласно *UDRP* должно производиться **арбитражным институтом**, который специально уполномочен (аккредитован) *ICANN*. Таких арбитражей, аккредитованных *ICANN*, или, как их принято именовать «аккредитованных арбитражных центров», на сегодняшний день насчитывается пять:

– Центр ВОИС по арбитражу и посредничеству, уже неоднократно упоминавшийся;

– Национальный арбитражный форум (США) (англ. *National Arbitration Forum*);

[1] См. об этом: https://www.nominet.uk/domains/resolving-uk-domain-disputes-and-complaints/#guidance

– Азиатский центр по рассмотрению споров о доменных именах (англ. *Asian Domain Name Dispute Resolution Centre*);

– Арбитражный центр Чешского арбитражного суда по рассмотрению споров, связанных с Интернетом (англ. *the Czech Arbitration Court Arbitration Center for Internet Disputes*);

– Арабский центр по рассмотрению споров о доменных именах (англ. *Arab Center for Domain Name Dispute Resolution*).

Все аккредитованные арбитражные центры при разбирательстве доменных споров должны руководствоваться едиными положениями, сформулированными в *UDRP,* и разработанными на ее основе Правила; при этом в каждом из центров – собственные правила рассмотрения доменных споров, основанные на *UDRP*; в каждом из центров возможно заочное рассмотрение доменного спора – без явки сторон, только на основании представленных документов.

Например, Арбитражный центр Чешского арбитражного суда по рассмотрению споров, связанных с Интернетом, уполномочен *ICANN* на рассмотрение споров в отношении не только национального домена Чехии – *.cz*, но и доменной зоны Европейского союза – *.eu*, национальных доменов *.co* и *.nl*, а также доменным зон *.com, .net, .org, .biz* и многих других[1].

Правообладатель, который полагает, что зарегистрированный домен нарушает его права на товарный знак, вправе выбрать наиболее удобный для него аккредитованный арбитражный центр (*forum-shopping*).

Так, в 2016 г. компания *Google* обратилась в Арбитражный центр Чешского арбитражного суда по рассмотрению споров, связанных с Интернетом, с требованием передать ей права на домен *google-statistics.eu,* который был зарегистрирован на гражданина России. Арбитражный центр, руководствуясь выработанными *ICANN* правилами для разрешения доменных споров, аннулировал права ответчика на домен и передал права на него компании *Google.* Примечательно, что в этом деле аккредитованный арбитражный центр учел не только предыдущее собственное решение в пользу компании *Google* по домену *googles.eu*, но и решение, вынесенное в пользу компании *Google* Национальным арбитражным форумом по доменному имени *google-status.com*.[2]

[1] См. подробнее о компетенции Арбитражного центра Чешского арбитражного суда по рассмотрению споров, связанных с Интернетом: http://eu.adr.eu/about_us/other_domains/index.php

[2] См. решение: http://eu.adr.eu/adr/decisions/decision.php?dispute_id=7127

Сказанное не означает, что все споры по поводу доменных имен, в которых заявителем выступает *Google,* решаются в ее пользу. Так, компания *Google* обратилась в Национальный арбитражный форум по поводу домена *Groovle.com*, принадлежащего канадской компании *207 Media*, полагая, что это доменное имя сходно до степени смешения с товарным знаком «*Google*». Однако решением этого арбитражного форума в удовлетворении требования было отказано – арбитры сочли, что название доменного имени отличается от товарного знака «*Google*», что позволяет избежать путаницы[1]. В то же время компания *Google* выиграла в Центре ВОИС по арбитражу и посредничеству другое дело – в отношении доменного имени *google.ir*, принадлежавшего гражданину Ирана[2].

Наиболее известным из аккредитованных арбитражных центров, бесспорно, является Центр ВОИС по арбитражу и посредничеству. Он основан в 1994 г. с целью содействовать альтернативному рассмотрению споров прежде всего в области интеллектуальной собственности, но под его юрисдикцию подпадают и различные доменные споры, причем количество доменных споров неуклонно повышается. Так, в начале 2017 г. ВОИС опубликовала информацию о разрешенных в 2016 г. доменных спорах: за год в порядке *UDRP* было рассмотрено 3036 жалоб, что на 10% превысило результат 2015 г.[3] Примечательно, что чаще всего (в 67% случаях) заявляются требования в отношении домена *.com*[4]*,* и лишь затем идут требования о *.xyz, .net, .top, .org.*

Для разбирательства споров Центром ВОИС по арбитражу и посредничеству разработан целый ряд процедур, к которым, в частности, относятся:

1) *процедура арбитража по делам в сфере интеллектуальной собственности* – процедура рассмотрения и разрешения спора одним или несколькими арбитрами, которая заканчивается вынесением обязательного для сторон решения;

---

[1] См. о нем: http://www.networkcomputing.com/networking/google-loses-groovle-domain-name-dispute/323485872. Это одно из немногих доменных споров, которые Google проиграла.

[2] См. решение Центра ВОИС по арбитражу и посредничеству: http://www.wipo.int/amc/en/domains/decisions/html/2005/dir2005-0001.html

[3] https://cctld.ru/ru/press_center/digest/detail.php?ID=11411.

[4] В доменной зоне *.com* больше всего зарегистрированных доменов второго уровня – почти каждая крупная компания стремится получить такой домен. Но эта зона не только самая многочисленная по количеству зарегистрированных доменов второго уровня, на доменах этой зоны размещено большинство самых посещаемых информационных ресурсов мирового киберпространства.

2) *процедура ускоренного арбитража по делам в сфере интеллектуальной собственности* – процедура арбитража, особенность которой – в оперативности рассмотрения и разрешения дела;

3) *процедура посредничества по делам в сфере интеллектуальной собственности* – процедура, в рамках которой нейтральный посредник помогает сторонам достичь урегулирования спора (обязательное для сторон решение не выносится);

4) *процедура посредничества по делам в сфере интеллектуальной собственности, за которым при недостижении урегулирования следует арбитраж* – процедура, которая начинается как посредничество, но при отсутствии результата переходит в процедуру арбитража;

5) *процедура арбитража по доменным спорам в соответствии с UDRP*;

5) *другие процедуры арбитража в отношении New gTLD*;

6) *процедуры арбитража в отношении национальных ccTLD*.

Компетенция арбитража на рассмотрение доменного спора в соответствии с UDRP. Компетенция государственного суда на пересмотр этого же спора

Под юрисдикцию вышеперечисленных аккредитованных арбитражных центров обычно подпадают споры, касающиеся использования в доменных именах чужих объектов интеллектуальной собственности, в частности товарных знаков и знаков обслуживания. Причем компетенция этих арбитражных центров на рассмотрение таких споров возникает не из традиционного, подписанного сторонами **арбитражного (третейского) соглашения**, а вследствие иных фактов. Рассмотрим их подробнее.

Заинтересованное лицо обращается к регистратору с целью зарегистрировать доменное имя, вследствие чего этими лицами заключается договор оказания услуг по регистрации доменного имени. Неотъемлемая (обязательная) часть любого такого договора – *UDRP* и Правила *UDRP,* а иногда и иные правила, относящиеся к регистрации и использованию конкретных доменов первого (верхнего) уровня. Таким образом, в результате заключения упомянутого договора аккредитованный регистратор (*Registrar*) и правообладатель доменного имени (*Registrant*) *оказываются связанными третейской оговоркой, в соответствии с которой споры о доменном имени рассматриваются в аккредитованном арбитражном центре*.

Но еще более важно то, что эта третейская оговорка распространяется не только на случаи возникновения спора между регистратором и правообладателем доменного имени. Она обязательна для правообладателя доменного имени и в случаях, когда в соответствующий арбитраж с требованием к этому правообладателю обращается третье лицо, ссылающееся на то, что зарегистрированное доменное имя нарушает его права[1]. Это прямо закреплено в § 3(a) Правил *UDRP*, согласно которому любое физическое или юридическое лицо может инициировать разбирательство в соответствии с *UDRP* и Правилами *UDRP*, направив свое требование в любой аккредитованный арбитражный центр по собственному выбору.

Иными словами, аккредитованный арбитражный центр может быть компетентен рассматривать доменный спор и в том случае, если с иском обращается лицо, которое по отношению к соглашению между правообладателем доменного имени (*Registrant*) и регистратором (*Registrar*) является **третьим лицом**, не подписавшим арбитражную оговорку. Обычно это ситуации, когда правообладатель товарного знака обращается в аккредитованный арбитражный центр, поскольку полагает, что регистрация и использование доменного имени, сходного с его товарным знаком, нарушают его права.

То обстоятельство, что правообладатель товарного знака является третьей стороной применительно к соглашению между регистратором и правообладателем доменного имени (так как он не подписывал непосредственно само соглашение, содержащее арбитражную оговорку), зачастую служит основанием для ошибочного вывода об отсутствии арбитражного соглашения как такового[2].

Между тем арбитражное соглашение по доменным спорам в соответствии с процедурой *UDRP* заключается следующими способами:

– со стороны правообладателя доменного имени (ответчика) – путем подписания соглашения (договора присоединения), содержащего арбитражную оговорку о передаче всех доменных споров на разрешение аккредитованного арбитражного центра в соответствии с *UDRP* и Правилами *UDRP,* в случае предъявления третьими лицами требований к правообладателю доменного имени;

– со стороны правообладателя товарного знака (истца) – путем предъявления соответствующего иска в аккредитованный арбитраж-

[1] Речь идет о доменных именах второго уровня в некоторых *gTLD* и во всех *New gTLD.*

[2] См., например: *Gün M., Hançer H.* Arbitrating Intellectual Property Disputes // *Ismael Esin, Ali Yesilirmak*. Arbitration in Turkey // Kluwer Law International. 2015. P. 292.

ный центр, что означает его согласие с компетенцией данного арбитража на рассмотрение доменного спора.

Таким образом, стороны доменного спора не подписывают напрямую арбитражное соглашение, но оно заключается между ними иным образом: со стороны ответчика – путем подписания договора присоединения, содержащего арбитражную оговорку, а со стороны истца – предъявлением соответствующего иска.

Это заключение не противоречит действующему законодательству о третейском разбирательстве. Так, ч. 4 ст. 7 ФЗ от 29.12.2015 № 382-ФЗ «Об арбитраже (третейском разбирательстве) в Российской Федерации» предусмотрено, что арбитражное соглашение считается заключенным в письменной форме, если оно заключено путем обмена процессуальными документами (в том числе подачей искового заявления), в которых одна из сторон заявляет о наличии соглашения, а другая против этого не возражает. Аналогичная норма содержится в ч. 5 ст. 7 Закона РФ от 07.07.1993 № 5338-I «О международном коммерческом арбитраже»[1].

Следует отметить, что в соответствии с ранее действовавшим ФЗ от 24.07.2002 № 102-ФЗ «О третейских судах в Российской Федерации» арбитражная оговорка, включенная в договор присоединения, не имела юридической силы – на основании ч. 3 ст. 5 этого Закона она признавалась недействительной. Именно эта норма стала препятствием для включения в Правила регистрации доменных имен в домене *.ru* и *.рф*, утвержденных Координационным центром национального домена в сети Интернет, возможности передачи на рассмотрение третейских судов доменных споров в зоне *.ru* и *.рф*.

В развитие сказанного следует обратить специальное внимание на § 4(k) *UDRP,* согласно которому правообладатель товарного знака или правообладатель доменного имени **до начала разбирательства** по *UDRP* или **после завершения такого разбирательства** вправе обратиться в компетентный государственный суд.

Данная норма часто трактуется как подтверждающая отсутствие арбитражного соглашения применительно к правообладателю доменного имени. При этом отмечается, что существование договора между правообладателем доменного имени и регистратором о рассмотрении

[1] См. *Афанасьев Д.В.* Комментарий к гл. 30, 31 Арбитражного процессуального кодекса РФ // Арбитражный процессуальный кодекс Российской Федерации с постатейными материалами судебной практики и комментариями / под ред. Т.К. Андреевой. М.: Статут, 2013 (СПС «КонсультантПлюс»).

доменных споров в соответствии с процедурой *UDRP* не имеет для правообладателя товарного знака дерогационного эффекта и не препятствует ни правообладателю доменного имени, ни тем более правообладателю товарного знака предъявить иск в отношении доменного имени в государственный суд[1].

Между тем суть закрепленного в § 4(k) *UDRP* правила в другом: доменный спор, *уже находящийся на рассмотрении в аккредитованном арбитражном центре*, не может быть передан на разрешение государственного суда **в период его разбирательства арбитражным центром,** т.е. *с момента начала разбирательства этого спора и до момента его завершения арбитражным центром*. До начала такого разбирательства или по окончании разбирательства аккредитованным арбитражным центром доменный спор может быть передан на рассмотрение государственного суда.

Таким образом, оговорка о рассмотрении всех доменных споров по процедуре *UDRP* (в договоре с регистратором) препятствует обращению правообладателя доменного имени в государственный суд **во время разбирательства** доменного спора аккредитованным арбитражным центром. Аналогичным образом правообладатель товарного знака не вправе обращаться в компетентный государственный суд **параллельно с разбирательством** доменного спора, ведущемуся аккредитованным арбитражным центром, после того как этот правообладатель признал компетенцию этого центра (посредством обращения с соответствующим иском). В противном случае возникает проблема *lis alibi pendens* – когда спор об одном и том же предмете между одними и теми же сторонами рассматривается в двух компетентных органах одновременно.

Важно заметить, что по окончании разбирательства доменного спора аккредитованным арбитражным центром проблема *lis alibi pendens* не снимается окончательно (см. об этом далее).

Как уже указывалось, у правообладателя товарного знака есть возможность предъявить требование по доменному спору **в государственный суд до начала** *разбирательства этого спора в аккредитованном арбитражном центре* в рамках *UDRP.* Если правообладатель товарного знака предъявит такое требование в государственный суд, это будет

[1] *Mareš A.* The Arbitrator and the Arbitration Procedure – «.EU Arbitration»: Solving .eu Domain Names Disputes in Prague / Gerold Zeiler, Irene Welser et al. (eds.) // Austrian Yearbook on International Arbitration. Vol. 2009. Manz'sche Verlags- und Universitätsbuchhandlung, 2009. P. 323.

свидетельствовать лишь об отсутствии у него намерения, чтобы *аккредитованный арбитражный центр* рассматривал его дело.

Но вынесение *аккредитованным арбитражным центром* решения по доменному спору не исключает для правообладателя товарного знака, равно как и для правообладателя доменного имени, возможность последующего обращения в государственный суд за разрешением этого же спора. То есть **после завершения** *разбирательства по правилам UDRP и вынесения аккредитованным арбитражным центром решения по доменному спору* и правообладатель товарного знака, и правообладатель доменного имени (в зависимости то того, кто является проигравшим в споре) могут обратиться **в компетентный государственный суд** с требованием в отношении этого же доменного имени.

Параграф 4(k) *UDRP* наделяет правообладателя доменного имени правом в течение **10 рабочих дней** после завершения разбирательства по *UDRP* представить в аккредитованный арбитражный центр документы об обращении в государственный суд по поводу того же спорного доменного имени (например, копию заявления в компетентный государственный суд). Если в этот срок никакие документы правообладателем не представляются, решение аккредитованного арбитражного центра подлежит исполнению.

Если же правообладатель доменного имени в течение указанного срока представил документы о начатом им судебном разбирательстве в государственном суде в отношении доменного имени, которое было предметом рассмотрения в аккредитованном арбитражном центре, то решение центра не исполняется до получения, в частности:

– удовлетворительных доказательств, подтверждающих урегулирование доменного спора между сторонами;

– удовлетворительных доказательств, подтверждающих отказ в удовлетворении требований правообладателя доменного имени или его отказ от иска;

– копии судебного акта об отклонении требований правообладателя доменного имени либо о его признании, что он не вправе более пользоваться доменным именем.

Очевидно, что в таких условиях разрешение доменного спора по *UDRP* не решает проблемы *lis alibi pendens*.

Это можно увидеть на примере спора о доменном имени *denso.com*, который первоначально был рассмотрен Центром ВОИС по арбитражу и посредничеству.

Иск был заявлен правообладателем товарного знака «*Denso*» к российской компании – ООО «ДенСо», являющемуся правообладателем доменного имени *denso.com*. По результатам процедуры *UDRP* Центр ВОИС по арбитражу и посредничеству признал требование правообладателя товарного знака «*Denso*» о передаче спорного доменного имени подлежащим удовлетворению.

ООО «ДенСо» не согласилось с решением Центра ВОИС и обратилось в компетентный государственный суд (российский арбитражный суд), предъявив правообладателю товарного знака «*Denso*» иск о признании права пользования доменным именем *denso.com*. Этот иск был заявлен по месту нахождения регистратора (*Registrar*), который регистрировал доменные имена в зоне *.com*, исходя из того, правообладатель товарного знака согласился на оспаривание решения Центра ВОИС по арбитражу и посредничеству, а также компетенцию суда по месту нахождению регистратора.

Арбитражные суды несколько раз пересматривали дело по иску правообладателя доменного имени к правообладателю товарного знака о признании права пользования доменным именем *denso.com*.

В определении ВАС РФ от 04.07.2008[1] указывалось, что фактически российский арбитражный суд рассмотрел требование правообладателя доменного имени о признании его действий по регистрации и использованию домена добросовестными и не нарушающими права на товарный знак, а также о снятии возможных препятствий в использовании доменного имени (например, в виде возможного требования со стороны правообладателя товарного знака о пресечении нарушения в доменном имени его исключительного права на товарный знак). Как отметил ВАС РФ, в итоге рассмотрения российским арбитражным судом такого требования возникли конкурирующие между собой, взаимоисключающие решения в России и Швейцарии по одному и тому же спору между теми же лицами.

В данном определении особо примечательно прямое указание ВАС РФ на то, что правообладатель доменного имени, предъявив требование о признании права на использование спорного доменного имени, **по сути, оспаривал решение аккредитованного арбитражного центра –** Центра ВОИС по арбитражу и посредничеству, который признал его действия по регистрации домена недобросовестными и принял решение передать доменное имя правообладателю товар-

[1] Определение ВАС РФ от 04.07.2008 № 5560/08 по делу А56-46111/2003.

ного знака. Вместе с тем, как отметил ВАС РФ, нормы АПК РФ *не позволили арбитражным судам рассмотреть это требование как требование об оспаривании решения третейского суда*.

Природа разбирательства споров о доменных именах в соответствии с процедурой UDRP

Как указывалось, правообладатель товарного знака может отказаться от использования альтернативного рассмотрения доменного спора и обратиться в государственный суд с соблюдением требований о юрисдикции (подведомственности, подсудности). То есть у правообладателя товарного знака есть выбор: либо обратиться за защитой своих прав в компетентный государственный суд, либо в арбитраж (третейский суд).

Аналогичные правила действуют и применительно к спорам о доменных именах в некоторых *ccTLD* (например, *.au* (Австралия), *.br* (Бразилия), *.es* (Испания), *.fr* (Франция), *.hn* (Гондурас) и т.д.). Хотя во многих случаях национальные регистратуры (администраторы национальных доменов) устанавливают другие правила, в силу которых споры о доменных именах предусматривают не альтернативное рассмотрение спора, а разрешение доменного спора в общем порядке государственными судами.

Например, в соответствии с Правилами регистрации доменных имен в домене .RU, разработанных Координационным центром национального домена сети Интернет, не упоминается о *UDRP* и Правилах *UDRP* в отношении доменных имен в доменах *.ru* и *.рф* – применительно к таким спорам компетентным судом становятся российские государственные суды (суды общей юрисдикции или арбитражные суды[1]).

То обстоятельство, что в *UDRP* и Правилах *UDRP* процедура рассмотрения доменного спора поименована как «административная процедура», а лица, ее осуществляющие, – как «административная комиссия» («административная группа») создало предпосылки для обоснования позиции, согласно которой аккредитованные арбитражные центры, рассматривающие доменные споры, не являются полно-

[1] Ранее доменные споры рассматривались арбитражными судами. Однако после разъяснения, данного ВС РФ в Обзоре судебной практики № 1 (2014) от 24.12.2014 (ответ на вопрос № 4) доменные споры с участием правообладателей доменных имен, не имеющих статуса индивидуального предпринимателя, стали рассматриваться в судах общей юрисдикции.

ценными арбитражами. Более того, высказываются утверждения, что упомянутое разбирательство представляет собой некую иную новую процедуру, неизвестную ранее российскому законодательству и юридической науке. Встречаются мнения, согласно которым разбирательство доменных споров в соответствии с *UDRP* и Правилами *UDRP* – это некая административная процедура, выполняемая непубличным частным органом и т.д.

Не соглашаясь с подобными измышлениями, следует вспомнить данную ранее характеристику прав на доменное имя (отраженную в упоминавшемся ранее деле ЕСПЧ «Паеффген против Германии»). Следовательно, разбирательство доменного спора в аккредитованном арбитражном центре в соответствии с положениями *UDRP* и Правилами *UDRP* представляет собой не что иное, как рассмотрение *частноправового спора об имущественных правах в международном арбитраже*.

Указание в документах *ICANN* на «административность» процедуры и состава лиц, разрешающих доменный спор, проистекает из другой особенности доменных споров, касающейся исполнении вынесенных по этим делам арбитражных решений. Эта особенность состоит в «оптимизации» исполнения решения – оно возможно без обращения за содействием к государственным судебным органам.

Как известно, при отсутствии добровольного исполнения «обычного» арбитражного решения заинтересованной стороне необходимо обратиться в государственный суд за исполнительным листом на принудительное исполнение этого решения. Применительно к доменным спорам имеет место совершенно другая ситуация: при удовлетворении требования истца (правообладателя товарного знака) об отмене регистрации доменного имени, о передаче домена другому лицу и т.д. вынесенное решение приводится в исполнение *аккредитованным регистратором* посредством внесения *соответствующей записи в реестр доменных имен*.

Подобное исполнение решения, нехарактерное для исполнения «обычных» арбитражных решений, имеет отчетливый административно-властный оттенок, что и оказало серьезное влияние на используемую в *UDRP* и Правилах *UDRP* терминологию. Однако это – специфика рассматриваемой процедуры, но не основание исключать ее из числа разновидностей арбитражных разбирательств.

В обоснование изложенной позиции следует специально обратить внимание на следующее.

Понятие «альтернативное рассмотрение споров» (англ. *Alternative Dispute Resolution* (*ADR*)) применяется для обозначения неформальных и более гибких процедур рассмотрения споров, которые используются *вместо государственного правосудия* (судебного разбирательства в государственном суде). Причем к *ADR*, как известно, относят не только третейское разбирательство, но и различные примирительные процедуры: мини-суд[1], доарбитражное производство, независимое экспертное заключение, переговоры, медиаторство и т.п.

Значимым является то, что в отличие от всякой примирительной процедуры, цель которой состоит в примирении спорящих сторон, в содействии им в *достижении взаимовыгодного, компромиссного соглашения*, удовлетворяющего обе эти стороны и прекращающего спор между ними, третейское разбирательство нацелено на *разрешение спора*, при котором арбитраж *выносит обязательное для сторон решение*[2]. Та же **цель разрешения спора** усматривается и за деятельностью комиссий, рассматривающих доменные споры в соответствии с *UDRP* и Правилами *UDRP*.

При этом большинство преимуществ третейского разбирательства перед государственным судом характерны и для разбирательства по доменным спорам: единство процедуры для сторон, находящихся в разных юрисдикциях; профессиональное рассмотрение спора специалистами, обладающими соответствующей квалификацией и знаниями в требуемой области; оперативность рассмотрения спора (недели, а то и дни) и т.д. Но исключением из общего правила следует признать **публичность арбитража по доменным спорам** (в отличие от общего принципа конфиденциальности), что обусловлено целью формирования

[1] Эта процедура в литературе признается промежуточной между арбитражем и примирительной процедурой. В этой процедуре комиссия, состоящая из руководства спорящих компаний и возглавляемая примирителем (он председательствует на мини-суде), получает информацию о сути спора, излагаемую специалистами с обеих сторон. Руководители после заслушивания специалистов относительно сути спора ведут переговоры по этому спору, получив объективную (двустороннюю) оценку причин этого спора и уяснив предложения специалистов о выходе из сложившегося конфликта. Задача примирителя – руководство ходом процедуры, контроль за взаимодействием сторон и помощь комиссии в выявлении предмета спора и сглаживании конфликта. См. об этом подробнее: *Рожкова М.А.* Соглашение о примирительной процедуре // *Рожкова М.А., Елисеев Н.Г., Скворцов О.Ю.* Договорное право: соглашения о подсудности, международной подсудности, примирительной процедуре, арбитражное (третейское) и мировое соглашения / под общ ред. М.А. Рожковой. М.: Статут, 2008. (СПС «КонсультантПлюс»).

[2] См. об этом подробнее, например: *Рожкова М.А.* Мировая сделка: использование в коммерческом обороте. М.: Статут, 2005 (СПС «КонсультантПлюс»).

единообразной практики, обеспечения *предвидимости арбитражных решений* по данным спорам. Эта особенность третейского разбирательства доменных споров в соответствии с *UDRP* и Правилами *UDRP* выделяет данную процедуру из прочих процедур третейского разбирательства, но не лишает ее частноправового характера.

Таким образом, нет никаких серьезных оснований для причисления разбирательства доменных споров в соответствии с *UDRP* и Правилами *UDRP* к числу правовых явлений с неясной правовой природой.

Завершая эту часть настоящей статьи, хотелось бы обратить внимание на не так давно введенную в действие процедуру Единой системы быстрого приостановления действия доменных имен (*URS*). Эта процедура действует с 2013 г. в отношении ***New gTLD*** – главные преимущества этой процедуры быстрота и низкая стоимость, но она имеет и недостатки и, возможно, будет еще дорабатываться. Данную процедуру в литературе нередко характеризуют как полностью заменяющую *UDRP*. Между тем это не так – *URS* является лишь *дополнением к процедуре UDRP*, поскольку на основании *URS* допускается ограничение правообладателя доменного имени (ответчика) в распоряжении правами на спорное доменное имя. Полное прекращение прав правообладателя доменного имени на управляемый домен возможно только по результатам арбитража в соответствии с *UDRP* и Правилами *UDRP*.

Единые критерии, применяемые при рассмотрении доменных споров

Все аккредитованные арбитражные центры при разрешении доменных споров должны руководствоваться едиными критериями, которые закреплены в § 4(a) *UDRP*. Арбитражу для удовлетворения иска необходимо установить, что:

1) доменное имя, зарегистрированное на правообладателя доменного имени (ответчика), идентично или сходно с товарным знаком или знаком обслуживания, правообладателем которых является истец;

2) у правообладателя доменного имени (ответчика) нет прав или законных интересов в отношении зарегистрированного доменного имени;

3) доменное имя было зарегистрировано и используется его правообладателем недобросовестно.

Примечательно то, что в случае указания правообладателем товарного знака (истцом) совокупности названных обстоятельств в иске, предъявленном в аккредитованный арбитражный центр, этот арби-

тражный центр признается компетентным судом даже и *в случае возражений правообладателя домена (ответчика) против компетенции арбитража*.

Применительно к обозначенным критериям, сформулированным в *UDRP*, важным является следующее: в Постановлении Президиума ВАС РФ от 11.11.2008[1] по упоминавшемуся делу о домене *denso.com* была закреплена позиция, *предписывающая российским судам учитывать эти критерии при разрешении доменных споров*. В этом Постановлении Президиум ВАС РФ со ссылкой на п. 1 ст. 5, п. 1 и 2 ст. 10 ГК РФ, § 2 и 3 ст. 10*bis* Парижской конвенции по охране промышленной собственности указал, что при решении вопроса о недобросовестности лица, участвующего в доменном споре, суд для установления содержания честных обычаев при регистрации и использовании (администрировании, делегировании и других действий) доменных имен может использовать положения, сформулированные в § 4(a), 4(b) и 4(c) *UDRP*.

Эта позиция об использовании при рассмотрении доменных споров критериев, поименованных в *UDRP,* нашла подтверждение и в упоминавшейся Справке по вопросам, возникающим при рассмотрении доменных споров, утвержденной Постановлением президиума СИП от 28.03.2014 № СП-21/4[2] (Справка № СП-21/4). В п. 3 Справки № СП-21/4 установлено, 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 для установления содержания честных обычаев при регистрации и использовании доменных имен может использовать положения, сформулированные в *UDRP*.

К сожалению, рекомендации, сформулированные в Постановлении Президиума ВАС РФ и подтвержденные в Справке № СП-21/4, не всегда применяются на практике, в том числе и самим СИП. Одним из самых показательных в этом смысле дел стало дело, в рамках которого был легализован «обратный захват домена».

Из материалов дела усматривалось следующее[3]. ИП Борисенко Г.О. – дизайнер бижутерии – придумала слово *GALOLBO*, которое составлено из начальных букв ее имени, отчества и фамилии (ГАЛина

[1] Постановление ВАС РФ от 11.11.2008 № 5560/08 по делу А56-46111/2003.

[2] См.: http://ipcmagazine.ru/official-cronicle/the-questions-that-arise-when-considering-domain-disputes.

[3] Постановление СИП от 03.08.2016 по делу № А41-81997/2015.

ОЛеговна БОрисенко), и использовала его в качестве творческого псевдонима – *GALA GALOLBO* – при указании авторства на изготовленные ею аксессуары. Работы автора под указанным псевдонимом продавались в центральных столичных магазинах (например, «Цветной», *Lotte Plaza* и др.). В 2008 г. она зарегистрировала доменное имя *galolbo.com*, которое использовалось для сайта по продаже ее работ в сети Интернет.

В 2013 г. *GALA GALOLBO* узнала, что ИП Костина М.А. незаконно использует обозначение «*GALOLBO*», продавая бижутерию, не имеющую отношения к самой *GALA GALOLBO*. В процессе рассмотрения дела по иску ИП Борисенко Г.О. к ИП Костиной М.А. вторая зарегистрировала на себя товарный знак «*GALOLBO*». И затем уже ИП Костина М.А. предъявила к ИП Борисенко Г.О. (*GALA GALOLBO*) иск с требованиями:

1) запретить ИП Борисенко Г.О. использовать обозначение, сходное с товарным знаком «*GALOLBO*» в сети Интернет, в том числе в доменном имени *galolbo.com*;

2) запретить ИП Борисенко Г.О. использовать товарный знак «*GALOLBO*» при изготовлении и реализации продукции 14 и 25 классов МКТУ;

3) изъять из оборота и уничтожить за счет ИП Борисенко Г.О. контрафактные товары, на которых размещен товарный знак «*GALOLBO*»;

4) взыскать с ответчика компенсацию за незаконное использование товарного знака «*GALOLBO*» в размере 500000 руб.

Постановлением СИП было поддержано решение суда первой инстанции, удовлетворившей иск практически полностью (с отменой апелляционного постановления). Таким образом, в итоге с *GALA GALOLBO* (ИП Борисенко Г.О.) взысканы 300 000 руб. компенсации, 13 800 руб. госпошлины, а также 3000 руб. расходов за подачу кассационной жалобы. Причем дизайнеру пришлось не только отказаться от управляемого домена, но и поменять собственный творческий псевдоним – она стала *Gala i-QU*[1].

Не касаясь вопросов регистрации товарного знака, в котором используется чужой псевдоним (этот вопрос заслуживает отдельного рассмотрения[2]), не давая оценки поведению *GALA GALOLBO*, своевремен-

[1] На момент написания настоящей статьи сайт *Gala i-QU* не работал.

[2] См. об этом подробнее: *Рожкова М.А.* Творческий псевдоним как товарный знак // https://zakon.ru/blog/2017/04/25/tvorcheskij_psevdonim_kak_tovarnyj_znak; *Она же*. Ис-

но не предпринявшей необходимых шагов для защиты своего бренда[1], хотелось бы обозначить ошибочность решения СИП, не «увидевшего» очевидного **обратного захвата домена**, который является по сути синонимом **недобросовестного иска**.

Бесспорно, российское законодательство не содержит формальных оснований для противодействия обратному захвату доменов. Однако никто не отменял действия ст. 10 ГК РФ, позволяющей суду отказать в иске в случае злоупотребления истцом правом.

СИП же злоупотребления правом в действиях истца не обнаружил и, более того, выразил недоумение по поводу выводов апелляционной инстанции, отменивший решение суда первой инстанции именно со ссылками на недобросовестность истца.

Не вспомнил судебный состав СИП и о существовании *UDRP*, которая подлежит применению к рассматриваемым правоотношениям[2].

Более того, не вспомнили судьи СИП и о п. 3 Справки № СП-21/4, в которой прямо закреплено, что по спорам о доменных именах, тождественных или сходных до степени смешения с товарными знаками, при рассмотрении вопросов о **недобросовестности лица**, участвующего в деле, может использовать положения, сформулированные в *UDRP* (в том числе в ее § 4(a), 4(b) и 4(c)). Причем в Приложении к самой Справке СИП указывается: «В параграфах 4(c)(i–iii) Политики отмечается, что если администратор доменного имени (ответчик) докажет существование одного или нескольких перечисленных ниже обстоятельств, это может служить основанием для отказа в удовлетворении требований об аннулировании или передаче регистрации доменного имени истцу... например:

(i) до получения извещения об иске администратор доменного имени (ответчик) использовал или готовился использовать доменное имя или имя, сходное до степени смешения с доменным именем, указанным в иске, с целью добросовестного предоставления товаров и услуг;

пользование имени и псевдонима, в том числе в качестве товарного знака // Хозяйство и право. 2017. № 8. С. 25–34.

[1] Юристы, специализирующиеся в области доменных имен, настоятельно рекомендуют коммерсантам после создания оригинального фантазийного доменного имени зарегистрировать его в качестве товарного знака.

[2] См., например: постановления СИП от 03.12.2015 № С01-809/2014 по делу № А56-10757/2014 постановление Президиума ВАС РФ от 11.11.2008 № 5560/08 по делу № А56-46111/2003, а также: *Новоселова Л.А., Михайлов С.В.* О правовом статусе документов, регулирующих регистрацию доменных имен и споров по ним // Закон. 2013. № 11.

(ii) администратор доменного имени был широко известен под спорным доменным именем, даже если при этом он не приобрел исключительного права на товарный знак, тождественный или сходный до степени смешения с доменным именем;

(iii) используя доменное имя, администратор доменного имени занимается законной некоммерческой или иной добросовестной деятельностью, не имея намерения ввести в заблуждение потребителей или нанести вред репутации товарного знака истца».

Является очевидным, что изложенная ситуация подпадает под действие § 4(c)(ii) *UDRP*: администратор доменного имени (ответчик) была широко известна под спорным доменным именем и хотя не приобрела исключительного права на товарный знак, неправомерно лишена прав на спорное доменное имя.

Рассматривая схожее дело *Zero International Holding GmbH & Co. Kommanditgesellschaft v. Beyonet Services and Stephen Urich*[1] в отношении доменного имени *zero.com*, Центр ВОИС по арбитражу и посредничеству учел позицию ответчика, указывающего, что действия истца представляют собой «обратный киберсквоттинг» («обратный захват домена»), поскольку истец пытается захватить доменное имя посредством спланированного и несправедливого лишения ответчика домена, правообладателем которого последний был почти 8 лет. Ответчик ссылался и на то, что при регистрации он не знал о существовании истца, добросовестно зарегистрировал доменное имя в профессиональных целях, причем доменное имя *zero.com* является единственным доменным именем, которое когда-либо он регистрировал.

По результатам рассмотрения данного дела Центр ВОИС по арбитражу и посредничеству признал, что ответчик обладает законным правом на доменное имя *zero.com*. В обоснование решения специально указывалось, что, не зная о существовании истца, ответчик добросовестно осуществил регистрацию доменного имени для достижения своих профессиональных целей на основе принципа «кто раньше», причем зарегистрировал только одно доменное имя[2].

[1] Решение Центра ВОИС по арбитражу и посредничеству от 15.05.2000 по делу № D2000-0161.

[2] Центр ВОИС по арбитражу и посредничеству подчеркнул, что использование доменного имени при отправке сообщений по электронной почте и других операциях передачи файлов является одной из разновидностей законного использования доменного имени.

Завершая настоящую статью, хотелось бы заметить, что в ситуации неправомерного лишения доменного имени российские граждане начинают обращаться к использованию различных средств правовой защиты.

Так, гражданин, являвшийся правообладателем домена *O2.ru*, был необоснованно лишен этого доменного имени по иску ООО «ОДВА». Такое решение выносилось государственными судами нескольких инстанций[1], несмотря на то, что гражданин не осуществлял коммерческой деятельности и на конкурировал с компанией-истцом, а само доменное имя было зарегистрировано за ним не несколько лет раньше, чем возникла компания-истец. Не удивительно, что в подобных обстоятельствах гражданин обратился с соответствующей жалобой в Европейский суд по правам человека, ведь вынося подобное решение, суды неправомерно лишили его части принадлежащего ему имущества.

Пристатейный библиографический список:

1. Интеллектуальная собственность в Интернет: обзор проблем. Женева: ВОИС, 2002.

2. *Курбалийя Й.* Управление Интернетом. М.: Координационный центр национального домена сети Интернет, 2010.

3. *Gün M., Hançer H.* Arbitrating Intellectual Property Disputes / *Ismael Esin, Ali Yesilirmak //* Arbitration in Turkey. Kluwer Law International, 2015.

4. *Афанасьев Д.В.* Комментарий к гл. 30, 31 Арбитражного процессуального кодекса РФ // Арбитражный процессуальный кодекс Российской Федерации с постатейными материалами судебной практики и комментариями / под ред. Т.К. Андреевой. М.: Статут, 2013 (СПС «КонсультантПлюс»).

5. *Mareš A.* The Arbitrator and the Arbitration Procedure – «EU Arbitration»: Solving .eu Domain Names Disputes in Prague / Gerold Zeiler, Irene Welser et al. (eds.) // Austrian Yearbook on International Arbitration. Vol. 2009. Manz'sche Verlags- und Universitätsbuchhandlung, 2009.

6. *Рожкова М.А.* Соглашение о примирительной процедуре // *Рожкова М.А., Елисеев Н.Г., Скворцов О.Ю.* Договорное право: соглашения о подсудности, международной подсудности, примирительной проце-

[1] Постановление ФАС Московского округа от 24.07.2013 по делу № А41-48441/12.

дуре, арбитражное (третейское) и мировое соглашения / под общ ред. М.А. Рожковой. М.: Статут, 2008 (СПС «КонсультантПлюс»).

7. *Рожкова М.А.* Мировая сделка: использование в коммерческом обороте. М.: Статут, 2005 (СПС «КонсультантПлюс»).

8. *Рожкова М.А.* Использование имени и псевдонима, в том числе в качестве товарного знака // Хозяйство и право. 2017. № 8.

9. *Новоселова Л.А., Михайлов С.В.* О правовом статусе документов, регулирующих регистрацию доменных имен и споров по ним // Закон. 2013. № 11.

А.Г. Дейнеко

ПРАВО КИБЕРПРОСТРАНСТВА: PRO ET CONTRA

Аннотация. *Данная статья преследует цель проанализировать возможные концептуальные подходы к новой отрасли (подотрасли) права – права киберпространства. Автор анализирует специфику правоотношений, складывающихся в информационно-телекоммуникационных сетях, а также возможности их правового регулирования.*

Ключевые слова: *теория права, Интернет, киберпространство, авторское право, информационное право, интеллектуальная собственность.*

XXI век можно смело назвать веком цифровой революции. Эта революция уже произошла, но ее итоги предстоит осмысливать еще длительное время. Новые технологии передачи информации не только кардинально ускорили процессы всемирного обмена знаниями, но и серьезнейшим образом изменили структуру общественных отношений. Усложнение общественных отношений, в свою очередь, поставило новые вызовы перед правом.

Еще в 2000 г. М.А. Федотов предложил рассматривать информационно-телекоммуникационные сети не просто как новый способ коммуникации, а как новую сферу обитания человечества и новую сферу применения права. Ученый отметил, что в процессе своего развития информационное право со временем должно сформировать внутри себя такие подотрасли, как информационное гражданское право, информационное уголовное право и т.д.[1]

Эта идея была поддержана многими отечественными правоведами, однако дискуссия о целесообразности расширения предмета правового регулирования информационного права и перспективах его развития не завершена и по сей день. В развитие этой дискуссии учеными поставлены вопросы об обоснованности и целесообразности выделения «права киберпространства» (*Cyberspace Law*) как самостоятельной отрасли (подотрасли) права и его соотношения с информационным правом.

[1] Актуальные проблемы информационного права: материалы науч.-теорет. конференции. Москва, МГЮА им. О.Е. Кутафина, 27 января 2000 г. // Труды по интеллектуальной собственности. Т. 2. М., 2000.

Следует заметить, что вопрос о правовом регулировании киберпространства актуален не только для России, но и для всех развитых стран мира.

В 1998 г. профессор Гарвардского университета Лоуренс Лессиг впервые предложил термин «*laws of Cyberspace*» – «право киберпространства». Уникальность киберпространства, по Лессигу, состоит не просто в невиданном ранее уровне интерактивности и скорости обмена информацией, но в том, что оно порождает принципиально новые общественные правоотношения, в том числе с точки зрения пределов действия норм права в пространстве, во времени и по кругу лиц. «Киберпространство неизбежно развивается, но при этом не поддается (правовому. – *А.Д.*) регулированию. Ни одно общество не может жить без киберпространства, но ни одно общество не может контролировать поведение в нем. Киберпространство – это место, где индивиды по своей сути свободны от контроля со стороны государственной власти»[1]. С этой характеристикой трудно не согласиться.

Термин «право киберпространства» пока не получил должного признания в российской правовой доктрине, несмотря на то, что впервые он был введен в отечественный научный оборот еще в 1998 г.[2]

Наиболее близким по значению к *Cyberspace Law* является термин «информационное право» при условии его трактовки в расширительном смысле. Основоположник науки российского информационного права И.Л. Бачило справедливо отмечает, что даже спустя много лет после признания информационного права в качестве дисциплины для преподавания в вузах и введения отдельной специальности для защиты диссертаций (12.00.14) сомнения некоторых юристов в легитимности выделения этой отрасли не исчезли[3].

Определяющим для информационного права, по мнению И.Л. Бачило, является особый предмет правового регулирования – информационные отношения, а также информация как фундамент этих отношений. Природа этих отношений столь специфична, что они не могут быть урегулированы при помощи традиционных методов правового регулирования. Это в полной мере относится и к киберпространству.

---

[1] *Lessig L.* The laws of Cyberspace. Draft: April 3, 1998. P. 3 (URL: http://cyber.harvard.edu/works/lessig/laws_cyberspace.pdf).

[2] *Федотов М.А.* Киберпространство как сфера обитания права // Бюллетень ЮНЕСКО по авторскому праву. 1998. № 2 (т. XXXII).

[3] *Бачило И.Л.* Информационное право: учебник. М.: Юрайт, 2011. С. 22.

Несколько упростив классическую теорию права, можно выделить два подхода к выделению самостоятельных отраслей в праве: на основе специфического предмета и метода правового регулирования или же на основе специфического круга правовых институтов, объединенных общими функциями и принципами.

Второй подход вряд ли может быть применим к праву киберпространства, поскольку специфические правовые институты в нем еще не сформировались, а основные принципы взаимодействия пользователей (например, *нетикет*[1]) имеют скорее морально-этическую, а не правовую природу. Существование таких неписаных правил, поддерживаемых большей частью интернет-сообщества, создает необходимые предпосылки для развития в киберпространстве механизмов саморегулирования, которые, в свою очередь, в ближайшем будущем могут свести к минимуму необходимость использования мер государственного принуждения.

Еще в догосударственный период человеческой истории первые социальные нормы поведения предполагали в качестве одного из самых строгих наказаний изгнание человека из общины (семьи, племени), объявление отверженным. Ценность человеческой жизни в то время была крайне невысока, поэтому даже смертная казнь не внушала людям такого ужаса, как перспектива быть изгнанным.

Возможность изгнать современного *Homo interneticus* из отдельно взятого участка киберпространства («забанить» на форуме, аннулировать учетную запись и др.) дает основания вновь говорить об актуальности неправовых способов регулирования общественных отношений. Право, как известно, есть *est ars boni et aequi*[2], и в киберпространстве «доброта» права, т.е. минимальное использование императивных правовых конструкций, а также «равенство» всех пользователей в отношениях с государством и друг с другом крайне важны для создания эффективной системы правового регулирования.

Отделить предмет права киберпространства от предмета информационного права довольно сложно, но именно этот критерий вы-

[1] Нетикет (сетевой этикет) – правила поведения в киберпространстве, сформировавшиеся естественным путем и зачастую носящие неписаный характер. Содержание нетикета неодинаково в различных интернет-сообществах, но к числу общих правил можно отнести обращение к незнакомым пользователям на «вы», соблюдение языковых правил, умеренное использование ненормативной лексики, цитат, «смайликов» и т.д. (подробнее см.: URL: https://ru.wikipedia.org/wiki/Сетевой_этикет).

[2] Искусство добра и справедливости (лат. *Celsius*).

деления отрасли права является в нашем случае определяющим. Вопрос о методе правового регулирования, как известно, является дискуссионным и при наиболее узкой трактовке позволяет выделить лишь две отрасли права – частного и публичного. Но даже при расширительном толковании выделить собственный метод правового регулирования для права киберпространства пока довольно трудно, поскольку на практике для регулирования рассматриваемых отношений применяется в основном национальное императивное регулирование.

Сложности с определением предмета информационного права и права киберпространства проистекают в первую очередь из некоторого сходства общественных отношений, составляющих предмет правового регулирования этих отраслей. Разграничить их можно, основываясь на том, что информация является объектом права, а киберпространство представляет собой саму (интерактивную) среду, где непрерывно происходит создание и обмен информацией.

Но не все отношения по созданию и обмену информацией имеют место в киберпространстве – они могут иметь место и вне его. Аналогичная ситуация наблюдается и применительно к киберпространству: не все отношения, возникающие в киберпространстве, обязательно связаны с созданием или обменом информацией – многие из них имеют совершенно другое предназначение.

Таким образом, отношения по поводу информации и отношения в киберпространстве пересекаются, но не совпадают полностью.

Исследование предмета правового регулирования неизбежно приводит нас к вопросу о допустимости рассмотрения информации в качестве объекта прав.

Как известно, до вступления в силу четвертой части ГК РФ информация была названа в ст. 129 ГК РФ в качестве объекта гражданских прав[1]. Вводным законом к части четвертой ГК РФ с 01.01.2008 информация была исключена из числа объектов гражданских прав, что породило известные научные дискуссии.

Исключение информации из числа объектов гражданских прав способствует отграничению информационного права от гражданского. В то же время это противоречит фактически существующей практике, поскольку участники оборота могут договориться между собой

[1] *Семилетов С.И.* Информация как особый объект права // Проблемы информатизации. 1999. № 3. С. 56.

о возмездной передаче любой (даже общеизвестной) информации посредством заключения гражданско-правовой сделки[1].

Одной из возможных причин, побудивших законодателя исключить информацию из числа объектов гражданских прав, мог быть тезис о том, что информация якобы не существует сама по себе, а находит свое выражение в материальных или нематериальных объектах, например, в результатах интеллектуальной или иной творческой деятельности. По нашему мнению, напротив, следует говорить о несводимости понятия «информация» к иным объектам гражданских прав, т.е. о ее самостоятельности в качестве объекта прав.

Кроме того, законодатель, приняв решение об исключении информации из числа объектов гражданских прав, в дальнейшем, кажется, сам запутался в терминологии.

Так, Закон об информации определяет информацию как «сведения (сообщения, данные) независимо от формы их представления» (п. 1 ст. 2). При этом оговаривается, что положения этого Закона не распространяются на правоотношения, возникающие при правовой охране результатов интеллектуальной деятельности (п. 2 ст. 1). Но в то же время Закон об информации неоднократно упоминает такую категорию, как «информация, содержащая объекты авторских и (или) смежных прав» (ст. 15.2, 15.6, 15.7). Следовательно, выделяется два вида сведений – сведения, являющиеся информацией и не относящиеся к объектам гражданских прав, и сведения, не являющиеся информацией и относящиеся к объектам гражданских прав.

Обратившись к положениям части четвертой ГК РФ, можно увидеть, что при определении понятия секрета производства (ноу-хау) в ст. 1465 ГК РФ использован термин «сведения», который невозможно противопоставить термину «информация». Это позволяет сделать вывод о том, что информация (сведения) признается объектом гражданских (исключительных) прав по крайней мере применительно к ноу-хау. Кодекс требует от правообладателя введения режима коммерческой тайны в отношении секрета производства, причем ст. 1 ФЗ от 29.07.2004 № 98-ФЗ «О коммерческой тайне» (далее – Закон о коммерческой тайне) устанавливает, что режим коммерческой тайны может быть установлен именно в отношении информации (а не сведений). Но в п. 2 ст. 3 Закона о коммерческой тайне вновь поставлен

[1] Это не отрицает возможности наступления уголовной ответственности за разглашение информации, составляющей государственную или иную охраняемую законом тайну.

знак равенства между понятиями «информация» и «сведения»: информация, составляющая коммерческую тайну, определена как «сведения любого характера».

Неопределенность в рассматриваемый вопрос добавляет и то, что административное и уголовное законодательство устанавливает ответственность то за разглашение информации, то за разглашение сведений, не позволяя определиться в части соотношения данных понятий. Так, ст. 7.31.1, 13.14 КоАП РФ устанавливают ответственность за разглашение информации, а ст. 13.15, 17.13 КоАП РФ и ст. 183, 283, 311, 320 УК РФ – за разглашение сведений.

Таким образом, понятие «информация» определяется через понятие «сведения» в нескольких федеральных законах, но не в части четвертой ГК РФ, где понятие информации вообще отсутствует.

В связи со сказанным нельзя не вспомнить правовую позицию КС РФ, согласно которой любая правовая норма должна отвечать общеправовому критерию формальной определенности, ясности и недвусмысленности, а ее несоответствие данным критериям само по себе является угрозой нарушения основных прав и свобод граждан[1]. В контексте широкого использования термина «информация» в текстах нормативных правовых актов различных уровней представляется, что он мог бы быть конкретизирован как минимум путем ответа на вопросы: *о чем могут быть сведения;* и *в какой именно форме они могут быть представлены*?

Понятие и предмет информационного права не охватывают всей палитры отношений, происходящих в информационно-телекоммуникационных сетях, в сети Интернет ежесекундно возникают отношения, подпадающие под предмет регулирования гражданского, административного, уголовного, финансового и других отраслей права. Обширный массив отношений складывается в иных информационно-телекоммуникационных сетях, таких как *FTP*-сети, пиринговые и *TOR*-сети, которые в совокупности с сетью Интернет и составляют киберпространство.

Необходимость ограничения предмета информационного права рамками общественных отношений, связанных с оборотом информации, вызвана спецификой информации как особого объекта прав, а также стремлением выделить во всем массиве отношений, происходящих в киберпространстве, относительно точно идентифицируемую

[1] Постановление КС РФ от 21.01.2010 № 1-П.

область. Стоит еще раз подчеркнуть, что такие отношения могут происходить и вне киберпространства.

В свою очередь, действие правовых норм в киберпространстве требует учета ряда важных моментов.

Как известно, все правовые нормы имеют ограниченную сферу действия. Эти ограничения диктуются их временными рамками, охватом определенного географического пространства и тем кругом лиц, для кого они обязательны к исполнению (на кого распространяются). Применительно к действию правовых норм в киберпространстве затруднительно говорить, например, о территории их действия, поскольку речь идет не об охвате географического пространства.

Например, неверным было бы определить доменные зоны .ru и .рф в качестве территории Российской Федерации в киберпространстве – национальная доменная зона вовсе не означает автоматического распространения российской юрисдикции на все правоотношения, происходящие в этой доменной зоне[1]. Сайт в домене .ru и .рф могут зарегистрировать иностранные юридические и физические лица, контент сайта вовсе не обязательно должен быть на русском языке, продавцами и покупателями товаров на сайте могут быть иностранцы и т.д. Развивая эту мысль, следует признать, даже если согласиться с тем, что все отношения, происходящие в национальных доменных зонах (.ru, .de, .fr и других), подчиняются национальному законодательству страны этого домена, невозможно будет определить право, подлежащее применению к отношениям в зонах доменов общего назначения (.com, .org, .net и др.).

С учетом сказанного является очевидным трансграничный характер киберпространства, это позволяет говорить о том, что киберпространство выходит далеко за рамки правового регулирования отечественного информационного права и дает основания для выделения права киберпространства в качестве самостоятельной отрасли (подотрасли) права.

В подтверждение сказанного можно вспомнить проблематику правовых режимов открытого моря или космического пространства[2]. Споры вокруг выделения в качестве самостоятельных отраслей меж-

[1] Этот вывод справедлив и в отношении доменной зоны .su, хотя на практике все вместе они именуются не иначе как «*русскоязычный сегмент Интернета*» (Рунет).

[2] См., например: Мировой океан и международное право. Открытое море. Международные проливы. Архипелажные воды / отв. ред. А.П. Мовчан. М.: Наука, 1988; *Ковалев Ф.Н., Черпов И.И.* На пути к космическому праву. М.: Изд-во ИМО, 1962.

дународного морского права и международного космического права все еще продолжаются, однако развитие общественных отношений подтверждает обоснованность такого подхода. В связи с этим нельзя не вспомнить слова И.А. Ильина, который еще в 1915 г. обратил внимание на следующее: «История свидетельствует о том, что развитие и усовершенствование положительного права совершается медленно, но неуклонно; медленно потому, что всегда есть группы людей, которым старое право полезнее и выгоднее и которые обыкновенно соглашаются на его отмену лишь после долгого и упорного сопротивления; неуклонно потому, что всегда появляются новые группы людей, неудовлетворенные старым правом, считающие его вредным или несправедливым»[1]. Этот вывод, сделанный более века назад, не потерял своей актуальности и сегодня.

Применительно к действию правовых норм в киберпространстве особенности усматриваются и в части распространения правовых норм по кругу лиц.

В качестве субъектов права в киберпространстве могут быть упомянуты, в частности, провайдеры (магистральные, сервисные и др.), администраторы доменов, владельцы сайтов, интернет-пользователи – отношения между ними возникают посредством технических устройств, подключенных к сети. Между тем, учитывая, что все чаще подобные связи возникают не только между людьми, но и между людьми и техническими устройствами, а то и только между техническими устройствами, исключением участия человека (см. интернет-вещей), все чаще звучат утверждения о допустимости признания правоотношений с участием технических устройств. Однако субъектами прав, на которых распространяется действие правовых норм, на сегодняшний день признается только физическое или юридическое лицо, но не техническое устройство. Хотя общие тенденции и готовящееся законодательство о роботах[2], не исключено, изменят это правило.

Изложенное, на наш взгляд, создает предпосылки для формирования самостоятельной отрасли (подотрасли) права, регулирующей

[1] *Ильин И.А.* Теория права и государства / под ред. В.А. Томсинова. М.: Зерцало, 2008 (серия «Русское юридическое наследие»). С. 268.

[2] Так, 16 февраля 2017 г. Европарламент проголосовал за резолюцию Еврокомиссии о законодательном регулировании статуса роботов и их отношений с людьми. В России также разрабатываются законопроекты, «регулирующие взаимоотношения робота и человека».

отношения в киберпространстве. Причем следует констатировать три возможных подхода к правовой институциализации и теоретическому осмыслению отношений, происходящих в киберпространстве.

При первом подходе отношения в киберпространстве будут рассматриваться как отношения, связанные исключительно с оборотом информации, функционированием информационных систем и обеспечением информационной безопасности, т.е. как отношения, регулируемые сегодня информационным правом. В то же время иные общественные отношения, даже и возникающие в киберпространстве, будут отданы «на откуп» традиционным отраслям права – гражданскому, уголовному и т.п. Используемые методы правового регулирования вряд ли претерпят при этом существенные изменения, но законодательные предписания, на наш взгляд, будут малоэффективными.

При втором подходе все отношения, происходящие в информационно-телекоммуникационных сетях, составят предмет новой, комплексной отрасли (подотрасли) права – права киберпространства. Метод правового регулирования, необходимый для этой отрасли, входящие в ее состав институты и категории и т.д. только предстоит определить. Однако предпочтительность использования такого подхода обусловлена рассмотренными выше особенностями общественных отношений, происходящих в киберпространстве.

Третий подход предполагает отказ от выделения новой отрасли, связанной с отношениями в киберпространстве. Но изложенное выше позволяет говорить о бесперспективности такого пути.

Пристатейный библиографический список:

1. Актуальные проблемы информационного права: материалы науч.-теорет. конференции. Москва, МГЮА им. О.Е. Кутафина, 27 января 2000 г. // Труды по интеллектуальной собственности. Т. 2. М., 2000.

2. *Бачило И.Л.* Информационное право: учебник. 2-е изд., перераб. и доп. М.: Юрайт, 2011.

3. *Дейнеко А.Г.* Интернет-радио: проблемы правовой квалификации // Вопросы правоведения. 2010. № 4.

4. *Дейнеко А.Г.* Проблемы правовой квалификации Интернет-телевещания в Российской Федерации // EuropeanSocialScienceJournal. 2011. № 11 (14).

5. *Ильин И.А.* Теория права и государства. 2-е изд., доп. / под ред. и с биограф. очерком В.А. Томсинова. М.: Зерцало, 2008 (серия «Русское юридическое наследие»).

6. *Ковалев Ф.Н., Черпов И.И.* На пути к космическому праву. М.: Изд-во ИМО, 1962.

7. Мировой океан и международное право. Открытое море. Международные проливы. Архипелажные воды / отв. ред. А.П. Мовчан. М.: Наука, 1988.

8. *Наумов В.Б.* Право и Интернет: очерки теории и практики. М.: КДУ, 2002.

9. *Рассолов И.М.* Право и Интернет. Теоретические проблемы. М.: Норма, 2009.

10. *Семилетов С.И.* Информация как особый объект права // Проблемы информатизации. 1999. № 3.

11. *Федотов М.А.* Киберпространство как сфера обитания права // Бюллетень ЮНЕСКО по авторскому праву. 1998. № 2 (т. XXXII).

12. *Федотов М.А.* Обретет ли Конституция свое Интернет-измерение? // Теория и практика российского конституционализма: сб. докладов науч.-практ. конференции, посвященной 75-летию со дня рождения академика О.Е. Кутафина, 26 июня 2012 г. / отв. ред. В.И. Фадеев. М.: Изд. центр Ун-та им. О.Е. Кутафина (МГЮА), 2013.

13. *Lessig L.* The laws of Cyberspace. Draft: April 3, 1998. P. 3 (URL: http://cyber.harvard.edu/works/lessig/laws_cyberspace.pdf).

В.А. Белов

DIGITAL PRIVATE LAW & RIGHTS: РАЗМЫШЛЕНИЯ О ПРЕОБРАЗОВАНИЯХ, УЖЕ ПРОИЗВЕДЕННЫХ В ЧАСТНОМ ПРАВЕ РАЗВИТИЕМ ГЛОБАЛЬНОЙ КОМПЬЮТЕРНОЙ СЕТИ ИТЕРНЕТ, И О РЕФОРМАХ, ЕГО СКОРО И НЕМИНУЕМО ПО ТОЙ ЖЕ ПРИЧИНЕ ОЖИДАЮЩИХ

Аннотация. *Статья посвящена обзору ключевых перемен в институтах частного права, вызванных появлением и развитием глобальной компьютерной сети Интернет, а также тех ближайших в нем изменений, которые (по той же причине) должны будут произойти. В частности, в статье обращается внимание на де-факто уже наступившую смерть авторского и смежных прав в их традиционном виде, колоссальные сложности, связанные с осуществлением и защитой патентных прав и прав на средства индивидуализации, фундаментальные изменения в договорном праве и праве собственности, в понятиях о субъектах прав, объектах прав и юридических фактах. По мнению автора, в недалеком будущем нас ожидает преобразование также понятий об объективном праве и субъективных правах – их замена соответствующими цифровыми аналогами.*

Ключевые слова: *интернет-право, научно-технический прогресс и право, исключительные права, права на средства индивидуализации, обязательственное право, вещное право.*

1. **Обзорно-библиографическое введение.** Развитие техники – фактор, который на протяжении всей человеческой истории оказывал принципиальное (качественное) воздействие на развитие права. Книгопечатание и промышленная революция, железные дороги, автомобили и самолеты, телеграф и телефон, лито- и фотография, радио, кино и телевидение, средства аудио- и видеозаписи, бытовые копировальные аппараты и магнитофоны, кабельные (проводные) и эфирные (беспроводные) средства передачи электромагнитных сигналов, снабжение энергией и некоторыми другими, пригодными для этого товарами через присоединенную сеть, автоматические устройства и роботы, достижения в области физики атомного ядра,

электронно-вычислительные машины, мобильная связь – все это лишь немногие изобретения и открытия, которые произвели переворот в *правовой оценке* (правовом регулировании) социальных отношений. Сообразно успехам научно-технического прогресса одни институты как частного, так и публичного характера исчезали, а другие появлялись; менялось содержание правовых институтов, их место в системе права, взаимное влияние, координация и соподчинение. Не было *пока*, впрочем, ни одного случая, чтобы развитие техники поставило под вопрос самое существование права в традиционном понимании этого термина.

Изменения, вносимые техническим прогрессом в юридическую жизнь, встречали самое живое внимание юристов. Широко известны русскоязычные монографии конца XIX – начала XX в. по железнодорожному, авторскому и патентному праву, написанные такими юристами, как С.А. Беляцкин, К.П. Змирлов, Я.А. Канторович, В.Д. Катков, А.А. Пиленко, И.М. Рабинович, И.Г. Табашников, Г.Ф. Шершеневич. Менее известны, но не менее интересны и значимы многочисленные публикации, посвященные юридическим аспектам заключения «договоров между отсутствующими», правам и обязанностям, рождающимся от воздушных сообщений и автомобильных перевозок, при сетевом снабжении электрической энергией и газом и т.д. Так, например, в статье В.М. Цвингмана анализируются вопросы (а) юридических последствий обмена телеграфными сообщениями, (б) распространения правомочий авторов и исполнителей произведений на их звуковую запись; (в) заключения и исполнения договоров с использованием автоматических устройств и (г) юридической квалификации самовольного подключения к электрической сети[1]. Наименования других подобных работ говорят сами за себя[2].

[1] См.: *Цвингман В.М.* О влиянии техники на развитие договорного права // Журнал Министерства юстиции. 1902. № 8. С. 149–173.

[2] См., например: *Миллер П.* Фотографическая собственность // Журнал гражданского и уголовного права. 1883. № 9. С. 63–96; *Он же.* Музыкальная собственность // Там же. 1886. Кн. 1. С. 37–76; *Катков В.* Заключение договоров при посредстве электричества // Журнал Юрид. Об-ва, сост. при Имп. СПб. Ун.-те, 1896. Кн. 7. С. 77–88; *Розин Н.Н.* О похищении электрической энергии // Вестник права. 1899. № 10. С. 89–104; *Гольденберг В.* Воздухоплавание и право. СПб., 1909; *Завадский А.В.* О праве на собственное изображение. Казань, 1909; *Ельяшевич Ф.* Договор по телефону (рецензия) // Журнал Мин-ва юстиции [ЖМЮ]. 1910. № 7. С. 295–300; *Он же.* Право воздухоплавания с англосаксонской точки зрения // Там же. 1910. № 8. С. 308–311;

Любили писать о влиянии научно-технического прогресса на развитие права и советские юристы[1]. Предметы таких исследований видоизменялись сообразно движению человеческой мысли: от электричества и телефонов (в эпоху становления Советской власти)[2] –

Бродский Л. К вопросу о праве на воздух в связи с воздухоплаванием // Вестник права и нотариата [ВПН]. 1911. № 20. С. 615–620; *Астров П.И.* Городской трамвай и давность // Там же. 1912. № 24. С. 723–726; *Ельяшевич Ф.* Влияние изобретений на право-развитие (рецензия) // ЖМЮ. 1912. № 2. С. 293–296; *Шиф Л.И.* Воздухоплавание и право. СПб., 1912; *Элиасберг Е.* Является ли авиатор-разведчик законным неприятелем или шпионом // ВПН. 1913. № 10. С. 296–298; *Гаврилов С.* Похищение электрической энергии // Юридический вестник [ЮВ]. 1914. Кн. VII–VIII. С. 286–296; *Мезенкампф Н.М.* Новейшие разъяснения понятия «эксплуатация» в ст. 683 т. X ч. 1 // Вестник гражданского права. 1914. № 2. С. 72–98; *Бутовский А.Н.* Домашние завещания и пишущие машины // Там же. 1915. № 3. С. 152–163; *Завадский А.В.* Действительность духовных завещаний, писаных на пишущей машине // Сб. ст. по гражданскому и торговому праву памяти Г.Ф. Шершеневича. М., 1915. С. 257–274; *Гуссаковский П.Н.* Договоры между отсутствующими // ЖМЮ. 1916. № 9. С. 1–29; № 10. С. 1–40; *Ключников Ю.* Воздухоплавание и международное право // ЮВ. 1916. Кн. XIV. С. 144–159.

[1] Общие вопросы см.: *Алексеев Н.С.* Научно-технический прогресс и право. Л., 1976; *Ведяхин В.М.* Правовое регулирование научно-технического прогресса: теоретико-правовой аспект. Куйбышев, 1990; *Венгеров А.Б.* Научно-технический прогресс и законодательство развитого социализма // Советское государство и право [СГП]. 1981. № 6. С. 24–33; *Он* же. Научно-технический прогресс и применение права // Правоведение. 1983. № 3. С. 21–28; Влияние научно-технического прогресса на юридическую жизнь (кол. авт.) / отв. ред. Ю.М. Батурин. М., 1988; *Дозорцев В.А.* Советское право и научно-технический прогресс. М., 1973; *Он же.* Законодательство и научно-технический прогресс. М., 1978; *Иойрыш А.И.* Научно-технический прогресс и новые проблемы права. М., 1981; *Казьмин И.Ф.* Общие проблемы права в условиях научно-технического прогресса. М., 1986; Правовые вопросы научно-технического прогресса в СССР (кол. авт.) / под общ. ред. М.М. Богуславского. М., 1967; *Райгородский Н.А.* Роль права в ускорении технического прогресса // Правоведение. 1961. № 2. С. 34–43; *Явич Л.С.* Научно-техническая революция, право и юридическая наука // Правоведение. 1973. № 5. С. 34–42. См. также работы, посвященные правовой стороне отношений в области самого НТП – публикации Ч.Н. Азимова, С.Д. Волошко, В.И. Жукова, И.А. Зенина, И.Э. Мамиофы, В.А. Рассудовского, М.П. Ринга, Г.П. Савичева, Н.Н. Яковлева и др.

[2] См., например: *Люблинский П.И.* К вопросу об электрификации железных дорог. Пг., 1920; *Тюфяев А.В.* Правовая природа авто-мото-имущества по действующему законодательству (К вопросу о раскрепощении авто-мото- транспорта) // Советское право [СП]. 1923. № 2. С. 65–74; *Канторович Я.* Сделки, совершаемые при посредстве телефона // Еженедельник Советской юстиции. 1924. № 11. С. 247–248; *Усаковский А.Н.* Радио и авторское право в иностранном законодательстве и судебной практике // СП. 1927. № 1. С. 121–126; *Губарев В.П.* Страхование самолетов // Вопросы воздушного права: сб. тр. Вып. 2. М.-Л., 1930; *Зарзар В.А.* Новейшее в современном аэронаутизме // Там же. С. 7–28; *Перетерский И.С.* Самолет как объект гражданско-

до атомного оружия, ядерной энергетики и освоения космоса[1]. Особенно привлекательным для правоведов эпохи «развитого социализма» оказался круг вопросов о тех, с одной стороны, юридических тонкостях и сложностях, вызываемых внедрением так называемых *АСУ – автоматизированных систем управления*[2], а с другой – о тех

го права // Там же. С. 150–154; *Фейтельберг М.Н.* Из литературы по автомобильному страховому праву // Закон и Суд. Рига. 1934. № 6. Стлб. 1607–1610; *Кацнельсон В.М.* Судебная защита квартиронанимателя от шума соседского радио // Там же. 1938. № 4. Стлб. 3969–3974; № 5. Стлб. 3989–3992.

[1] См., например: Космос и международное право: сб. ст. / отв. ред. Е.А. Коровин. М., 1962; *Осницкая Г. А.* Освоение космоса и международное право. М., 1962; *Рыбаков Ю.М.* Правовая регламентация ответственности за ущерб в связи с деятельностью государств в космосе // Правоведение. 1967. № 1. С. 115–121; *Иойрыш А.И.* Атом и право. М., 1969; *Василевская Э.Г.* Правовые проблемы освоения Луны и планет. М., 1974; *Верещетин В.С.* Космос. Сотрудничество. Право. М., 1974; *Малинин С.А. Мусин В.А.* Правовые проблемы морской атомной деятельности. Л., 1974; *Брылов А.Н.* Международно-правовые аспекты использования сверхзвуковых транспортных самолетов (СТС) в международных воздушных сообщениях: дис. ... канд. юрид. наук. М., 1977; *Бордунов В.Д., Марков В.Н.* Космос. Земля. Право. М., 1978; *Василевская Э.Г.* Правовой статус природных ресурсов Луны и планет: проблемы и суждения. М., 1978; *Чопорняк А.Б.* Ядерный ущерб: гражданско-правовая ответственность и страхование: дис. ... канд. юрид. наук. М., 1979; Космос и право: сб. ст. / отв. ред. Ю.М. Колосов. М., 1980; *Иойрыш А.И.* Научно-технический прогресс и новые проблемы права. М., 1981; Ядерная энергия и мировой океан: международно-правовое регулирование: сб. ст. / под ред. А.И. Иойрыша, М.И. Лазарева, Л.В. Сперанской. М., 1981; Правовые проблемы использования атомной энергии: сб. ст. / под ред. А.И. Иойрыша, В.И. Менжинского, А.М. Петросьянца. М., 1985; Советское атомное право (кол. авт.) / отв. ред. П.Н. Бургасов. М., 1986; *Афанасьева Л.А.* Ядерное страхование в капиталистических странах: Сравнительно-правовое исследование. М., 1989; *Иойрыш А.И., Чопорняк А.Б.* Атомное законодательство капиталистических стран: сравнительно-правовой анализ. М., 1990. По вопросу ядерного вооружения и разоружения советская литература международного *публичного* права столь колоссальна, что не поддается никакому обозрению.

[2] См., например: Автоматизированные системы управления предприятиями: сб. ст. Кишинев, 1971; *Венгеров А.Б.* Право и информация в условиях автоматизации управления: теоретические вопросы. М., 1978; *Венгеров А. Б., Пертцик В.А., Самощенко И.С.* Правовые основы автоматизации управления народным хозяйством СССР. М., 1979; *Вишняков В.Г.* Право и автоматизированные системы управления. М., 1976; *Волошко С.Д.* Хозяйственные отношения и автоматизация управления: уч. пообиес. Харьков, 1980; *Гальперин Л.Б.* Автоматизированные системы управления и их правовое обеспечение. Томск, 1978; *Евдокимов В.В., Нильва А.И., Морев В.Н.* Автоматизированные системы управления промышленными предприятиями. Л., 1975; *Калюжный Р.А.* Правовые вопросы технического обеспечения АСУ. Киев, 1980; Комментарий к основным нормативным актам об автоматизированных системах управления / отв. ред. А.Б. Венгеров, Н.Г. Калинин. М., 1982; *Ольшанецкий А.Г.* Правовое обеспе-

высотах, которые неизбежно удастся достичь с их более или менее широким внедрением во все мыслимые области народного хозяйства, не исключая, кстати, и самого правоведения. Не будет преувеличением сказать, что юристы СССР просто-таки *обожали* писать о тех горизонтах, которы должны открыться им самим и представляемой ими науке с использованием *электронно-вычислительной техники* (ЭВТ или, как стали сокращать позже, ЭВМ)[1]. Правда, доступа к такой технике они в большинстве своем не имели – пользовались услугами библиотек и кодификационных бюро, но это уже совсем другой вопрос.

Одним из многочисленных непосредственных следствий развития систем машинной (автоматизированной), а затем электронной обработки информации и электронной связи и стал тот феномен, юридическое значение которого мы и планируем рассмотреть в настоящей статье, – ***феномен глобальной компьютерной сети Интернет***.

чение автоматизированных систем управления. М., 1979; Правовые проблемы АСУ: сб. ст. М., 1973; *Самохин Ю.М., Хайдас Г.И.* Создание автоматизированной системы плановых расчетов // Советское государство и право. 1973. № 8. С. 65–69; *Тарапон О.Ф.* Правовые вопросы автоматизации управления производственным объединением. Киев, 1979; *Толстошеев В.В.* Организационные и правовые проблемы АСУ. М., 1976; *Фаткудинов З.М.* Право и автоматизированная система плановых расчетов. Казань, 1977.

[1] См., например: Актуальные проблемы теории и практики применения математических методов и ЭВМ в деятельности органов юстиции: тез. докладов. М., 1975; *Бродский И.Л.* Вычислительные центры: организация и деятельность // Правоведение. 1975. № 4. С. 110–113; *Буркин Ю.В., Пионтковский А.А.* К вопросу о правовых нормах и возможности их формализации // Правовые проблемы АСУ. М., 1973. С. 86–88; Информатика и право: сб. науч. тр. / отв. ред. Ю.С. Вишняков, Б.Н, Наумов, Б.И. Остроухов, Н.С. Соломенко. Л., 1988; *Кулль И.Г., Нигол Р.П., Сильдмяэ И.Я., Ээремаа К.А.* Информационно-поисковая система для законодательного материала // Правоведение. 1970. № 4. С. 102–105; *Москвин С.С.* Информационно-поисковая система нормативных материалов // СГП. 1972. № 2. С. 121–126; *Марков В.* О возможности использования автоматизированных методов обработки информации в правотворческих процессах // Правоведение. 1989. № 4. С. 13–19; *Ольшанецкий А.Г.* Содержание правового обеспечения АСУ и формализация правовых норм // Правовые проблемы АСУ. М., 1973. С. 47–50; *Он же.* Проблемы формализации правовых норм // СГП. 1974. № 2. С. 127–130; Право и информатика / под ред. Е.А. Суханова. М., 1990; Применение математических методов и вычислительной техники в праве, криминалистике и судебной экспертизе: мат. симпозиума. М., 1970; Проблемы правовой кибернетики: мат.-лы симпозиума. М., 1968; *Прянишников Е.А.* Автоматизированные системы правовой информации капиталистических стран. М., 1978; *Раудсалу В.Ю., Ребане И.А., Сильдмяэ И.Я.* О создании автоматизированной системы юридической информации // СГП. 1974. № 5. С. 28–36.

Благодаря Интернету мы уже теперь имеем по сути неограниченные возможности хранения, передачи, поиска и обработки любых объемов знаковой, образной, звуковой и аудиовизуальной информации. Оставаясь в своей московской квартире или офисе, каждый из нас может «позвонить» хоть по аудио-, хоть по видеосвязи в любую точку мира, отправить кому угодно (например, в любой государственный орган, муниципалитет, банк, патентное ведомство и т.д. любой страны мира) и получить от кого угодно любые документы, провести переговоры, купить любой (!) товар (естественно, получив исчерпывающую информацию о его производителе, составе, рецептуре, способе эксплуатации и пр.), уплатить любую (!) денежную сумму в любой валюте (!) в любое время (хоть в 3 часа ночи) из любой и в любую точку мира (!), проконсультироваться у врача или юриста, внести вклад, взять кредит, «купить» полис страхования жилища и домашнего имущества, медицинского страхования или ОСАГО, да и вообще заключить практически любой (!) договор; посмотреть (в реальном времени!), что происходит на другой стороне Земли, прогуляться по улицам Лондона, Вашингтона или Сиднея, взобраться на Пирамиды и Мачу-Пикчу, совершить виртуальные экскурсии в основные музеи мира, пролистать как минимум каталоги, а может быть, и кое-какие (уникальные!) оцифрованные издания из РГБ, *British Library*, Библиотеки Института Макса Планка или Конгресса США, ознакомиться с любой отечественной нормативно-правовой документацией, а также оригинальными (и главное – актуальными!) текстами *Allgemeines bürgerliches Gesetzbuch, Bürgerliches Gesetzbuch, Code Napoléon, DCFR, PECL, PICC, Sale of Goods Act, Schweizerisches Zivilgesetzbuch (Code civil suisse/Codice Civile Svizzero/Cudesch civil), UCP600, Uniform Commercial Code, York-Antwerp. Rules*, и мн. др. источниками, прежде доступными только «избранным»; предъявить иск или претензию, подать жалобу и возражения, поприсутствовать на судебном процессе (как на собственном в качестве истца или ответчика, так и на чужом в качестве зрителя), послушать (и посмотреть «интерактивные») лекции или семинары всемирно известного профессора (при необходимости даже задать ему интересующие вопросы), послушать и посмотреть концерт в Венской опере или в Ла-Скала, поучаствовать в научной или международной конференции, организованной под эгидой ООН, юридического факультета МГУ или *LCIA*, пройти курс дистанционного обучения практически по любой дисциплине, настроить любой (!) музыкальный инструмент и т.д.

и т.д.[1,2] Словом, даже изменения, *уже произведенные* Интернетом в нашей жизни, колоссальны; изменения же, которых можно ждать уже в самое ближайшее (и на которые можно надеяться в чуть более отдаленное) время, не поддаются никакому воображению – реальная жизнь будет несоизмеримо богаче любой фантазии.

Под стать всему этому и изменения, произведенные Интернетом в праве[3].

[1] Конечно, Интернет предоставляет массу разнообразных возможностей по достижению разного рода *противоправных* целей, например: по хищению имущества у всякого и каждого (включая банки, страховые компании, промышленные и торговые предприятия, рядовых граждан – владельцев банковских, в особенности карточных, счетов, электронных кошельков, лицевых счетов по оплате услуг операторов мобильной связи и пр.); по усложнению жизни всякому и каждому (например, путем хищения, видоизменения или уничтожения электронных записей о регистрации юридических лиц, прав и сделок с недвижимостью, актов гражданского состояния и пр.); возможностей в сфере оскорблений и клеветы и пр. Пока подобные возможности мы не обсуждаем.

[2] Разумеется, Интернет активно используется не только частными лицами, но и *публично-правовыми образованиями*. Для чего? Посмотрим на этот вопрос вот с какой точки зрения: примем во внимание, что развитие интернет-технологий сегодня происходит в общем и в основном благодаря *частной* инициативе и *частным* деньгам (т.е. без сколько-нибудь активной помощи государств), но в то же время *и без сколько-нибудь заметного противодействия государств такому развитию* (исключая, конечно, Северную Корею и иные подобные, очень немногочисленные и совсем уж критические случаи). О чем это говорит? О том, что ***средством, способным внести весомые позитивные перемены в общественную жизнь, государства Интернет пока что не считают***. Считали бы – непременно и тесно им бы занялись. В то же время государства, очевидно уже увидели в Интернете ***средство минимизации последствий проявления некоторых негативных тенденций и факторов, сопутствующих современному этапу социального развития***. Очевидно, стало быть, что для государств Интернет есть в первую очередь средство (а) *управления общественным мнением* (его успокоения, возбуждения, консолидации, раздробления, направления в нужное русло и т.п.); (б) *утилизации различного рода социально неустойчивых (маргинальных) элементов*, – средство занять их, заполнив свободное время и предоставив возможности для относительно безобидной самореализации (пусть лучше народ ругает власть в «Одноклассниках», чем на Болотной площади); (в) средство получения информации о планируемой и осуществленной противоправной деятельности во имя *предупреждения, выявления и раскрытия преступлений*.

[3] Российская литература по интернет-праву огромна; иностранная (по *Cyber Law или Digital Law*) – просто неисчислима. Назовем буквально несколько ключевых отечественных монографий (по различным аспектам нашей темы): *Азаров М.С.* Правовой институт доменных имен в развитии информационного пространства России. М., 2010; *Бабкин С.А.* Интеллектуальная собственность в глобальной компьютерной сети «Интернет»: проблемы гражданско-правового регулирования в России и США (сравнительно-правовой анализ): дис. ... канд. юрид. наук. М., 2005; *Он же.* Интеллектуальная собственность в Интернет. М., 2006; *Он же.* Право, применимое к отношениям, возникающим при использовании сети «Интернет»: основные проблемы. М., 2003; *Вацковский Ю.Ф.* Доменные споры. Защита товарных знаков и фирменных наименований. М.,

2. **Предварительные замечания и общие вопросы.** В задачи настоящей статьи не входит выработка ни своего собственного, ни (тем более) универсального *юридического* определения понятия Интернет. Трудности, которые при этом придется преодолеть, и время, которое для этого нужно будет потратить, весьма значительны, а те достижения и выгоды, которые полученный результат мог бы иметь, весьма эфемерны[1]. Для наших целей будет вполне достаточно охарактеризовать Интернет с чисто функциональных позиций, а именно – как ***средство размещения (предоставления), хранения, поиска, доступа, обработки и использования информации, представленной в виде электроманитных сигналов*** (цифровом виде). Чуть более подробное описание, мини-

2009; *Войниканис Е.А.* Право интеллектуальной собственности в цифровую эпоху: парадигма баланса и гибкости. М., 2013; *Войниканис Е.А., Якушев М.В.* Информация. Собственность. Интернет: традиция и новеллы в современном праве. М., 2004; *Герцева Е.Н., Гринкевич А.П.* Доменные споры. Судебная практика в России. М., 2014; *Даниленков А.В.* Интернет-право. М., 2014; *Дмитрик Н.А.* Осуществление субъективных гражданских прав с использованием сети Интернет. М., 2006; *Дремлюга Р.И.* Интернет-преступность. Владивосток, 2008; *Комаров А.А.* Интернет-мошенничество: проблемы детерминации и предупреждения. М., 2013; Компьютер и Интернет в нотариальной практике: практ. пособие / отв. ред. Й. Беттендорф; пер. с нем.; предисл. В.В. Яркова. М., 2005; *Корупаев А.Е.* Права человека в Интернете, киберпространстве и компания Google. М., 2011; *Кудашкин Я.В.* Административно-правовое регулирование отношений в сети Интернет в РФ. Саранск, 2012; *Лебедева Н.Н.* Право. Личность. Интернет. М., 2004; *Луцкер А.П.* Авторское право в цифровых технологиях и СМИ. М., 2005; *Минков А.М.* Рассмотрение споров о доменных именах в соответствии с процедурой UDRP. М., 2004; *Миронова С.Н.* Использование возможностей сети Интернет при разрешении гражданско-правовых споров. М., 2010; *Наумов В.Б.* Право и Интернет: очерки теории и практики. М., 2002; *Незнамов А.В.* Особенности компетенции по рассмотрению Интернет-споров. М., 2011; *Петровский С.В.* Интернет-услуги в российском праве. М., 2003; Правовые аспекты использования интернет-технологий / под ред. Д. В. Головерова, А.С. Кемрадж. М., 2002; *Рассолов И. М.* Право и Интернет: теоретические проблемы. М., 2009; *Он же.* Интернет-право: учеб. пособие. М., 2012; *Салиев И.Р.* Гражданско-правовое регулирование электронной торговли в сети Интернет. Тюмень, 2011; *Сальникова Л.В.* Сделки в Интернет. Советует юрист. Ростов н/Д, 2006; *Серго А.Г.* Доменные имена. М., 2006/2013; *Он же.* Доменные имена в свете нового законодательства. М., 2010; *Он же.* Интернет и право. М., 2003; *Середа М.Ю., Середа В.Н.* Защита прав и свобод человека и гражданина в сети Интернет. Воронеж, 2013; *Тедеев А.А.* Информационное право (право Интернета): учеб. пособие. М., 2005; Телекоммуникационное законодательство: сб. / сост.: Ю.В. Волков. Екатеринбург, 2006; Трансформация авторского права в Интернете: зарубежные тенденции, бизнес-модели, рекомендации для России / под ред. И. Засурского, В. Харитонова. М., 2013; *Чеботарева А.А.* Средства массовой информации в сети Интернет: проблемы юридической ответственности. Чита, 2009. См. также современную литературу по информационному праву, правовой информатике и кибернетике, кибербезопасности и кибер-преступности.

[1] Ибо неясна самая *цель* существования в праве такого определения.

мально раскрывающее основные признаки определяемого понятия, могло бы быть следующим: ***Интернет – это организационно-централизованная система (сеть) оконечных электронных устройств, связанных кабельной и эфирной связью, позволяющая заранее неопределенному кругу лиц («всякому и каждому») одновременно*** (а) ***размещать,*** (б) ***хранить и*** (в) ***искать информацию, размещенную на соответствующих устройствах,*** (г) ***получать доступ к такой информации,*** (д) ***обрабатывать и*** (е) ***использовать ее, в частности видоизменять, копировать и осуществлять ее дальнейшее распространение от своего имени различными (в техническом отношении) способами***.

Разумеется, конкретные возможности совершения любого из перечисленных действий пользователями оконечных устройств *могут быть ограничены с помощью программных и технических средств*. Эти ограничения могут иметь различные цели и различный характер, могут быть постоянными (бессрочными) и временными, касаться всех или некоторых возможностей (например, только обработки информации или даже только некоторых ее способов), всех или только отдельных пользователей и т.д. Это – вопрос конкретных ситуаций (устройств, пользователей, обстоятельств и пр.), для наших целей пока не важный. Важен другой вопрос: ***каково главное юридически значимое свойство Интернета?*** Какое из качеств Всемирной паутины имеет *важнейшее* значение для сферы частного права. *Почему* и в чем это его значение состоит *конкретно*?

В приведенных выше описаниях мы отметили как раз несколько таких свойств сети, каждое из которых в том или ином отношении представляет важность для права, юридической практики и науки. Но главным из них – тем важнейшим качеством, которым предопределяются все *правовые* последствия, вызывающиеся к жизни наличием и эксплуатацией Интернета, – является ***неопределенный круг лиц*** (благодаря Интернету), ***получающих возможность одновременной работы с юридически значимой и (или) охраняемой правом информацией***. К информации, размещенной на любом из устройств (серверов), включенном в Интернет, может получить доступ ***любое лицо*** (располагающее соответствующими техническими и программными средствами) ***в одно и то же время***; российский ГК, как известно, называет размещение информации в сети Интернет ее ***доведением до всеобщего сведения***. В переводе на юридический язык это означает ***возникновение нового, невиданного прежде субъекта частного права – неопределенного круга лиц*** *или* (чуть более предметно) ***всякого и каждого***. Интернет совершил то,

что ранее было возможно лишь гипотетически: он *предоставил* ***реальную возможность совершения юридически значимых действий*** (*а*) ***любым интересующим нас лицом – в отношении всякого и каждого;*** (*б*) ***всяким и каждым – в отношении любого интересующего лица***. Подобного технического средства в распоряжении человечества еще никогда не было.

В самом деле, какие средства распространения информации (пока даже не станем говорить о средствах ее обработки) существовали ранее? Беседы личные и по телефону, переписка и телеграф, направление различного рода официальных заявлений, сообщений, уведомлений, повесток, доносов, расклеивание объявлений на столбах и в иных специально отведенных для того местах; получение доступа к дневникам и архивным документам – способы, которые с Интернетом нет никакого смысла сравнивать. Информация, передаваемая *такими* способами, по самой своей сути, очевидно, может быть доступна только очень и очень узкому кругу лиц[1]. Более перспективно сравнение с распространением информации посредством ее заключения в *полиграфическую продукцию – произведения печати* (книги, брошюры, журналы, газеты и т.д.). Очевидно, что и с информацией, распространяемой *таким* способом, тоже могут ознакомиться далеко не все желающие – их круг ограничен количеством напечатанных экземпляров (тиражом), некоторым числом посетителей библиотек, а также тех, кто ознакомится с нелегальной («пиратской») копией произведения[2]. Очевидно, однако, что и число потенциальных посетителей библиотек является ограниченным (вместимостью помещений, имеющимся в их распоряжении числом экземпляров произведения, временем работы и темпом исполнения читательских заказов и пр.), и количество «пиратских» копий (как бы велико оно в отдельных случаях ни было). Значит, остается конечным и число лиц, способных ознакомиться с информацией, распространяемой в печати.

Конечен и круг лиц, сведению которых могут быть доступны сообщения, передаваемые *по радио и телевидению,* – он ограничен

[1] Во все времена существовали, конечно, такие явления, как молва или «сарафанное радио» (распространение сплетен и слухов), но их можно сбросить со счетов, так как «информация», получаемая подобным образом, обычно никуда не годилась и ни для каких юридических целей использована быть не могла – ни с содержательной, ни с формальной точки зрения.

[2] По мере развития техники (ксероксов, сканеров, принтеров и т.д.) изготовление таких копий становится занятием все более быстрым и дешевым, а значит, доступным все большему числу «желающих».

числом соответствующих радио- и ТВ-приемников и особенностями тех конкретных мест, в которых они установлены (ими определяется то количество народа, которое способно одновременно находиться возле радио- (теле-) приемника и при этом слушать/смотреть соответствующую передачу). К ним следует прибавить некоторое количество тех, кто сможет ознакомиться с аудио- или видео*записью* передачи[1]. Точно так же конечен и круг потенциальных слушателей и зрителей публичных выступлений, театральных постановок, балетов, иных представлений, а также слушателей музыкальных произведений. Долгое время он был ограничен количеством лиц, способных получить информацию путем ее восприятия непосредственно в самый момент предоставления, т.е. присутствовать на соответствующем зрелищном мероприятии: ведь всякое место его проведения – дворец спорта, театр, аудитория, городская площадь и т.д. – обладает известной (ограниченной) вместимостью, а само мероприятие может производиться лишь с определенной частотой. Сегодня круг таких лиц расширился за счет тех, кто может послушать/посмотреть прямую трансляцию мероприятия, а также ее запись, но круг тех и других тоже является небеспредельным (конечным).

Наконец, произведениями живописи, архитектуры, скульптуры, кино- и фотоискусства поначалу могли наслаждаться только те, кто имел возможность их непосредственного восприятия на выставке, вернисаже, в музее, ином месте постоянного нахождения, установки или демонстрации. Число и таких лиц, как бы оно ни было в отдельных случаях велико, очевидно, всегда было и будет исчерпывающим (конечным). Сейчас и их круг стал шире за счет тех, кто удовлетворяется обозрением репродукций, фотоснимков и видеозаписей произведений искусства, тиражи которых, однако... тоже конечны. Значит, и в таком (суррогатном) виде произведения искусства оставались доступны далеко не всем.

Как же разительно отличается от всех рассмотренных способов распространения информации Интернет – ***техническое средство, обеспечивающее доведение информации до всеобщего сведения***! Притом не просто доведения до *всеобщего* сведения, но доведения ***быстрого*** (моментального), ***самого дешевого*** и ***технологически элементарного***.

[1] Возможности по оперативному и дешевому изготовлению таких записей даже в бытовых условиях современные технические средства (аудио- и видеомагнитофоны, средства цифровой аудио- и видео-записи) обеспечивают едва ли не лучше, чем копирование полиграфической продукции.

Чтобы оценить последние качества – скорость, дешевизну и простоту, сравним еще раз доведение информации до всеобщего сведения с помощью Интернета с распространением информации в полиграфической продукции. Сделаем следующее фантастическое допущение: пусть нам удалось изготовить такое количество экземпляров известного произведения, которое равно числу людей на Планете. Первый вопрос: *как скоро* каждый из этих экземпляров будет доставлен своему потребителю? Очевидно, для этого потребуется некоторое время, причем – даже с учетом возможностей современного транспорта и почты и в предположении об их наиболее полном и оптимальном задействовании – довольно значительное. О *дороговизне* такого способа распространения информации говорить, думается, не нужно (очевидно, что чем больше будет объем распространяемой информации и чем чаще ее будет необходимо обновлять, тем дороже выйдет), как и о *технической сложности* (попробуй, например, доставь журнал или газету какому-нибудь военнослужащему, моряку, геологу, заключенному или скрывающемуся от всего и вся неоплатному должнику). Интернет – среда принципиально иная: в ней информация распространяется и доставляется *со скоростью света*, при помощи таких технических средств, которые обеспечивают возможность ее *неоднократного* предоставления, получения и обновления *во всякое удобное получателю время*, притом таким образом, что *стоимость* этих операций мало связана с объемом предоставляемой, обновляемой и получаемой информации.

Еще одной очень важной в практическом отношении особенностью распространения информации через Интернет является *технологическое разделение актов ее предоставления и получения*. Особенно ярко она проявляется при ее сопоставлении с информацией, распространяемой в рамках *беседы*, где по сути своей дело не может обстоять так, чтобы ее участники действовали разновременно. Тот, кто в ходе беседы задает какой-нибудь вопрос, рассчитывает на *немедленное* получение ответа; тот, кто нечто сообщает, рассчитывает на какую-нибудь, но опять-таки *немедленную* реакцию на свое сообщение. Такой расчет невольно, но неизбежно *связывает* собеседника, заставляя этот расчет оправдывать. Даже если он по какой-то причине не может дать немедленного ответа или немедленно отреагировать на сообщенные ему сведения *по существу*, он все равно (исходя из самой сути понятия о разговоре (беседе, диалоге)) должен дать некую обратную связь, опять-таки *немедленную* (хотя бы объявить собеседнику, что ответить на вопрос прямо сейчас он не готов). Иначе общения не получится.

В Интернете дело обстоит принципиально иначе. Тот, кто заинтересован в распространении информации, своим *односторонним действием* (!) размещает ее в сети («вывешивает» на каком-нибудь сайте), понимая, что реакция на такое размещение может последовать *как немедленно, так и через какое-то* (может быть, значительное) *время, так и не последовать вовсе* (если размещенная информация никого не заинтересует). Почему? Потому что условия обмена информацией в Интернете таковы, что инициатива в *получении* информации и в *реакции* на нее всецело принадлежит *получателю* информации и от ожиданий лица, ее предоставляющего, никак не зависит. В этом отношении обмен информацией через Интернет похож на переписку: тот, кто получил письмо (телеграмму, *SMS*-сообщение и пр.), волен ответить на него как немедленно, через какое-то время, так и не отвечать совсем. Беседа «вживую» – это *акт один, единый и двусторонний*; беседа же в Интернете (как и обмен письмами) – это *совокупность двух* (*или более*) *односторонних актов*. К тому же круг реальных собеседников (как бы он ни был в том или ином конкретном случае велик – артист и публика, лектор и студенты, оратор и митингующие и пр.) все-таки всегда *конечен*; через Интернет же может пообщаться ***всякий и каждый***.

Почему же все перечисленные особенности Интернета мы считаем важными для права и юриспруденции; в чем пресловутая «важность» состоит конкретно? Выясним: «примерим» таковые к традиционным подразделениям частного права и видам субъективных гражданских прав. Начнем с прав ***исключительных*** и ***личных*** как прав на объекты *информационной* (!) природы, ибо Интернет как раз и есть средство работы с информацией; неудивительно поэтому, что тематика влияния сети Интернет на подобные права разработана в нашей литературе наиболее подробно[1]. Завершающая треть статьи будет посвящена обсуждению прав ***договорно-обязательственных*** и ***вещных***.

3. **Влияние Интернета на авторские и смежные права**. Итак, начнем. Почему расширение круга лиц – потенциальных участников доступа к информации и ее обработки – до неопределенно широкого (всякого и каждого) имеет принципиальное значение для авторского и смежных прав?

[1] См. сноску выше, содержащую перечень современных отечественных книг и диссертаций по интернет-праву. Даже по наименованиям видна их непосредственная связь с проблематикой исключительных прав и прав на средства индивидуализации.

Со всем тем, что «выложено в Интернет», теоретически может ознакомиться ***все человечество*** в течение самого короткого времени – того, что разумно необходимо на восприятие информации соответствующего содержания и объема относительно подготовленными к тому («средними») пользователями. Притом не просто *ознакомиться* – разово воспринять ту информацию, доступ к которой удалось получить, но и в известных пределах ее ***обработать и использовать***, в частности: (а) снабдить комментариями; (б) скопировать; (в) создать себе и (или) другим лицам возможность такого копирования; (г) распространить далее от своего имени, а в некоторых случаях – даже (д) изменить (исправить описки и фактические ошибки, перевести, переработать в иной текст или жанр и пр.). Все перечисленные действия могут преследовать различные цели, в том числе и *коммерческую* – извлечение прибыли лицом, их совершающим, его личное обогащение. Как к совершению подобных действий относится частное право? Позволяет ли оно совершать таковые всякому и каждому или же признает за кем-либо особые (монопольные, исключительные и т.д.) возможности по их совершению? Вообще, охраняет ли частное право состояния принадлежности (присвоенности) каких-нибудь ценностей *информационной природы*, а также возможности по фактическому над ними господству? Да, конечно, именно *информационную* природу имеют такие ценности, как ***результаты интеллектуальной деятельности***.

За последние 200 лет человечество уже привыкло к разделению результатов интеллектуальной деятельности на юридически ***неохраняемые*** (находящиеся в так называемом *общественном достоянии*) и ***охраняемые*** (находящиеся, как принято говорить, под копирайтом (англ. *copyright*)). Ряд информационных ценностей, воплощенных в объективную форму (в частности, записанных на материальный носитель), охраняется при помощи так называемых ***исключительных прав*** – *прав, в силу которых как самое совершение любых действий, направленных на копирование и эксплуатацию охраняемых объектов, так и* (*разрешение или запрет*) *таких действий составляют* ***исключительную прерогативу одного или нескольких конкретных управомоченных лиц***, в первую очередь субъектов ***авторских*** и ***смежных*** прав. Нарушители этих прав несут перед их обладателями установленную законом ответственность[1]. Но одно дело,

[1] Коллизионный аспект проблемы, т.е. вопрос о том, по законодательству *какого государства* надлежит обсуждать и охранять авторские и смежные права на произведения, размещенные в сети Интернет (по законодательству какого государства решается вопрос о том, имело ли место их нарушение и в чем оно состояло, определять меры и условия

когда личности таких нарушителей могут быть конкретно определены, а их число (как бы ни было велико) конечно. И совсем другое, когда весьма сильна презумпция того, что «нарушителем» известного права мог, вообще говоря, стать... ***всякий и каждый***.

Кто же это такой – «всякий и каждый»? Выше мы сказали, что по сути речь идет о *новом субъекте права* – да, с традиционных позиций это совершенно верно, но не надо упускать значительную специфику этого субъекта. «Всякого и каждого» к ответственности не привлечешь[1]; иска ко «всякому и каждому» не предъявишь; жестких дисков

ответственности и т.д.), мы оставляем за рамками настоящей статьи. Тот же подход мы применяем и во всех остальных случаях, т.е. говоря обо всех других типах субъективных гражданских прав. Отметим лишь следующее: коль скоро доступ к размещенному в Интернете объекту авторского и (или) смежного права можно получить из любой страны мира (а авторские и смежные права охраняются на территориях отнюдь не всех стран), то тем самым, очевидно, создается *возможность нарушения авторских и смежных прав пользователями Интернете, находящимися в тех странах, которые этих прав не признают и не охраняют*. *Фактически* данные лица будут чужое право нарушать, а *юридически* – нет. Иными словами, даже решив указанный в этой сноске коллизионный вопрос, мы все равно не сможем предоставить обладателю авторских и смежных прав необходимой юридической защиты. Если же учесть еще и то, что можно получить доступ в Интернет через серверы, функционирующие в любом государстве мира, то станет ясно, что ***при наличии на Земле хотя бы одного государства, чье законодательство не признает и не охраняет авторских (смежных) прав иностранцев, эти права можно будет нарушать совершенно безнаказанно***: достаточно будет получать доступ к охраняемым произведениям через серверы, находящиеся на территории такой страны.

[1] Впрочем, со всякого и каждого можно взыскать какой-нибудь (главное, чтобы определенный и равный для всех) *сбор*, например, «за доступ в Интернет» (условно – по копейке за каждый случай доступа к любому сайту, содержащему материалы, находящиеся «под копирайтом»), подобный тому, который взимается с покупателей средств аудио- и видеозаписи, аудио- и видеокассет, а также других аналогичных магнитных носителей, предназначенных для записи и воспроизведения объектов авторских и смежных прав. Конечно, совсем не обязательно, что все приобретатели «чистых» кассет и пр. непременно выполнят на них такую запись, которая будет рассматриваться как нарушение чьего-либо исключительного права; и тем не менее своеобразный «налог» на приобретение такой возможности платят все. Собранные таким образом суммы распределяются между авторами, исполнителями и производителями фонограмм, записываемых на подобные кассеты по 40, 30 и 30% соответственно (см. об этом п. 3 ст. 1245 ГК РФ). Подобная же судьба должна постигать и «интернет-сборы» (если они будут введены): они должны направляться на уплату вознаграждений лицам, чьи произведения размещены на посещаемых сайтах. Думается, что к этой же области относится и недавно предложенный (URL.: https://qz.com/911968/bill-gates-the-robot-that-takes-your-job-should-pay-taxes/) Биллом Гейтсом «налог на роботов»: платить его должны, конечно, не владельцы роботов (автоматических устройств), а лица, пользующиеся услугами этих самых роботов или приобретающие произведенную с их помощью продукцию, т.е. *потребители*. Собранные таким образом средства действительно могли бы направлять-

и флэш-карт «всякого и каждого» не осмотришь (на предмет того, не скачал ли этот «всякий и каждый» чего-нибудь неположенного); даже объяснений со «всякого и каждого» насчет того, не скопировал ли он чье-нибудь произведение, охраняемого авторским или смежным правом (?!) и если скопировал – то почему(?), что потом с этой копией сделал (?) – не потребуешь. «С миром не судись!», «на мир суда нет», «в миру, что в море: виноватого нет», «в миру жить – мирское и творить»[1], «миром положено – так тому и быть» – учит народная мудрость, ибо «от мира отстал – сиротою стал». Как та бабка, которая сердилась три года на весь мир, а мир того и не заметил.

В переводе с языка пословиц-поговорок на язык юридический сказанное можно выразить так: правильно ли в данном случае вообще рассуждать о каком бы то ни было *нарушении исключительного права*? Нарушение есть поведение аномальное, отклоняющееся от общего; такое поведение, которому стараются не следовать, а возможности для него, его условия и предпосылки – исключить и уж конечно специально не создавать. Здесь же все наоборот: вопрос идет о ***квалификации таких поведенческих актов, возможности к совершению которых с недавних пор имеет всякий и каждый***, притом ***благодаря*** чему же? – Интернету, т.е., ни много ни мало благодаря одному из ***результатов развития научно-технического прогресса***! Неужто право возьмет на себя смелость отрицать такой прогресс, бороться с ним, закрывать глаза на его наличие? Отрицательные ответы на все эти вопросы слишком очевидны, чтобы быть предметом особого обоснования и объяснения. Ну а если так, то возможное поведение *всякого и каждого* – это никакое не правонарушение. Напротив, это поведение *нормальное*, т.е. та самая ***норма***, на формальное закрепление, практическую реализацию, охрану и защиту которой и должны быть направлены усилия права.

Итак, получается следующее. Научно-технический прогресс *кардинально изменил те социальные условия, в которых приходится действовать праву*. Прежнее («до-интернетовское», «предцифровое») авторское и смежное право строилось по образцу и подобию *вещных* прав, а именно исходя из предположения о том, что *нарушение охраняемых им возможностей авторов, издателей, исполнителей и иных управомоченных субъектов* ***со стороны неопределенного круга лиц возможно только гипоте-***

ся на возмещение (в течение какого-то времени) утраченного заработка лицам, сокращенным в ходе автоматизации и роботизации промышленности, а также на оплату их профессионального переобучения и переподготовки.

[1] Вариант – «с волками жить – по-волчьи выть».

тически; ***реально же они могут последовать только от строго определенных конкретных лиц***. Круг этих лиц был так или иначе *ограничен,* в него входили лишь те, кто известным образом «соприкасался» (непосредственно взаимодействовал) либо с самим обладателем права, либо с экземпляром произведения, составляющего объект такого права[1]. Понятие «всякий и каждый» для этого («предцифрового») права было понятием не о субъекте права, а о социальной среде – массе законопослушных физических и юридических лиц – одном из условий действия права. Сегодня это мировосприятие уже неактуально. Интернет предоставил ***реальную*** (а не теоретическую!) ***возможность «нарушения» любых*** (!) ***авторских и смежных прав всякому и каждому***, т.е. с точки зрения традиционного права превратил доселе предполагаемую законопослушной массу граждан и организаций в «подозреваемых» – кандидатов на роль правонарушителей. Ни частное, ни публичное право прежде не сталкивалось ни с чем с подобным; соответственно ни то, ни другое ***просто не имеет в своем распоряжении правовых средств защиты, которые могли бы быть применены против всякого и каждого***. Это и понятно, ведь ***все*** правонарушителями быть никак не могут. Традиционное представление об авторском и смежных правах в новых условиях оказалось внутренне противоречивым; неудивительно, что базирующиеся на нем правовые нормы и субъективные права утратили способность к эффективному функционированию. До тех пор, пока соответствующим ситуации образом не изменится само право, пока оно будет оставаться прежним – тем, каким оно было до появления и широкого распространения Интернета, пока оно не станет ему адекватным, пока не превратится в интернет-право (*digital law*), оно *объективно не сможет предложить адекватных решений новых жизненных ситуаций*, ибо просто «не подходит» к ним, им не соответствует, на них не рассчитано. Да, когда-то оно было релевантным социальным условиям и среде; увы, но ныне ни этих условий, ни этой среды больше нет.

Конечно, какое-то количество конкретных лиц – уже не подозреваемых, а реальных нарушителей авторских и смежных прав на про-

[1] Так называемые *вещные* (нахваливаемые за их *абсолютность*) иски все равно всегда предъявляются *к конкретным ответчикам* – лицам, в данных обстоятельствах своими конкретными действиями воспрепятствовавшим, например, собственнику в деле осуществления им его хозяйственного господства над вещью. Аналогично строились и иски, направленные на защиту *личных неимущественных прав* (на жизнь, свободу, телесную неприкосновенность и пр.), и, разумеется, иски, направленные на защиту *авторских и смежных* прав.

изведения, «доведенные до всеобщего сведения» при помощи Интернета, – «отловить» все-таки возможно[1]. Так, например, очевидно, что к их числу будут относиться лица, которых пострадавшему автору, издателю, исполнителю, производителю фонограммы и т.д. «повезло» уличить в незаконном копировании (в частности, распространении) своего произведения, застать за его незаконной обработкой или иным неразрешенным использованием; ясно и то, что таким нарушителем будет и тот, кто «вывесил» соответствующий объект в Интернет без санкции правообладателя (если это имело место); согласно недавно появившимся нормам нарушителем авторских и смежных прав окажется и тот, кто «разломал» установленные правообладателем средства технической защиты произведения от копирования или обработки (опять-таки, если такие средства вообще были применены и если кто-то их «ломал»). Но это не отменяет того факта, что и все остальные частные лица – хотя бы и ни в чем конкретном и не замеченные – продолжают пребывать в числе «подозреваемых». То, что, допустим, на незаконном копировании известного произведения, вывешенного в Интернете, были пойманы лица A, B и C, еще не означает, что точно таким же (а может быть, и более эффективным, в более значительных масштабах) копированием не занимались лица D, E, F, G, H и т.д. вплоть до ***всякого и каждого***; более того, то, что A, B и C «попались» только на незаконном копировании, еще не гарантирует того, что они не сделали и чего-то еще (например, не создали условий для копирования и распространения объекта чужого исключительного права третьими лицами), в результате чего вроде бы охраняемое исключительным правом произведение рискует оказаться (если уже не оказалось) фактическим достоянием ***всякого и каждого***[2].

[1] Хотя и с этим связаны определенные сложности. Интернет, как никакая другая техническая среда, обеспечивает *анонимность пользования*; в результате применение традиционных норм права (о право- и дееспособности, юридических обязанностях, запретах, ограничениях и пр.) к пользователям сети Интернет оказывается невозможным без ряда *презумпций и постулатов, которые могут быть установлены только законом*. Центральный из них: ***лицом, совершившим все действия с определенного IP-адреса, предполагается владелец этого адреса (т.е. тот, на чье имя адрес зарегистрирован предоставившим его IP-провайдером), если не будет доказано иное***. Излишне добавлять, что подобных норм в отечественном законодательстве не имеется, а вопрос об их разработке пока даже не обсуждается.

[2] Сравним с «классическими» нарушениями абсолютных прав: *права собственности* (некто украл вещь), того же *авторского* или *патентного права* (некто изготовил и распространил известное число экземпляров произведения без разрешения автора или занялся выпуском и продажей товара, представляющего собой защищенное чужим па-

Описанная логика отчасти «работает» и в случаях с традиционными формами представления охраняемых исключительными правами произведений. Так, например, авторы книг и статей никогда не могут быть уверены в том, что напечатанные и распространенные с их согласия экземпляры таковых кто-нибудь не откопирует или не сдаст в возмездное пользование. Точно так же и исполнители известных произведений не могут быть уверены в том, что с записей их исполнений, законно выполненных и распространенных, не станут сниматься «пиратские» копии, что сами эти записи не начнут без их согласия и разрешения воспроизводиться в коммерческих целях, использоваться в различного рода рекламе, сокращаться, комментироваться, иным образом искажаться и т.д. Все может быть. Но нужно видеть принципиальную разницу: во всех подобных случаях количество нелегальных пользователей (нарушителей исключительного права) все равно будет ***конечным***, а в масштабах всего человечества – так еще и ***незначительным***. Даже самые кассовые фильмы (аудиовизуальные произведения) редко смотрит более 100 млн человек; тиражи охраняемых авторским правом бестселлеров почти никогда не превышают 50 млн экземпляров; аудитория самых популярных радио- и телепередач не дотягивает даже до этих цифр. Что же касается интернет-технологий, то они изменяют ситуацию радикально, поскольку ***предоставляют доступ к произведению-объекту авторских или смежных прав всякому и каждому***[1], а зна-

тентом изобретение без согласия патентообладателя), *личного права* (некто причинил гражданину смерть или телесное повреждение). Видно, что личность «традиционных» нарушителей всегда ***конкретна***, их число – всегда ***конечно***, и, главное, все остальные суть ***лица, свободные от всяких подозрений и обвинений***. Лица, *предполагаемые законопослушными, разумными и добросовестными*. С появлением Интернета дело стало обстоять совершенно иначе.

[1] Да, конечно, Интернет проник пока еще не в каждый дом. Из 7,340 млрд людей, живущих на Земле Интернетом пользуются «лишь»... 3,675 млрд человек (URL.: http://www.internetworldstats.com/). Но здесь нужно учесть несколько обстоятельств. Во-первых, даже существующая цифра не так уж и мала (половина населения Планеты!). Во-вторых, в отдельных странах (а именно такой показатель – памятуя о территориально-ограниченном действии авторских и смежных прав – и следует принимать в расчет) этот уровень много выше (например, в России или США Интернетом пользуется почти 75% населения; в Австралии, Германии, Франции и Южной Корее – около или более 85%; в Великобритании, Нидерландах, Швеции и Японии – более 90%). Не охваченными Интернетом остаются, главным образом, страны Африки и Западной Азии, т.е. страны, роль которых в деле международной охраны авторских и смежных прав и без Интернета весьма сомнительна. В-третьих, приведенный показатель на самом деле означает лишь количество оконечных устройств в сети, но не тех лиц, которые имеют доступ к таким устройствам. Об их числе он позволяет судить лишь предположительно.

чит, и ***не позволяют исключить из числа подозреваемых в нарушениях авторских и смежных прав вообще никого***. Интернет-технологии (с их «общим доступом» и «доведением до всеобщего сведения») оказались ***принципиально несовместимы с основами того общественного устройства, в рамках которого сформировались понятия об авторских и смежных правах, а значит – и с самими этими институтами***. Для отказа от Интернета и возврата к прежним условиям никаких предпосылок не имеется; стало быть, репутацию ***убийцы авторских и смежных прав*** Интернет получил вполне заслуженно.

Встречающиеся в литературе высказывания о некоторых «отдельных проблемах», «сложностях», «затруднениях», вызываемых Интернетом в деле обеспечения, охраны и защиты авторских и смежных правах, о недостаточной «гибкости» последних и необходимости их «трансформации», «усовершенствования», «приспособления» под воздействием Интернета для достижения какого-то «баланса» и «компромисса», представляются слишком мягкими; в жертву этой мягкости приносится суть происходящего. Быть может, непросто, но необходимо признать, что дальнейшее развитие и распространение интернет-технологий неизбежно должно будет привести ***к тому, что изучение авторских и смежных прав из удела цивилистов и коммерциалистов превратится в вотчину историков права***. Авторские и смежные права должны будут оказаться (если де-факто они еще не там) в юридическом архиве или кладовой, на чем-то вроде острова «съехавших» юридических талисманов – т.е. там, куда в разное время и по различным причинам были помещены многочисленные, чрезвычайно разнообразные, когда-то совершенно реальные и весьма функциональные юридические институты[1].

Так, например, очевидно, что с одного и того же (например, «домашнего») компьютера (*IP*-адреса) получить доступ в Интернет могут все лица, проживающие в месте его установки (доме или квартире), – а их обыкновенное число составляет три–пять человек; если же речь идет о рабочем месте в офисе, а тем более – о компьютере в интернет-клубе или кафе, открытом для доступа публики, то, очевидно, что число реальных пользователей сети нужно будет весьма существенно увеличить. Ну и, наконец, в-четвертых – это ведь только «пока»...

[1] Рабство, отцовская и мужняя власть, левират; элементы сословного устройства общества, включая дворянство, вилланство (холопство и прочие формы крепостной зависимости), коммендацию, корпорации купеческие (гильдии), ремесленные (цеха), религиозные (братства); феодальное, аллодиальное, вакуфное, чиншевое и четвертное землевладение; презумпция государственной собственности и генеральная ипотека; колхозное право и право трудовых товариществ (артелей); многочисленные государст-

Возможен ли какой-нибудь более мягкий сценарий – например, такое ***реформирование (качественное преобразование) авторских и смежных прав***, после которого соответствующие понятия («авторские права» и «смежные права») все-таки сохранятся? И да, и нет. Сохранение *терминов*, разумеется, возможно, вот только что они будут обозначать? Бесспорно, нечто совершенно иное, чем теперь. Соответствующие процессы мы уже имеем возможность наблюдать: в распоряжение обладателей прав, которые пока все еще по инерции продолжают называть *авторскими* и *смежными*, теперь предоставлены такие возможности, о которых еще два десятка лет назад никто не мог и помыслить. Таковы правомочия *разрешать/запрещать, контролировать и пресекать,* (а) *доведение* охраняемых произведений *до всеобщего сведения*; (б) изготовление, хранение, введение в оборот, импорт и даже самое *использование* (!) *электронных устройств* (любых или предоставляющих известные технические возможности); (в) *установку и применение технических и программных средств защиты* от копирования и распространения; (г) *действий, направленных на обход такого рода средств защиты*; (д) *эксплуатацию сетевых ресурсов*, содержащих «пиратский» контент. Все это великолепие пока венчает правомочие (е) требовать *конфискации* и *уничтожения* не только контрафактных экземпляров произведений (кстати, что это такое в современную цифровую эпоху?), но также *технических средств, материалов и оборудования*, используемых для доступа

венные регалии (монополии), в том числе банковского дела, валютная, внешнеторговая и др.; незаконнорожденные, в том числе внебрачные, дети и их узаконение; ограничение дееспособности расточителей; конкубинат; право первой брачной ночи; право барщины и иных форм отработок; право взимания вергельда и иных форм оброков; различного рода натуральные и денежные повинности; право посессионное и пропинационное; внутренний таможенный контроль; разделение имущества на родовое и благоприобретенное; крепостная форма юридических актов и ввод во владение недвижимым имуществом; высочайшие пожалования; религиозное (в том числе каноническое) и церковное право; манципация, стипуляция, делегация, корреальные обязательства, корабельные товарищества, береговое и морское призовое право, бодмерея; крестьянские земельные прикупки и заимки; общинное, чересполосное, подворное, усадебное и пожизненное наследуемое владение; трудовая и хозяйственная аренда, арендный, бригадный и семейный подряд; акции в смысле документарных ценных бумаг, общества с дополнительной (правильно – ограниченной) ответственностью, колхозные дворы и (вот-вот исчезнут с карты «юридического мира») личные подсобные хозяйства; оценочные неустойки; личное задержание за долги (долговая тюрьма или «яма»); ростовщичество, лихва, преимущество бокового наследования перед наследованием восходящим, улиточные записи, «вдовья часть», фидеикомиссы, вызов наследников и прочие подобные правовые «субстанции».

в Интернет, для изготовления и обхода средств защиты от копирования и пересылки информации, доведенной до всеобщего сведения, и некоторых других целей. Неужели кто-то и вправду думает, что объектами подобных правомочий все еще остаются *результаты интеллектуальной деятельности*? И если не думает, то при чем тут авторские и смежные права – права на *результаты интеллектуальной деятельности*? А ведь уже не за горами и такое правомочие, как возможность ***разрешать/запрещать заниматься известной деятельностью*** (например, программированием), если она осуществляется в целях обхода средств защиты от копирования, для самого такого копирования и распространения охраняемых правом произведений; нельзя поручиться и за то, что однажды в каких-то случаях за «авторами», «исполнителями» и прочими обладателями «исключительных» прав признают прерогативу ***разрешать, запрещать, пресекать и контролировать приобретение и принадлежность известных технических и программных средств***. Дело, конечно же, не в том, чтобы попытаться сейчас спрогнозировать то, в каком конкретно направлении будет эволюционировать содержание прав перечисленных лиц, а в том, чтобы не позволить забыть о следующем (собственно юридическом) вопросе: никаких оснований считать такие возможности компонентами *исключительных* (да и вообще, *субъективных*) прав нет и не может быть. Перед нами не просто «не-авторские» и «не-смежные» права, перед нами *вообще не субъективные права*. Перед нами – поведенческие возможности особого рода, юридическая природа которых нуждается в исследовании и выяснении.

4. **Интернет и права на средства индивидуализации**. От рассуждений о правах *авторских* и *смежных* логично перейти к соседствующей сфере – к ***правам промышленной собственности – патентным*** (т.е. правам на изобретения, полезные модели, промышленные образцы и селекционные достижения) и ***правам на средства индивидуализации, приравненные к результатам интеллектуальной деятельности*** (т.е. к правам на товарный знак (знак обслуживания), фирменное наименование, торговую марку, коммерческое обозначение, творческое имя, псевдоним и пр.). Оказывает ли Интернет – со своим «общим доступом» и «доведением до всеобщего сведения» – влияние на их существование, содержание, осуществление и историческую судьбу? Да, безусловно. Скажем больше, то, что Интернет представляет собой среду, не слишком дружественную, по крайней мере ***правам на средства индивидуализации***, заметили едва ли не раньше, чем присвоили ему звание «убийцы» авторских прав.

Если информация, размещенная в Интернете, становится «видимой» (доступной для поиска и ознакомления) ***всякому и каждому***, то Интернет оказывается средством, как будто нарочно созданным для распространения *информации* ***коммерческой*** – о предлагаемых к продаже товарах (работах и услугах), их достоинствах (если информацию распространяет продавец товаров) и недостатках (если речь идет о товарах, предлагаемых конкурентами распространителя информации), о ценах на них, условиях их поставки, доставки, монтажа (установки, подключения и пр.), текущего сервисного обслуживания, гарантийных сроках, содержании гарантий и порядке осуществления их и пр. Абсолютно естественно, что в ходе распространения *такой* информации самым широким образом используются (копируются, воспроизводятся) разнообразные и многочисленные ***средства индивидуализации, охраняемые правом того или иного государства*** (нескольких государств)[1]. Интернет-среда предоставила новые возможности по использованию таких средств – так, широко известны многочисленные споры о законности/незаконности применения известных брендов («Кодак», «Мерседес», «Грюндинг» и т.д.) в наименованиях интернет-сайтов (доменов), в электронных адресах и при межстраничной переадресации (в гиперссылках), но вместе с тем создала и почву для совершения новых, прежде невиданных деяний-нарушений исключительных прав на средства индивидуализации.

Подчеркнем следующее. Не надо понимать сказанное только в том смысле, что дело сводится к чисто количественным (математическим) изменениям: вот, дескать, раньше можно было использовать чужой товарный знак *только* (!) в вывесках, печатях, штампах, бланках, рекламе, газетах, журналах, на телевидении и на продукции, *а теперь стало возможно использовать его еще и другими, новыми способами* – на интернет-страницах, в названиях доменов и адресов, гиперссылках и т.д. Расширение возможных вариантов использования, конечно, тоже важно, но оно происходило и раньше. Сначала средневековый реме-

[1] Еще раз отмечаем, что вопрос о том, правом *какого государства* должны охраняться средства индивидуализации для того, чтобы обсуждать его применение к актам использования таких средств в Интернете, мы оставляем за рамками настоящей статьи. Во всяком случае, общедоступность средства индивидуализации, размещенного в Интернете, создает *возможность нарушения исключительного права на него пользователями, находящимися и в таких странах, которые соответствующего права не признают и не охраняют*. Иными словами, как и в случае с авторскими/смежными правами, будет существовать весьма значительное число лиц, *фактически* чужое право нарушающих, но с *юридической* точки зрения нарушителями не считающихся.

сленник наносил свое личное (или цеховое) клеймо только на готовые изделия; потом кто-то догадался вывесить изображение такого клейма перед входом в свою мастерскую; с распространением грамотности и возникновением периодической печати появилась возможность использования такого рода клейм (обозначений) в публикациях и т.д. и т.п. Человечество не стоит на месте, а значит, развиваются среди прочего и способы использования индивидуализирующих обозначений. В этом как раз нет ничего удивительного, и дело не в этом. Дело в том (и это очень важно правильно и точно понимать), что интернет-технологии внесли в нашу жизнь не просто *очередной новый способ* использования средств индивидуализации – они привнесли такой способ, который *принципиально отличается от всех* предыдущих. Чем (?) – как раз именно своей ***общедоступностью***. *Использование средства индивидуализации в Интернете формирует известную* (*правильную или неправильную*) *ассоциацию с данным средством индивидуализации* ***у заранее неопределенного круга лиц – всякого и каждого***.

Сравним несколько ситуаций.

Кого мог бы ввести в заблуждение недобросовестный коммерсант, маркирующий чужим (популярным и позитивно известным) товарным знаком *свою продукцию* (более низкого качества, почти не пользующуюся спросом, но зато много более дешевую)? Очевидно, только тех, кто воочию столкнется с этой продукцией на рынке, а точнее, у прилавков торговых точек и в стенах тех конкретных магазинов, где она будет предложена к продаже. Как бы велико ни было число экземпляров соответствующей продукции, как бы ни был широк круг ее «физических» продавцов и потенциальных потребителей, то, другое и третье всегда конечно, а в масштабах всего рынка аналогичной продукции – еще и незначительно. Сообразными будут и масштабы как выгоды, полученной правонарушителем, так и ущерба, понесенного правообладателем.

Идем дальше. Допустим, что наш недобросовестный коммерсант стал размещать чужой товарный знак еще и в *рекламе* своей продукции. К чему это приведет? Очевидно, *к расширению круга лиц*, готовых связать товарный знак с продукцией, ему не соответствующей. Магазинам придется столкнуться с наплывом покупателей, которые прежде в них даже не заглядывали. Откуда они возьмутся? Придут «по рекламе», которую увидят на биллбордах, прочтут ее в газетах, услышат по радио, посмотрят в кино или телепередаче. Но и такое расширение круга потребителей тоже не будет безграничным: круг тех,

кто придет «по рекламе», хотя и окажется шире, чем тех, кто «всегда заходит» в определенные магазины, но все-таки тоже будет конечным и во всяком случае вряд ли выйдет за пределы известной страны или даже ее отдельно взятого региона.

Но вот наш недобросовестный коммерсант совершает третий шаг: он рекламирует свою продукцию с использованием чужого товарного знака в *Интернете*. Чем последствия этого шага будут принципиально отличаться от последствий всех предыдущих шагов? Тем же, чем будут отличаться последствия контрафактной публикации в Интернете от последствий ее публикации в «бумажном» СМИ: благодаря Интернету соответствующая реклама будет ***доведена до всеобщего сведения, станет доступна всякому и каждому***; обратить на нее внимание и, значит, купить (заказать) товар способом, указанным в интернет-рекламе, сможет ***любой желающий во всякой стране мира***. Для обладателя права на товарный знак итог может оказаться весьма печальным: ***его товарный знак станет ассоциироваться с продукцией недобросовестного коммерсанта уже не на одном отдельно взятом рынке, а во всем мире***. В результате в течение какого-то времени (пока покупатели не сообразят, что их вводят в заблуждение) недобросовестный коммерсант получит возможность извлекать *необоснованную прибыль от сбыта своей продукции* (благодаря своей дешевизне, легко вытесняющей с рынка оригинальную продукцию), тем самым *причиняя ущерб обладателю права на товарный знак*, и все это – ***в масштабах всего мира***. Ни один ранее известный способ использования товарного знака подобной возможности не предоставлял. Как в таких условиях прикинуть хотя бы размер *компенсации* за нарушение исключительного права? Об *убытках* мы и не говорим.

Понятное дело, что не всякая *возможность* превращается в *действительность*. Обладатель права на товарный знак уж конечно не станет сидеть сложа руки, глядя на его незаконное использование. Судебный процесс, направленный как минимум на *запрет* дальнейшего использования товарного знака, на *изъятие из оборота продукции, им маркированной*, а также на выплату *компенсации*, обеспечен любому нарушителю. Ясно и то, что и правообладатель тоже постарается использовать Интернет для того, чтобы скорректировать формирующиеся (или уже сформировавшиеся) ошибочные ассоциации между его товарным знаком и чужой продукции. Но... насчет процесса мы немного сказали выше; что же касается попыток разубеждения общественности в ее заблуждении, то никак нельзя, очевидно, предсказать, будут ли они

более успешны, чем то, что уже достиг нарушитель. В итоге к убыткам правообладателя от незаконного использования его товарного знака присоединятся еще и расходы на рекламную антикампанию в Интернете, оказавшуюся бесполезной, а может быть – еще и судебные расходы.

Со средствами индивидуализации связан еще один любопытный аспект. Как уже отмечалось, до недавнего времени общественные ассоциации средства индивидуализации с известным товаром, лицом или другим предметом редко преодолевали географические границы страны – места нахождения коммерческого предприятия правообладателя. Почему? Прежде всего потому, что и *самые предложения товара к продаже долгое время могли быть сделаны только в достаточно ограниченных субъектных и территориальных рамках*. Да, имели место и исключения: транснациональные корпорации открывали свои представительства, филиалы и даже производственные предприятия во многих странах, в результате чего их продукция и товары расходились по всему миру. Соответственно, и средства индивидуализации (в первую очередь товарные знаки) становились одинаково знакомы потребителям разных стран и разных частей света, вследствие чего, кстати, возникло понятие «*общеизвестные товарные знаки»,* но и они (для приобретения такого статуса и получения международной охраны) должны были пройти определенную регистрационную процедуру. К тому же почти никогда не случалось так, чтобы обладатель права на известное средство индивидуализации сообщал ему одинаковую ценность *во всех* областях коммерческой деятельности. Руководствуясь именно этими соображениями, человечество установило принцип *регистрационной охраны средств индивидуализации*, придав ей ***ограниченное территориальное и предметное действие***: те же самые товарные знаки, к примеру, охраняются по общему правилу *только на территории той страны, где они в соответствующем качестве зарегистрированы*, и *только по тем классам товаров и услуг, которые заявлены при регистрации*.

Так было до появления Интернета. С появлением же такового коммерсанты получили возможность, как это было отмечено, ***доводить предложения о продаже товаров (производстве работ и оказании услуг) до сведения всякого и каждого***, т.е. ***предлагать свои товары (работы и услуги) в масштабах всего мира***. Теперь для этого совсем не обязательно становиться транснациональной корпорацией с производственными, торговыми и складскими помещениями в разных странах – достаточно иметь необходимый штат сотрудников и эффективно налаженное взаимодействие с организациями перевозки и свя-

зи (для своевременной доставки и пересылки купленных товаров)[1]. Не вставая с кресла в офисе, располагающемся на 36-м этаже одного из небоскребов Москва-Сити, вполне реально проинформировать о товарах, предлагаемых к продаже, потребителей, находящихся хоть в самой Москве, в Лондоне, Париже и Берлине, в Нью-Йорке, в Шанхае, в Сиднее, в Кейптауне, в Рио-де-Жанейро, в Гонолулу, на острове Пасхи. Даже тех потребителей, которые находятся в данный момент посреди Тихого океана на каком-нибудь круизном теплоходе, лишь бы на нем работали антенны, способные «поймать» сигнал соответствующего спутника. Даже Федору Конюхову, летящему на воздушном шаре над какими-нибудь африканскими джунглями, товары вполне можно предложить с помощью интернет-рекламы. И не просто *предложить*, но и в конечном счете *продать*. Подобное расширение масштабов коммерческой деятельности – от географически обособленных частей отдельных стран до всего мира – ***совершенно не соответствует прежде выработанным принципам правовой охраны средств индивидуализации***. А это значит, что в той же самой степени, в какой Интернет выступает убийцей авторских и смежных прав, он является ***убийцей еще и прав на средства индивидуализации***, по крайней мере в их традиционном – регистрационном, территориально и предметно ограниченном[2] – варианте признания и охраны. Какие возможности должны занять их место(?) – пока сказать невозможно; если таковые человечество когда-нибудь и выработает, то вряд ли они будут иметь что-то общее с традиционными. Новые возможности, предоставляемые Интернетом, должны быть облечены в адекватные правовые формы – *digital private rights*.

5. **Интернет и патентные права.** Теперь несколько слов о судьбе ***патентных прав,*** о том, что их ждет в самом ближайшем будущем при условии сохранения тех темпов и того направления развития сети Интернет, которые мы наблюдаем сегодня. «Несколько», потому что

[1] Дальнейшее развитие Интернета, очевидно, приведет к тому, что в скором времени не понадобится даже этого (см. подробнее далее).

[2] Ну и, конечно, в традиционном *содержательном*. Собственно говоря, многочисленные правомочия в сфере инспектирования, изъятия из оборота, конфискации и уничтожения товаров, с незаконно нанесенными на них товарными знаками и иными подобными обозначениями, признанные за обладателями исключительных прав на таковые Соглашением ТРИПС, – есть наглядное подтверждение сказанного. Будучи поначалу *правом на активные действия по исключительному использованию средства индивидуализации правообладателем,* оно уже сейчас превратилось в право на активные действия по запрещению, ограничению и пресечению такого использования посторонними лицами.

читатель в общем и сам уже сможет догадаться, о чем пойдет речь. Ведь патентные права, подобно правам на средства индивидуализации – базируются в своей охране на *регистрационном* начале, а сама их охрана имеет *территориально ограниченный характер*. Если продукцию и товары, представляющие собой (или заключающие в себе) охраняемые патентами технические и (или) художественно-конструкторские (дизайнерские) решения[1] либо селекционные достижения, Интернет позволяет ***предлагать к продаже всякому и каждому – неопределенному кругу лиц, – осуществляя, таким образом, коммерческую деятельность не в одной только отдельно взятой стране*** (например, той самой, в которой выдан соответствующий патент), ***а во всем мире*** (т.е. и в таких странах, патентами которых соответствующие решения не защищены), то очевидно, что патентное право в его традиционном понимании оказывается неспособным обеспечить такую деятельность. Или оно должно будет изменить свое содержание и принципы, или же оно будет дополнено какими-то новыми правовыми принципами, предписаниями и положениями, не похожими ни на что известное нам до сих пор. В самом первом приближении можно предположить, что *какой-то минимум возможностей коммерческой эксплуатации патентоспособных объектов через некоторое время* – по мере того, как международные торговые отношения будут дистанцироваться от политики, по мере того, как их глобализация и интеграция будут выходить на новые, более глубокие уровни – *будет признаваться и охраняться не только в стране, в которой выдан патент, но и за ее пределами*. Но, поскольку такая охрана не будет предоставляться во всем мире (в лучшем случае она охватит страны – участницы каких-нибудь международных конвенций (например, Парижской 1883 г.), или международных организаций (например, ВОИС или ВТО)), останется возможность нарушения даже этого патентного минимума на территориях (с территорий) других стран, тех, которые не станут участвовать в подобной охране. Вернее же всего то, что признание и охрана пресловутого минимума патентных прав станет осуществляться *независимо от наличия у претендующего на это коммерсанта какого-либо патента*, т.е. этот самый минимум будет охраняться не в ***регистрационном*** (патентном), а в ***декларационном*** (авторско-правовом) режиме. Во всяком случае, расходы времени и денег на получение патентно-правовой защиты в течение вот уже более

[1] Вариант – изготовленные с применением технических средств, оборудования или способов, которые охраняются патентами.

полувека таковы, что во многих случаях лишают ее всякого смысла. Ну а в последнее десятилетие человечество столкнулось с совсем уж невиданным явлением: громадное большинство патентоспособных объектов морально устаревают, прежде чем их успеют запатентовать!

Но это только один (уже успевший стать актуальным) аспект патентно-правовой проблематики. Есть и другой, пока менее очевидный, но в перспективе еще более серьезный аспект, делающий перспективы самого дальнейшего сохранения и существования патентного права весьма проблематичными. То направление, в котором сейчас развиваются информационные технологии, позволяет предположить, что ***уже не за горами тот день, когда Интернет станет точно таким же средством нарушения патентных прав, каким он уже успел стать применительно к правам авторским и смежным***. Строго говоря, уже теперь существуют запатентованные объекты, патентные права на которые, благодаря существованию и развитию интернет-технологий, могут быть нарушены (и, весьма вероятно, нарушаются) неопределенным кругом лиц (всяким и каждым), т.е. такие патентные права, которые де-факто оказываются ***бесполезными***. Чтобы было понятно, о чем идет речь, просто приведем несколько примеров такого рода объектов. Так, в некоторых странах патентно-правовой охраной пользуются такие объекты, как *программы для ЭВМ и базы данных* – ***цифровые продукты*** (*digital contents*), которые легко могут быть выложены в Интернет, после чего доступ к ним потенциально открыт всякому и каждому: их можно будет «скачать» (скопировать), а затем *практически использовать* на своем техническом оборудовании или, записав на материальные носители (диски, флэш-карты и пр.) *распространить* (ввести в оборот). Далее, даже в рамках российского законодательства можно патентовать различного рода *технологии, способы, рецептуры, методы и методики*, в частности, алгоритмы (совокупности команд), предназначенных для выполнения известных действий на ЭВМ, правила приготовления известных лекарств и пр. И эти патентоспособные объекты могут быть представлены в виде ***цифровых продуктов***, с которыми можно совершить все те же самые действия, какие совершаются по отношению к объектам авторских и смежных прав: их можно «выложить в Интернет», сделав доступными не только для ознакомления и копирования (скачивания), но и для *практического использования* (применения), а также *распространения* (в том числе на материальных носителях – введения в оборот). А все это, несомненно, входит в число правомочий патентообладателя. Затем по нашему законодательству можно запатентовать ряд изделий в каче-

стве ***промышленных образцов***, в том числе таких изделий, практическое использование которых может осуществляться в интернет-среде. Так, например, можно запатентовать в качестве промышленного образца макет интернет-сайта, газеты, книги, внешний вид шрифта, элементы декоративного оформления иллюстраций или текстов и пр. – все эти и другие подобные объекты без труда могут быть выложены во всеобщий доступ и стать предметом такого доступа.

Итак, мы видим, что уже сегодня (!) отдельные (не все!) объекты патентного права с точки зрения их доступности для использования неограниченным кругом лиц (всяким и каждым) ничем не отличаются от объектов авторского права. Но это – положение дел сегодняшнего дня. А что если заглянуть в будущее, хотя бы и совсем недалекое? Уже сейчас существуют и быстрыми темпами продолжают развиваться так называемые ***объемные*** (или ***3D-***) ***принтеры***: достаточно заправить такой принтер расходным материалом, соответствующим технологии его работы, и запустить соответствующую программу, чтобы на выходе получать... ***определенную вещь***. Классический материальный предмет, ничем не отличающийся от тех, которые потребители привыкли покупать на рынках, в киосках и магазинах, а предприниматели – получать с производств или складов. Пока круг возможностей таких принтеров невелик: предметы, которые с их помощью можно «напечатать», относятся к числу самых незатейливых, патентами не защищаемых. Но и их ассортимент уже достаточно широк – от различного рода аксессуаров и безделушек (чехлы для телефонов и смартфонов, брелоки для ключей, кошельки, шкатулки, бижутерия, пуговицы, заклепки, заколки, фигурки людей и животных и т.п.) до товаров самостоятельного значения, повседневного и широкого спроса (продукты питания, тарелки, чашки, ложки, вилки, ножи, другая посуда и столовые приборы, полотенца, скатерти, несложные по исполнению предметы одежды, обувь и пр.), а также сырья, материалов и запчастей (копии сломанных и изношенных деталей – шестерней, осей, колес и т.п.; гвозди, болты, шурупы, гайки, скобы, скрепы; оконные профили, рамы, стекла и даже сами готовые окна; элементы фундаментных, стеновых, кровельных и других строительных конструкций и т.д.). Нет никаких сомнений в том, что в скором времени ***на 3D-принтерах можно будет напечатать практически все что угодно, в том числе – предметы*** (устройства, машины, механизмы и т.д.) ***и биологические объекты, защищенные патентами на изобретения, промышленные образцы, полезные модели и селекционные достижения***. Интегральные микросхемы, соответству-

ющие запатентованным топологиям, в принципе, можно самопечатать уже теперь, а от их *массовой* самопечати нас отделяет максимум три года; самопечать копий любых памятников старины, произведений искусства, живописи, скульптуры, рукописей, книжных и журнальных изданий (как древних, уникальных, так и современных) станет возможна, как мы понимаем, уже лет через 5–7; ну а через 10–15 лет каждый желающий сможет позволить себе «напечатать» смартфон, ноутбук, часы, фотоаппарат, любой предмет бытовой техники, музыкальный инструмент, автомобиль, самолет и всякое вообще технически сложное изделие, смоделированное как по его индивидуальному «изысканному» вкусу, по требуемым конкретно ему размерам и прочим параметрам, так и с использованием любой опубликованной (тем паче – общедоступной) патентной информации[1]. Не будет никаких препятствий и к тому, чтобы печатать даже... *недвижимые вещи* (дома, иные здания, а также сооружения). Типографии в таких условиях либо умрут за ненадобностью (либо превратятся в пункты публичного доступа к объемным принтерам); функции издательств кардинально изменятся, а промышленным предприятиям, хоть какой угодно иной отрасли – металлургической, текстильной, пищевой, фармацевтической – останется производство... одних только расходных материалов для объемных принтеров. Промышленность добывающая, лесная и сельскохозяйственная, конечно, останется – она станет поставщиком сырья для выработки таких материалов; в той степени, в какой это окажется необходимым для перевозки того или другого, сохранятся транспортные компании. Но это практически и все[2]: детали для буровых установок, запчасти для горнопроходческих и зерноуборочных комбайнов, трубы для газопроводов по перекачке нефти и газа и даже элементы 3D-принтеров будут «печатать»... сами 3D-принтеры.

В таких условиях использование Интернета приведет уже не к *нарушениям* патентных прав, а опять-таки к их фактическому «убийст-

[1] Естественно, «напечатанные» элементы этих вещей потребуется собрать (смонтировать); очевидно, что создание роботов, занимающихся их сборкой, – ближайший этап развития индустрии самопроизводства товаров, открытой объемными принтерами. Пока этого не произойдет – сохранится надобность в услугах специальных сборочных предприятий или специалистов-сборщиков (монтажников, установщиков).

[2] Какое-то время еще будут сохраняться и такие производства, технология которых предполагает соблюдение известного времени – например, производства растительной, животной и кисломолочной продукции, копченостей, солений, сыра, вина, крепких спиртных напитков и т.п. Но постепенно, по мере развития технологий, отомрут и они; во всяком случае, их продукция не будет ни дешевой, ни массовой.

ву», точно такому же, какое уже произошло с правами *авторскими и смежными*. Лицо, имеющее необходимую квалификацию, сможет, ознакомившись с описанием существа запатентованного объекта, или (в зависимости от того, что представляет собой этот объект) – с комплектом его рисунков, чертежей или фотографий, написать *программу* по изготовлению такого объекта на объемном принтере[1]. Если эта программа попадет в сеть, то патентообладателю можно будет забыть о своем патенте: его «белая» (оригинальная, лицензионная) продукция окажется никому не нужной – будет дешевле и быстрее «напечатать» точно такую же продукцию, оплатив ресурс 3D-принтера (время, расходные материалы и, быть может, разовый доступ к соответствующей программе). А далее применительно к патентным правам становятся актуальными все те рассуждения и сомнения, которые мы сформулировали выше относительно судьбы прав авторских и смежных: ***в своем существующем виде и содержании они окажутся ничего не обеспечивающими и не защищающими***. Потребуется что-то поменять – создать ***digital patent law***[2], тем самым признав, что традиционных («бумажных») патентных прав более не существует.

6. **Интернет и личные права**. Но это все, наверняка возразят нам, права *исключительные*. Права на результаты интеллектуальной деятельности и приравненные к ним средства индивидуализации – права на объекты *информационной природы*. Да, немаловажные (особенно в современном – информационном, интеллектуальном и инновационном – мире), но все-таки далеко не единственные отделы частного права. А что же с другими его конструкциями, институтами и подотраслями? Претерпевают ли они на себе какое-либо влияние Интернета (и созданного им нового субъекта частного права – «всякого и каждого»), и если претерпевают – то какое? Может быть, Интернет является «убийцей» не только исключительных прав, но и каких-нибудь других

[1] Скоро такие программы будут писать ЭВМ, а чуть погодя... сами 3D-принтеры.

[2] Например, дать патентообладателю *возможность разрешать и запрещать создание программ самоизготовления запатентованного объекта* (в частности, на объемном принтере), *создание и распространение экземпляров таких программ*, а также *доведение таковых до всеобщего сведения*; исключительную возможность применения технических средств защиты таких программ от копирования и контроля за их использованием; права требования изъятия из оборота с последующим уничтожением экземпляров подобных программ, 3D-принтеров, иного оборудования и расходных материалов к нему, если они используются для нарушения патентных прав и т.п. См. примеры изменений, уже происшедших в содержании авторских и смежных прав, а также прав на средства индивидуализации, описанные выше.

подразделений традиционной («аналоговой») цивилистики? Весьма близки к правам исключительным ***права личные***, поэтому логично продолжить обсуждение именно с них.

Задача всяких ***личных*** прав – ***обеспечение идентификации и автономии личности***. Их объектами выступают различного рода нематериальные блага *социального происхождения*[1], и чем далее развивается общество, тем они многочисленнее. Таковы, в частности, *средства личной идентификации* (личное, профессиональное и творческое имя, внешний облик, изображение, подпись, документы, половая, социальная принадлежность, отношение к религии и пр.); *специальные наименования профессиональных, творческих и иных достижений, награды, титулы и звания*; *состояния неприкосновенности и конфиденциальности* (тайны, неизвестности) персональных данных, сведений о личной, семейной, творческой, коммерческой и иной деятельности, сведений о своем имущественном и правовом положении; *индивидуальные ассоциации, впечатления и психические переживания, связанные с самим собой, собственным состоянием и отношением к самому себе* (чувство собственного достоинства), *с конкретными лицами* (родственниками, друзьями, коллегами, знакомыми, «знаменитостями» и пр.) *и их организациями, предметами, событиями или явлениями*; наконец, таковы *социальные условия формирования социальных ассоциаций о лице* – условия формирования его доброго имени, чести, деловой, профессиональной, трудовой и иной репутации. Все это тот минимум (!) объектов, что охраняется во всяком современном обществе с помощью особого рода субъективных прав, обычно именуемых (в зависимости от того, с какой точки зрения – цивилистической или публичной – он освещает во-

[1] Нематериальные блага, существующие *объективно* (т.е. независимо от их признания или непризнания в обществе), такие как жизнь, физическое и психическое здоровье, душевное спокойствие, телесная и половая неприкосновенность, способности к производительному труду и творческой деятельности, к само- и социальной организации и, наконец, сообщаемая рождением свобода воли (свобода располагать собой, своим временем и всеми перечисленными ресурсами), рассматриваются правом как ***элементы нормального повседневного общественного устройства*** – элементы гражданского мира или правопорядка, а потому и ***охраняются правом непосредственно, без их признания объектами особых субъективных прав***. Такие нематериальные блага всегда *неразрывно связаны с конкретной личностью – их носителем*, а потому не могут быть ни отчуждены кому-либо, ни кем бы то ни было использованы, без установления чьих-либо прав на саму личность, т.е. без рассмотрения личности в качестве объекта прав. Излишне напоминать, что современному правопорядку подобные институты неизвестны.

прос) ***личными правами*** или ***правами человека***[1]. Выдерживают ли такие права «пришествие» Интернета? С большим трудом.

Возьмем ***права на разного рода средства идентификации*** – на профессиональное и творческое имя, на подпись, на изображение, внешний облик, манеру поведения, голос, визитные карточки и пр. Как можно было нарушить эти и им подобные права прежде? Можно было, например, выдав себя за другого (представившись чужим именем) попасть на какое-нибудь «закрытое» мероприятие (встречу, конференцию, банкет и т.п.); можно было подписать чужим именем свое сочинение (дабы привлечь внимание или к этому сочинению, или к тому имени, которым оно подписано); можно было присвоить себе авторство чужого сочинения; можно было воспользоваться чужими правами, льготами или привилегиями, чужим добрым именем, благожелательным или снисходительным к нему (его родственнику, другу, знакомому, работодателю и т.д.) отношением; можно было подписать чужим именем письмо какого-нибудь негодяйского содержания (дабы расстроить отношения мнимого подписанта с адресатом) или юридические документы, дабы «повесить» на чужое имя различного рода обязательства и т.п. Отличительная черта всех подобных нарушений – их ***чрезвычайно ограниченные со всех точек зрения масштабы*** (а значит – и ущерб, который они потенциально способны нанести, и выгода, которую они способны доставить), а вместе с тем ***высокий риск быть разоблаченным и привлеченным к ответственности***[2]. Даже публикация под чужим именем или присвоение авторства – как бы широко ни разошлось соответствующее произведение – не доставит ни нарушителю баснословных барышей, ни пострадавшему сколько-нибудь существенных проблем, ибо целевая читательская аудитория быстро раскусит как тот, так и другой подлог. Кстати, именно по этим причинам нарушения личных прав обычно затеняются их более существенными (имущественными) последствиями.

[1] Перечень основных международных (!) документов по этим вопросам см.: URL.: http://constitution.garant.ru/act/right/megdunar/. При всей его обширности этот перечень никак нельзя назвать полным; так, в частности, он не включает в себя Страсбургскую конвенцию (Конвенцию Совета Европы) о защите личности в связи с автоматической обработкой персональных данных от 28.01.1981 (рус. пер. М. Петросян. СПб., 1996) и некоторые другие значимые документы.

[2] Вспомним, как Остап Бендер наставлял недалекого Шуру Балаганова: «...Что это за профессия такая, прости господи! Сын лейтенанта Шмидта! Ну, год еще, ну, два. А дальше что? Дальше ваши рыжие кудри примелькаются, и вас просто начнут бить» («Золотой теленок», И. Ильф, Е. Петров).

Все меняется, когда приходит Интернет. Теперь перед нарушителем права на имя – уже не одна только *целевая* читательская аудитория, не *конкретный председатель* исполкома местного совета (как в примере с Шурой Балагановым), и даже не *конкретная* творческая или научная «тусовка», способная уличить и разоблачить любой подлог с именем и иным средством личной идентификации, теперь перед нарушителем открыты необозримые горизонты. То, что он сделает, Интернет ***доведет до всеобщего сведения***, в том числе и до сведения таких лиц, которые прежде не имели сколько-нибудь четкого представления ни о самом потерпевшем (обладателе нарушенного права), ни об объектах его личных прав. Слава Богу, если все ограничится размещением на сайте какой-нибудь белиберды о ценных бумагах, подписанной «В.А. Белов», или же объявлением того же самого «В.А. Белова» рецензентом каких-нибудь бредней по вексельному праву! – такие произведения все равно мало кого заинтересуют, кроме узкого круга профессионалов, а значит, последствия их интернет-размещения хотя и будут несколько отличаться от последствий их «бумажной» публикации, но не особенно сильно. А вот если некий негодяй свяжет с именем того же В.А. Белова деятельность по *краут-фандингу* (англ. *crowd funding* – сбор денег с неопределенного круга лиц) какого-нибудь сомнительного проекта (так называемого *стартапа* – от англ. *startup*), призыв к применению оружия массового уничтожения или какой-нибудь другой военно-политической авантюре, речь, ненавистническую по отношению к лицам той или иной профессиональной, национальной или социальной принадлежности, организацию *флэш-моба* (англ. *flash mob*) в поддержку рабовладения, торговли оружием или наркотиками, терроризма и пр., то последствия таких действий могут оказаться, конечно, самыми непредсказуемыми и весьма тяжкими[1]. И «спасибо» за эти последствия нужно будет сказать именно Интернету, ибо ни одна из традиционных форм распространения подобной информации – будь то заявления и обращения, сделанные вживую, напечатанные на бумаге, транслированные в эфир или сообщенные по кабелю – не смогла бы обеспечить ничего подобного той аудитории потенциальных получателей информации, какую предоставляют интернет-возможности.

[1] Последствия могут принять и вовсе глобальный масштаб, если подобные призывы, речи и высказывания приурочат не к «В.А. Белову», а к *публичной фигуре* – имени партийного, политического или государственного деятеля. Уровень занимаемой им должности и значение представляемого им государства на международной арене определят масштаб последствий – от общегосударственного до планетарного.

Идем дальше. Рассмотрим ***право на сохранение в состоянии неприкосновенности и неизвестности различного рода информации*** – начиная с персональных данных, сведений о своей заработной плате, состоянии банковских счетов, имущественном положении и обязательствах и заканчивая сведениями о заболеваниях, страхах, сомнениях, фобиях, чувствах, переживаниях, отношениях с родственниками и друзьями, об усыновлении и удочерении; начиная со своих стихов, писем и дневников и заканчивая фотографиями, точно так же не предназначенными для чьего бы то ни было ознакомления, как эти самые стихи, письма и дневники. Когда в подобную тайну проникает какой-то *единичный конкретный излишне любопытный субъект,* это, конечно, очень неприятно, но не смертельно, ибо не только гражданское, но в ряде случаев и административное, а также уголовное законодательство позволяют сделать так, чтобы далее этого самого негодяя информация не ушла. Но что делать, если этот самый негодяй успел разгласить украденный «компромат», вывесив его в Интернете? Увы, сделать будет уже ничего невозможно. Слово не воробей: вылетит – не поймаешь. Тем более, если этот воробей влетит в Интернет: сколько бы времени украденная информация ни «провисела» на сайте, невозможно дать никаких гарантий в том, что она не разошлась далее. Как широко и к кому она разошлась; не продолжится ли ее распространение; какими путями; к каким последствиям все это приведет; – как скоро и в какой области пресловутый компромат «выстрелит»? – ничего этого предсказать в момент нарушения, конечно, невозможно[1]. С гражданско-правовой точки зрения это означает невозможность потерпевшего: (а) ни принять своевременные и адекватные ситуации (нарушению) меры по пресечению ее дальнейшего усугубления; (б) ни определить (хотя бы и самым приблизительным образом) сумму причиненных ему убытков[2]. Как в таком случае можно было бы наказать правонарушителя? Вопрос этот, очевидно, повисает в воздухе (остается без ответа).

Нельзя не принять во внимание еще и следующий (любопытный именно с частноправовой точки зрения) аспект проблемы. Хорошо

[1] Особенно болезненно эта неопределенность дает о себе знать, когда из-под контроля обладателя выходят не пылкие юношеские письма и пикантные фотографии (здесь-то с последствиями как раз все понятно), а информация, составляющая тайну (а) *коммерческую*, в частности *ноу-хау*; (б) *профессиональную* (банковскую, страховую, медицинскую и т.д.) и (в) *государственную*.

[2] О компенсации *морального вреда*, причинение которого в подобных случаях безусловно налицо, мы даже и не беремся рассуждать.

известно, что многие сведения, конфиденциальность которых частные лица желали бы сохранить, размещаются в Интернете... ***самими этими частными лицами***. Другое дело, что они не предназначаются для доведения до всеобщего сведения[1]. Так, например, два друга переписываются по электронной почте; в ходе этой переписки сообщают друг другу (не намереваясь сообщать никому более!) сведения, составляющие их личную, семейную, коммерческую и прочую тайну. По той же электронной почте один гражданин может общаться с медицинским учреждением, предоставляя сведения о состоянии своего здоровья и получая от него результаты своих анализов, обследований, осмотров и пр. документы, содержащие врачебную тайну; другой – переписываться с сотрудниками обслуживающего его банка; третий – со своими коллегами по работе и т.д. Затем одно лицо может предоставить другому доступ к своим фотографиям, выложенным в какое-нибудь «облако» или на какой-нибудь публичный сервер (файлообменник); может открыть для доступа конкретного лица какие-нибудь фотографии, картинки или записи в своем «Живом журнале» или на своей странице в социальной сети; больше того, бывает и так, что конфиденциальная информация выкладывается самим обладателем права на сохранение ее конфиденциальности даже в открытый доступ! Так может случиться, в частности, вследствие сбоя в работе программного обеспечения, по ошибке пользователя или же по его... наивности (глупости), потому что он просто «не подумал» о том, что сообщенные им сведения могут предоставлять хоть для кого-то какую-нибудь

[1] Вариант – информация размещается в сети Интернет *государственными органами*, по роду своей деятельности взаимодействующими с частными лицами в различных сферах общественных отношений, – налоговой и таможенной службой, службой валютного и экспортного контроля, органами государственной регистрации прав на недвижимое имущество и сделок с ним, органами кадастрового учета, ЗАГС, ГИБДД и т.д. Частные лица, быть может, и не хотели бы предоставлять им информацию о самих себе, своей деятельности, ее «товарных» и «денежных» результатах, но, увы, их никто об этом не спрашивает; выбора у них нет. В результате такая информация оказывается в базах данных государственных органов, в том числе – базах данных, которые ведутся в электронном виде на их серверах. Естественно, к этим базам данных или нет свободного доступа совсем, или он ограничивается предоставлением строго определенных данных в известном формате, но... кому же неизвестны сообщения о *хакерских атаках* (в том числе и успешных) на подобные серверы? Кому неизвестны случаи «сливания» конфиденциальных данных (включая все базы целиком) сотрудниками таких органов за деньги? Как быть частному лицу, конфиденциальная информация о жизни и деятельности которого оказалась доведена до всеобщего сведения из-за недостаточной «взломостойкости» подобных серверов и обслуживающих их сотрудников?

ценность[1]. Подобные ситуации порождают множество вопросов, в том числе частноправовых. Один из них – ***имеется ли в данном случае налицо вина потерпевшего и если да, то как она должна учитываться при решении вопроса о защите его интересов***? Конечно, никто не снимает вины с лица, «взломавшего» средства программной и технической защиты «закрытой» («подзамóчной») информации, – но ведь и тот, кто решил воспользоваться подобными интернет-технологиями, очевидно, также должен был отдавать себе отчет в том, что нечто подобное может произойти. Если тем не менее он (несмотря на подобный риск) все же довел задуманное до конца, т.е. выложил конфиденциальную информацию в сеть, то не стоит ли именно на него и возложить связанные с этим риски, по крайней мере некоторые из них (например, риск ненадежности пароля (типа «123») или сбоя использованного программного обеспечения)? Тем более, не возложить ли на него последствия собственных ошибок и глупостей?

Еще одна категория личных прав (последняя, которую мы здесь рассмотрим) – ***прав на надлежащие социальные условия формирования представлений о самом себе и других частных лицах*** (прав на условия формирования доброго имени, чести, достоинства, деловой и прочей репутации) – от своего нарушения с помощью сети Интернет, кажется, даже... выигрывает. Если не соответствующая действительности информация порочащего характера вывешена в Интернет, то, безусловно, налицо ее ***распространение*** (если режим доступа к ней ограничен) или даже ***доведение до всеобщего сведения***[2]. Конечно, в российских судах может возникнуть вопрос о *доказательствах* этого факта, но он, кажется, решаем: многие нотариусы (во всяком случае, московские) уже более десятка лет совершают такое «нотариальное действие», как *осмотр интернет-страницы и удостоверение ее содержимого*. Уровень же сегодняшнего развития средств доступа в Интернет уже таков, что позволяет обойтись даже без этого – судья может обратиться к соответствующему вэбресурсу прямо в ходе судебного заседания (не вставая с судейского

[1] Ставший уже классическим пример – случаи, когда дети сообщают на своих страницах в социальных сетях сведения о предполагаемом месте и времени проведения каникул, выходных или отпусков родителей. Сложенные воедино с данными о месте проживания таких пользователей эти сведения становятся идеальной наводкой для воров-домушников.

[2] Этот момент, кстати, может иметь значение еще и для *уголовного* права – для установления элементов объективной стороны составов таких преступлений, как клевета и оскорбление.

кресла), т.е. *наблюдать факт (процесс) распространения порочащих и не соответствующих действительности сведений непосредственно* (в реальном времени), а значит – и удостоверить этот факт и исследовать его в процессуально необходимых пределах. Вот только всякий ли судья захочет этим заниматься? Но это уже, впрочем, другой вопрос.

Да и насчет «выигрывает» мы, конечно, иронизируем. Никакого выигрыша от того, что порочащие и несоответствующие действительности сведения расходятся ***по всему миру*** и рискуют стать ***всеобщим достоянием***, нет и не может быть. Сколько народу прочитает «заказную» статью в областной газете, как местный предприниматель Сидоров под видом итальянской мебели продает мебель китайскую или польскую? В самом лучшем случае – несколько десятков тысяч человек. Аудитория, совершенно несопоставимая с кругом тех лиц, которые[1] смогут ознакомиться с соответствующей информацией в Интернете. Понятно, что для бизнеса уровня безликого «предпринимателя Сидорова» эта разница большого значения не имеет[2]; но если речь заходит о субъекте – участнике рынка национального масштаба, тем паче – о транснациональной корпорации, разница будет более чем очевидна. Много ли народу узнает о ногтях в гамбургерах, мышиных трупиках в бутылках с газированной водой или о сбое в работе банковских карт в какомнибудь областном (тем более районном) центре, из *местной* газеты? Ответ очевиден. А из Интернета? Ответ еще более очевиден: притом, чем *крупнее* та корпорация, под эгидой которой продаются гамбургеры, изготовляется «газировка» или эмитируются банковские карты, тем более широкий резонанс соответствующая публикация вызовет; тем более масштабными и ощутимыми станут ее последствия как для репутации, так и для выручки (и прибыли) компании. Сообщение об одном мышином трупике, случайно закатанном в бутылку «газировки» где-нибудь в Бразилии, Венгрии или Новосибирской области, окажется способным если не обрушить, то существенно ударить по бизнесу недосмотревшей компании *во всем мире*. Даже если в последующем выяснится, что сообщение не соответствовало действительности. И все благодаря чему? Интернету!

[1] Даже с учетом языкового барьера и явно невысокой посещаемости тех сайтов, которые согласятся разместить у себя подобную публикацию.

[2] Хотя может и иметь: при распространении порочащих сведений через областную газету Сидорову (дабы нивелировать нанесенный его бизнесу ущерб) достаточно будет переориентировать свой бизнес на потребителей из соседних регионов; в случае же с Интернетом это уже явно не спасет.

7. **Интернет и договорно-обязательственное право.** О возможности использования системы Интернет для ***переговоров, переписки*** и ***обмена документами***, в том числе представляющими собой с юридической точки зрения ***оферту*** и ***акцепт***[1], а значит – и о возможности заключения, изменения и расторжения традиционных гражданско-правовых договоров (установления, изменения и прекращения договорных обязательств) с помощью Интернет, говорить, кажется, уже и не стоит. Почему? Потому что для большинства стран это уже давно известный и в значительной мере пройденный этап. Правда, в России договоры до сих пор предпочитают подписывать по-старинке, заботясь о «синих» (собственноручных) подписях и «синих» же оттисках печатей – для этого народ просиживает многие часы, выпивает литры кофе и съедает пачки печенья (как это было столетия назад) в очных переговорах, «обеспечивает» визы и подписи руководства, после чего обменивается подписанными «оригиналами» договоров посредством курьерской и почтовой связи[2]. Никто в мире уже давно не делает не только *так*, но и мало кто использует для этого возможности куда более оперативных непосредственных контактов, предоставляемых Интернетом. Вчерашний день.

Точно так же, видимо, уже не стоит особо долго говорить и об использовании Интернета для целей заключения ***типовых контрактов*** – тех самых, условия которых предлагается сперва прочесть, недостающие графы (если они там есть) – заполнить, а затем, поставив необходимую «галочку» («Я принимаю условия», «Я согласен с условиями» и т.п.) и кликнув «мышкой» на кнопке «ОК», заключить договор. Так заключаются договоры на приобретение (поставку) программного обеспечения, баз данных, о предоставлении доступа к литературным, художественным, музыкальным и графическим оцифрованным произведениям, об оказании платежных услуг, услуг

[1] А также любые юридически значимые заявления, сообщения, уведомления, кредитные и верительные письма, доверенности, справки, гарантии и причие подобные документы. Здесь главный юридический вопрос состоит в том, с какого момента такие сообщения следует считать полученными их адресатами; по всей видимости, это *момент, с которого адресат имеет обычную возможность получения доступа к содержанию таких сообщений*.

[2] Почему так происходит? Причин много; на поверхности лежат три, видимо, главные: (а) в стремлении не исполнять собственных обязательств российские частные лица готовы «цепляться» за что угодно, в том числе отрицать очевидное; в результате (б) никто никому ни в чем не верит, к тому же (в) «синих» подписей и печатей требуют... государственные органы. Грустно.

электронной очереди, услуг по приему и передаче данных и т.д. и т.п. Заключение и исполнение таких договоров сегодня уже мало кем замечается. Как в середине прошлого века вызывало удивление и непонимание заявление о том, что, получая в автомате стакан минеральной воды, вы тем самым заключаете договор купли-продажи, а входя в автобус – договор перевозки пассажира, точно так же большинство современных пользователей сети Интернет вряд ли задумываются над тем, что, каждый раз нажимая виртуальные кнопки «ОК», они принимают условия какого-нибудь договора, настолько распространенным, само собою разумеющимся, простым и естественным стало это действие.

Далее, пока есть еще некоторый смысл в том, чтобы обратить внимание на средства Интернета как среду и платформу, предоставляющую в распоряжение частных лиц ***новый способ совершения договорно-имущественных предоставлений***, в том числе во имя установления, исполнения, изменения и прекращения обязательств. Нужно купить определенную программу; базу данных; цифровые копии объектов исключительных прав? – уже давно нет надобности заказывать пересылку или доставку диска с записями подобных «ценностей», ибо все они могут быть пересланы в виде файлов (или гиперссылок, предоставляющих возможность «скачивания» файлов с тех удаленных серверов, на которых они размещены). Точно так же, введя определенные данные (например, о своей кредитной карте, номере онлайн-счета и т.п.), заполнив необходимые сведения о планируемой транзакции и нажав очередное «ОК», можно заплатить следуемую с вас по какому-нибудь основанию денежную сумму. Это может быть платеж *по собственной инициативе производящего его лица* (например, в качестве аванса, во имя предоставления займа, уплаты страхового взноса и т.п.), во исполнение каких-нибудь *гражданско-правовых обязательств* (например, по оплате приобретенных товаров, жилищно-коммунальных услуг, услуг телефонной связи, алиментов, в целях возврата кредита и пр.) или, наконец, какой-нибудь *публично-правовой обязанности* (уплата налога на имущество, государственной или таможенной пошлины и пр.). Видно, что круг имущества, которое можно «передавать» (пересылать) с помощью Интернета, ограничен одними только виртуальными (цифровыми, информационными) объектами, но это только пока, как отмечалось выше (в отделе настоящей статьи о патентных правах), не за горами то время, когда присланные по Интернету виртуальные объекты

смогут приобретать абсолютно осязаемую (вещественную) форму[1]. Очевидно, что с течением времени использование возможностей сети Интернет для имущественных предоставлений будет расширяться.

Затем есть смысл обратить внимание на те возможности Интернета в сфере договорно-обязательственного права, которыми можно воспользоваться, ***получив доступ к уже многократно помянутому новому субъекту права – неопределенному кругу лиц (всякому и каждому)***. Зайдем на любой сайт, который предлагает к продаже какие-нибудь цифровые продукты, например программное обеспечение. Увидим инструкции насчет того, что нужно сделать – где какие «галочки» поставить, какие поля и чем заполнить, на какие «кнопочки» нажать – для того, чтобы получить на указанный электронный адрес или ссылку для скачивания программы, или код ее установки/активации, или, наконец, сам файл, распаковка или запуск которого приведет к инсталляции программы. Вопрос: *какова юридическая природа предложения о заключении договора* (в частности, по продаже программного продукта), *сделанного на интернет-сайте*? Публичная оферта? И да, и нет. Да – потому что предложение это делается публике и выражает готовность того, кто его сделал, считать себя связанным договором с любым, кто на него отзовется – примет его (п. 2 ст. 437 ГК РФ); нет – потому это предложение становится достоянием не просто «публики», а *всякого и каждого*, т.е. ***доводится до всеобщего сведения***. Ни один из традиционных способов сделать публичную оферту[2] подобного не обеспечивает – обратиться ко всякому и каждому, сделать намерение обязаться по договору всеобщим достоянием (опубличить или огласить его) они не позволяют[3]. Интернет позво-

[1] Здесь, впрочем, можно задаться другим вопросом: а долго ли еще человеку будут необходимы такие реальные, материальные, вещественные объекты или, во всяком случае, большинство известных нам сегодня подобных объектов? Но этот вопрос в пределы настоящей статьи явно не вписывается.

[2] Жестикуляция и крики типа «Подходите, покупайте!», выставление товара в магазинных витринах, на выставках, ярмарках, площадях, в иных местах, открытых для общего доступа, раздача «флаеров», публикация, объявления по радио и телевидению и пр.

[3] Все сказанное распространяется и на *рекламу* в Интернете: теоретически ознакомиться с ней может кто угодно; разного рода современные технологии (например, так называемой контекстной рекламы) весьма сильно приближают такую возможность к действительности: даже если вы не собираетесь знакомиться с рекламой, вы все равно с ней ознакомитесь. Точно так же все сказанное касается и разного рода заявлений, сообщений, уведомлений и прочих подобных юридически значимых волеизъявлений, сделанных в Интернете. Будучи обращенными *к неопределенному кругу лиц,* таковые точно следует считать (или, во всяком случае, предполагать) ***до-***

ляет. Тот, кто разместит предложение о заключении договора не где-нибудь, а в Интернете, тем самым выразит *готовность связать себя соответствующими договорами со всяким и каждым*; иное должно либо следовать из существа объявления[1], либо быть прямо оговорено в нем. Получаем (а) *оферту, которая обращена ко всякому и каждому* и оттого (б) *юридически связывает оферента в отношении всякого и каждого*. Эта юридическая связанность есть состояние, обеспечивающее (в) *секундарные права, предоставленные всякому и каждому*; реализация таких прав односторонними действиями их обладателей способна привести к тому, что оферент окажется (г) *участником однотипных гражданско-правовых договоров со всяким и каждым*, т.е. должником по максимально возможному (предельно мыслимому) числу однородных обязательств, которые (д) ему рано или поздно нужно будет *исполнять*[2]. Ничего подобного частное право до сих пор не знало.

Ну и, конечно же, нельзя не упомянуть о том, что сегодня является, по-видимому, наивысшей точкой развития договорно-обязательственного интернет-права. Речь идет о явлении, известном в литературе как ***автоматизированные,*** или **«*умные*», *договоры* (*Smart Contracts*)**. Их главная отличительная черта сосоит в том, что *человеку достаточно лишь инициировать их заключение*; *все остальное* (в том числе

стигшими всех заинтересованных лиц**, в том числе и своих предполагаемых адресатов*, а содержащиеся в них сведения (например, об ограничении дееспособности, признании известного должника несостоятельным (банкротом), о внесении определенных изменений в устав юридического лица, о принятии общим собранием участников гражданско-правового сообщества известных решений, о наличии претензий или возражений относительно прав на известное имущество, о факте заключения и содержании определенных договоров, о выдаче, отзыве и возвращении доверенностей, об утрате или хищении определенных вещей, ценных бумаг и пр. ценностей, о протесте векселей и неоплате чеков и т.д.) – ***общедоступными. Разумеется, положительный закон волен обставить сказанное известными условиями, например, определить пределы юридического значения тех или иных актов волеизъявления, сделанных в сети Интернет, или предъявить к этим актам определенные требования (например, чтобы они совершались с использованием определенных сайтов, в известные сроки, в определенных выражениях, чтобы информация «бросалась в глаза» заинтересованным лицам, чтобы она «обнаруживалась» известными алгоритмами поиска и пр.).

[1] Например, если оно касается предложения к продаже какой-нибудь индивидуально-определенной вещи (картины, монеты, уникальной книги и пр.).

[2] Значит, должно быть налицо достаточное количество предметов, необходимых для исполнения подобных обязательств. Это возможно только при условии, что речь идет о предметах идеальных (умозрительных), в частности, о цифровых продуктах, работах, услугах, либо о предметах общего пользования.

само заключение таких договоров, при необходимости их изменение и расторжение, а также исполнение (!), притом именно самих договоров, а не обязательств, которых просто не будет возникать) *произойдет в автоматическом режиме* (без участия оферентов, акцептантов, кредиторов и должников). Наличие недавней (наинтереснейшей!) публикации А.И. Савельева освобождает нас от необходимости подробного рассказа об этом явлении[1]; кроме того, в скором времени должна выйти из печати и наша статья, посвященная одному из видов таких вот «умных» контрактов – договорам, направленным на установление и исполнение так называемых ***Bank Payment Obligations*** – банковских платежных обязательств[2]. Просто «для затравки» – т.е. если не заинтриговать, то хотя бы немного заинтересовать читателей (а заодно и подготовить их к восприятию происходящего, показав уровень тех проблем, с которыми юриспруденция уже столкнулась, что называется, лицом к лицу), – законспектируем несколько основных положений статьи А.И. Савельева[3]:

1) «...для развитого информационного общества периода повсеместного распространения «Интернета вещей» и искусственного интеллекта» будет характерно понятие автоматизированных договоров, предполагающих свое «...заключение... в дистанционном режиме и минимальное участие сторон в процессе его заключения, а также

[1] См.: *Савельев А.И.* Договорное право 2.0: «умные» контракты как начало конца классического договорного права // Вестник гражданского права. 2016. № 3. С. 32–60.

[2] Эта статья так и будет называться «Банковские платежные обязательства / Bank Payment Obligations (БПО/BPO): понятие, технология создания и применения, правовое регулирование, юридическая природа, соотношение со смежными институтами и отношениями». Она была написана в начале 2015 г. и планировалась к публикации в одном из сборников (который по независящим от нас причинам так и не вышел), а затем в одном из журналов (редакция которого, к сожалению, повела себя несколько некорректно). Будем надеяться, что статья эта все же будет напечатана в журнале «Коммерческое право», в его первом номере за 2017 г.

[3] Общее представление о содержании этих выводов позволяет составить уже само наименование статьи «...«умные» контракты как *начало конца классического договорного права*». Интернет, стало быть, оказался «убийцей» не только исключительных и личных прав. Мы в нашей статье (о БПО) столь радикальных выводов не делаем, напротив, стараемся (по возможности) «вписать» новый, доселе невиданный способ установления и исполнения обязательств (то и другое в БПО осуществляется «решением» электронной системы, принятым по результатам автоматического сопоставления загруженных в нее данных) в рамки традиционных правовых категорий, таких как оферта, акцепт, договор, обязательство, исполнение обязательства и т.д. Увы, сделать это у нас получилось не всегда. Видимо, следует согласиться с А.И. Савельевым в том, что такие попытки обречены на провал, что называется, *a priori*.

предопределенность большинства условий договора и параметров его исполнения электронными агентами»[1];

2) «...умные контракты... опосредуют перемещение определенных ценностей от одного лица к другому... опосредуют экономические отношения обмена»; они «...не падают на пользователя с неба, он должен выразить свою волю на участие в них, способом, установленным в соответствующей системе...»; «...после совершения таких действий лицо является связанным условиями такого договора, хотя... характер такой связанности существенно отличается от возникающего в традиционных договорах»[2];

3) такие договоры «существуют исключительно в электронной среде», заключаются по модели договоров присоединения и направляются на распоряжение цифровыми активами; их условия излагаются в особой форме и строго формализованным языком, в связи с чем приобретают повышенную точность (определенность); они имеют условный характер и исполняются, как уже отмечалось, без участия человека[3];

4) появление «умных» контрактов приводит, в частности, к тому, что «понятие «обязательство» и связанные с ним концепции утрачивают значение»[4] (оно и понятно, ибо если контракты исполняются без участия человека, то обязательства здесь, и вправду, ни к чему); ««умный» контракт не может быть нарушен»[5] (опять-таки потому, что техника и программное обеспечение неизбежно сделают следуемое[6]);

---

[1] *Савельев А.И.* Указ. соч. С. 41.

[2] Там же. С. 43.

[3] См. там же. С. 44–47.

[4] Там же. С. 48.

[5] Там же. С. 50.

[6] Практика, кстати, знает подобные «договоры», не имеющие отношения к использованию сети Интернет – они заключаются и исполняются в сфере *снабжения через присоединенную сеть* и *финансовых расчетов за фактически потребленный таким образом сетевой ресурс*. Подробнее см.: *Белов В.А.* Что такое передача через присоединенную сеть и является ли она передачей в юридическом смысле этого слова (traditio)? // Законодательство. 2011. № 8. С. 30–38; *Он же*. Гражданско-правовые формы отношений снабжения через присоединенную сеть // Проблемы современной цивилистики: сб. ст., посв. памяти профессора С.М. Корнеева. М., 2013. С. 149–190. Основная мысль, доказываемая в этих статьях – в том, что отношения снабжения энергией и товарами через присоединенную сеть облекаются не в обязательственную, а в особую, оригинальную правовую форму. Аналогичным («автоматическим») образом в течение вот уже многих десятилетий прекращаются «обязательства» («закрываются позиции» или, как еще иногда говорят, «схлопываются» отношения) из биржевых договоров. И по окончании торгового времени, с подведением итогов состоявшихся торгов, и в ходе самих торгов, если

«...для «умного» контракта иррелевантны пороки воли, допущенные на стадии заключения... в «умных» контрактах не может быть коллизии между волей и волеизъявлением: значение имеет [мы бы сказали просто: *существует*] лишь волеизъявление, выраженное в программном коде...»[1]; наконец, для функционирования «умных» контрактов «не требуется правовая система. Они вполне могут существовать и без права»[2].

Как говорится, ни прибавить, ни убавить!

Впрочем, нет, кажется, есть что прибавить: технологическая подкладка «умных» контрактов такова, что вполне способна обслужить не одно только заключение и исполнение договоров. Что бы, интересно, сказали российские деятели «от юридической практики», если бы им сообщили о создании, допустим, ***smart*** (***digital***, or ***electronic***) ***justice,*** т.е. системы ***«умного»*** (***цифрового*** или ***электронного***) ***правосудия***? Речь, разумеется, не о тех *web*-трансляциях из залов судебных заседаний, которыми нас примерно десять лет назад впервые удивил блаженной памяти Высший Арбитражный Суд РФ, а о процессе ***«машинного»*** (***автоматизированного*** – происходящего без участия судей, прокуроров, адвокатов) ***разрешения юридических споров***. Это же просто сказка какая-то: ***Digital Procedure Code***! Конфликтующие стороны, вводя в предлагаемые им для этого электронные формы известные фактические данные, загружают их в систему, которая через мгновение отвечает на все интересующие спорщиков вопросы – кто прав, кто виноват, кто, чего и с кого может требовать, кто, к чему и перед кем обязан и т.д. Существующие технологии (описанные, в частности, в указанной статье А.И. Савельева) позволяют создать подобные системы (правда, пока не по всем юридическим вопросам) уже сейчас. Можно организовать и такие системы, которые будут решать споры лишь после того, как стороны конфликта предоставят необходимое «электронное обеспечение» исполнения будущего решения; в таком случае системе даже не нужно будет информировать стороны о каких бы то ни было их правах и обязанностях – по результатам рассмотре-

курсы биржевых активов достигли таких цен (значений), преодоление которых (с учетом условий заключенных сделок) приведет к невозможности исполнения обязательств. Разница только в том, что сотню лет назад все эти вещи отслеживали котировальные комиссии и расчетные (клиринговые) отделы (палаты) соответствующих бирж; теперь же этим занимаются компьютерные программы.

[1] *Савельев А.И.* Указ. соч. С. 50–51.

[2] Там же. С. 53.

ния спора она просто произведет необходимые списания-зачисления по счетам оппонентов, направив им электронные выписки об автоматически совершенных транзакциях.

8. **Интернет и вещные права.** Или, вернее сказать, ***защищенные правом возможности по абсолютному господству определенного лица над известными ценностями***, не обязательно одними только телесными вещами. Но обо всем по порядку.

Проблема, касающаяся признания и юридической квалификации возможностей абсолютного господства над различного рода ценностями, назрела уже очень давно. Произошло это вне всякой связи с Интернетом. В этом легко убедиться, если вспомнить о существовании таких квазивещных нематериальных благ, как ***безналичные денежные средства*** и ***бездокументарные ценные бумаги***. Упоминание о тех и других с недавних пор «проникло» даже в ст. 128 ГК РФ, а бездокументарные ценные бумаги удостоились еще и подробной регламентации в нормах § 3 гл. 7 Кодекса. С традиционной юридической точки зрения оба рода ценностей сводятся к *относительным правам*. Безналичные деньги – это *денежные требования* клиентов к обслуживающим их банкам; бездокументарные ценные бумаги – опять-таки либо *денежные требования* их «владельцев» к эмитентам (облигации), либо корпоративные права (акции), либо секундарные (опционы эмитента). Записи обо всех этих правах составляют так называемые *счета – банковские*, если предметом записей выступают «безналичные деньги», или же *счета владельца бездокументарных ценных бумаг*, открываемые в реестрах таких владельцев или у депозитариев (счета депо). Как и всякие юридические возможности права, известные в обиходе под наименованиями безналичных денежных средств и бездокументарных ценных бумаг, могут быть ***осуществлены*** их обладателями – лицами, которым они принадлежат. Кроме того, будучи правами имущественными и способными к свободному обращению, безналичные денежные средства и бездокументарные ценные бумаги представляют собой предмет ***распоряжения*** со стороны обладающих ими лиц. Способности к осуществлению любых субъективных и секундарных прав, а также к распоряжению ими (т.е. способности к реализации признанных и обеспеченных правом (юридических) возможностей) – это ***элементы гражданской правоспособности***.

Если установленные общие положения верны, то они должны быть относимы в равной степени ко всем субъективным и секундарным правам или, по крайней мере, к подавляющему их большинству (кроме

строго личных). Предметом точно такого же осуществления и распоряжения выступают именно субъективные гражданские права, включая между прочим и такое широко известное, как ***право собственности***. Именно оно, это самое субъективное право собственности, а вовсе не вещь, являющаяся объектом этого права, как почему-то принято считать, и является объектом распоряжения собственника. Стало быть, выражения типа «собственник распоряжается вещью», «собственник продает вещь» безусловно неточны: ***собственник может распорядиться только правом на вещь, но не самой вещью***, ибо распоряжение – элемент правоспособности, – способность к совершению действия *с субъективнымм правами*, но не с их объектами (вещами). Они тем не менее допустимы, если правильно понимаются, а именно – в том смысле, что продажа *известной вещи* есть один из вариантов акта *распоряжения правом собственности* на вещь, а именно – акт прекращения права собственности продавца с одновременным его возникновением в лице покупателя (акт перенесения права собственности с продавца на покупателя), совершаемый за деньги.

Акт *распоряжения правом на вещь* – действие *юридическое* – легко спутать с актом *передачи вещи* – действием *фактическим*. Означает ли подобное действие – передача вещи из владения («из рук») одного лица во владение (в руки, в сферу господства или под контроль) другого лица – также совершение и действия по распоряжению правом на переданную вещь? Не обязательно: может быть и так, и этак – зависит от той цели, для достижения которой совершается передача вещи. И тем не менее обыденное воззрение неискушенных в юриспруденции лиц таково, что склонно не просто путать, но даже и отождествлять передачу владения вещью с распоряжением правом на вещь; больше того, и не одну только передачу – любую перемену владельца вещи. Как часто можно слышать заявления типа: «Я это нашел – теперь это мое!»; «У меня в руках находится – значит, мое!»; «Он все свои (!) деньги украл» и т.д. Что ими хотят сказать? Стал владельцем *вещи* – значит, стал и обладателем *права собственности на эту вещь*, ее собственником. Перемены *фактического* характера смешивают с *юридическими*.

Подобный подход конечно неправилен, но он по крайней мере объясним. Представление о субъективном праве собственности как возможности *юридической* весьма абстрактно и эфемерно в отличие от представления о *фактических* возможностях владельца вещи – более чем реальных и ощутимых. Естественно, что второе понятие в непрофессиональном сознании затмевает первое: обывателю куда понят-

нее выражение «купить (продать, получить, завещать, унаследовать и т.д.) ***дом***», чем «купить (продать, получить, завещать, унаследовать и т.д.) ***право собственности на дом***». Почему так происходит? Потому что речь идет о праве *собственности*, т.е. о праве на *вещь телесную*, т.е. на такой объект, который *является чем-то внешним по отношению к собственнику и имеет независимое от собственника существование*. В тех случаях, когда такого – материального, внешнего, независимо от лица существующего – объекта в природе не имеется, утрачивается и надобность в отделении *фактической* стороны ситуации от *юридической*. Неслучайно даже российский законодатель старается не говорить о распоряжении объектами исключительных или обязательственных прав – только *самими правами* на такие объекты. Никто не может купить литературное произведение, фонограмму, промышленный образец или вещь, являющиеся предметом требования, но можно купить *исключительное право* на произведение, фонограмму и промышленный образец, а также *право требования* вещи.

Почему эти в целом элементарные и хорошо известные положения так важны для целей настоящей статьи? Потому что *фактическая* ситуация способна развиваться самостоятельно и независимо от *юридической*, вне связи с ней и даже ей вопреки. Так, вещь может быть передана собственником в аренду или на хранение, утеряна им или украдена у него – в результате она окажется во владении совсем не того лица, кто является ее собственником – быть может, законного, а может быть, и незаконного ее владельца. Иными словами, фактическое развитие событий может быть как правомерным, так и противоправным[1]. В *юридическом* же мире дела могут идти *только правомерно* – иначе какой же он будет «юридический»? *Передача владения* может быть правомерной или неправомерной, но *распоряжение правом* (например, собственности) – *только правомерным*. Понятие о «неправомерном распоряжении» – нонсенс. Если акт распоряжения – это действие, имеющее «распорядительные» последствия (т.е. приводящее к перемене субъекта известного права, того, каким

[1] Осуществлять можно как свое, так и чужое *субъективное* право, причем то и другое делать как *правомерно*, так и *неправомерно*. Почему такое «раздвоение» становится возможным? Потому что субъективное право есть мера *фактического* поведения его обладателя – мера воздействия на вещи, объекты исключительных, личных, наследственных и прочих прав. Иначе с осуществлением прав *секундарных*, т.е. прав на *юридические* действия: такое осуществление по идее может быть только правомерным (как и действие по распоряжению правом). Бывает, однако, по-разному (см. далее).

распоряжались), то этот акт не может быть неправомерен, ибо если он неправомерен, то он... не может иметь намеченных им распорядительных последствий. Мы пришли к противоречию, подтверждающему верность нашего предположения: или «распоряжение», или «неправомерность», но не то и другое вместе. Если нечто есть ***распоряжение***, то оно может быть ***только правомерным***. С точки зрения логики иначе быть никак не может.

А с точки зрения практики – может, и еще как! *Относительные субъективные и секундарные гражданские права* есть субстанции чисто умозрительные (мыслимые), т.е. не имеющие существования самостоятельного и независимого от лиц, которыми они мыслятся, не представляющие собой чего-то внешнего и объективного по отношению к таким лицам. С точки зрения логики это означает, что *относительные субъективные и секундарные гражданские права могут быть предметом распоряжения только со стороны способных к этому лиц*. Но практика вот уже долгие годы неумолимо свидетельствует об ином: ***как минимум те относительные права, которые являются безналичными денежными средствами и бездокументарными ценными бумагами*** (как максимум – все те относительные права, которые фиксируются (учитываются) на счетах)***, могут стать и действительно становятся предметом юридически результативных актов распоряжения, совершаемых лицами, к их совершению не способными***.

Почему так получилось – объяснить легко: стремясь к защите добросовестных участников оборота, *человечество организовало обращение некоторых умозрительных* (*идеальных*) *ценностей по тем же правилам, по которым осуществляется обращение ценностей реальных* (*вещей*), т.е. по правилам, допускающим раздельное существование и внутренне противоречивое развитие фактической и юридической сторон одной и той же ситуации. Нет, говорите, той реальной ценности, которая могла бы быть объектом фактических отношений? – не беда! Давайте ее создадим. Сначала ею стали ***самые настоящие телесные вещи – документы***, в частности бумажные деньги и ценные бумаги, а через некоторое время роль такой – вроде бы независимой от участников оборота, самостоятельной – ценностью стали... идеальные понятия, т.е. ***счета*** (банковские, реестровые и депо). Вопрос о *господстве над* ***счетом по учету прав*** стал самостоятельным, чисто внешне никак не связанным с вопросом о *господстве над* ***правами, числящимися на счете***: первое стало аналогом *фактического господства над вещью*, второе – так и осталось господством *юридическим*, т.е. господством *над правом*.

В итоге мы имеем, например, *иски о взыскании безналичных денежных средств*: на счете должника они просто числятся, находятся, должник господствует над ними, но чисто внешним образом, подобно тому, как над предметом поклажи господствует хранитель, а над грузом – перевозчик. В действительности же эти денежные средства – способность распорядиться их определенной суммой (требованиями на эту сумму) принадлежат – совсем другому лицу (кредитору)[1]. Или же мы имеем *иски о восстановлении корпоративного контроля* – иски, предполагающие признание того прелюбопытного с логической точки зрения факта, что некое количество спорных акций принадлежит ответчику лишь «формально», т.е. «просто числится» на его счете в реестре акционеров (подобно тому, как похищенная вещь находится во владении вора); «на самом же деле» (!) «строго юридически» они принадлежат совсем другому субъекту (истцу).

И вот та точка, в которой наши рассуждения, на первый взгляд не имеющие никакого отношения к тематике настоящей статьи, наконец, с нею связываются. Круг ценностей информационной природы не ограничивается одними только объектами авторских, смежных, патентных, личных и обязательственных прав. Интернет – среда, приспособленная для существования и таких объектов, как *систематизированные записи о требованиях и иных относительных правах*, т.е. ***счета безналичных (электронных!) денежных средств*** и ***бездокументарных (цифровых!) ценных бумаг***; и таких (доселе неизвестных) ценностей, которые теперь объединяют общим наименованием ***виртуального имущества (цифровых активов)***. Сюда попадают, помимо записей по «денежным» и «ценно-бумажным» счетам, также (а) автоматически сформированные записи об электронных деньгах, «привязанных» для целей распоряжения к определенному пользователю; (б) интернет-сайты, в особенности – предназначенные для оказания известных услуг пользователям сети (в том числе интернет-магазины, платежные системы, электронные библиотеки, аудио- и видеотеки, виртуальные кинотеатры, сайты с программным обеспечением, играми и пр.); (в) *web*-страницы, профили и аккаунты (учетные записи) в социальных сетях, форумах и конференциях, мессенджерах, чатах, сетевых играх, платежных системах и т.п.; (г) блоги и записи в блогах, «Живые журналы», электронные

[1] В обыденной жизни скажут проще: на счете должника Д. числятся средства кредитора К.

дневники и т.п.; (д) используемые в цифровой среде специальные средства индивидуализации (электронные (*IP*) адреса, доменные имена, ник, цифровой персонаж, иконка, аватар (англ. *avatar*), ЭЦП, логины, пароли, ключи и коды активации и др.); (е) возможности и преимущества, «купленные» за деньги, «заработанные» путем совершения определенных онлайн-действий, выигранные в сетевых играх или приобретенные иначе (различного рода *скидки, баллы и бонусы*, количество «лайков», виртуальных друзей и т.п.).

Ко всему этому сетевому великолепию может быть поставлен только один юридический вопрос: ***объектами каких прав являются подобные (электронные, цифровые, виртуальные) объекты?*** Конкретно: *который из двух известных праву подходов будет избран для оформления состояния принадлежности* (*присвоенности*) *всех перечисленных* (да и любых других, появляющихся с пугающей регулярностью) *виртуальных ценностей*, а также *перехода* – как сингулярного (в порядке отчуждения), так и универсального (например, по наследованию) – *прав на подобные объекты*? Ограничится ли частное право подходом чисто юридическим (т.е. сконструирует специфические абсолютные права на подобные объекты, этакие ***цифровые*** или ***виртуальные частные права*** (*digital or virtually private rights*)) или же попытается произвести очередное удвоение реальности, признав наряду с пресловутыми *digital private rights* на подобные объекты еще и сами эти объекты некими особыми (мыслимыми, умозрительными, но все же имеющими самостоятельное бытие) субстанциями, т.е. отведя им роль, аналогичную той, которую в реальном мире выполняют вещи – предметы *фактического* (а в данном случае *технического*) господства? Учитывая то, что техническое господство над цифровыми объектами – штука куда более конкретная и реальная, чем трудно объяснимый гражданину, не испорченному юридическим образованием, статус «владельца банковского счета» (счета депо или счета в реестре), представляется весьма вероятным, что *digital private law* двинется как раз по второму – уже проторенному «аналоговой» цивилистикой пути.

Если дело станет развиваться именно так, то и в Интернете мы будем иметь ситуации, в которых вопрос ***о самом субъективном праве с материальной точки зрения*** (о принадлежности субъективного права) станет решаться одним способом (например, по общим нормам ГК РФ о приобретении и прекращении прав, о сделках, договорах, наследовании и т.д.), а вопрос ***о фактическом осуществлении такого права*** – совсем другим – чисто техническим. Принадлежит право *одно-*

му лицу (тому, кто его приобрел), а осуществляет его *другое* лицо (тот, кто имеет доступ к логину, паролю, ключу, ЭЦП и т.п.)[1]. Во что это может вылиться в цифровой среде – сказать пока сложно; очевидно лишь то, что и в этой сфере Интернет не добавляет оптимизма. В том смысле, что его развитие если и позволит в течение какого-то времени сохранять те представления об абсолютных (в том числе вещных) правах, к которым человечество привыкло в последние несколько сотен лет, то пока нет уверенности в том, что это будет хорошо и правильно[2]. И не было бы лучше, если бы как раз в этой сфере Интернет все-таки что-то поменял, например, приблизив *юридическую* мысль к *математической* (формальной, машинной) *логике*. В конце концов, существует уже столько цифровых (виртуальных) ценностей – почему бы не прибавить к ним и такие, как ***цифровое частное право в объективном смысле*** и ***цифровые субъективные частные права – digital private law & digital private rights***?

Пристатейный библиографический список:

1. *Азаров М.С.* Правовой институт доменных имен в развитии информационного пространства России. М., 2010.

2. *Бабкин С.А.* Интеллектуальная собственность в Интернет. М., 2006.

3. *Бабкин С.А.* Право, применимое к отношениям, возникающим при использовании сети «Интернет»: основные проблемы. М., 2003.

4. *Вацковский Ю Ф.* Доменные споры. Защита товарных знаков и фирменных наименований. М., 2009.

5. *Войниканис Е.А.* Право интеллектуальной собственности в цифровую эпоху: парадигма баланса и гибкости. М., 2013.

[1] Это означает, кстати, что теоретическое учение о классических (документарных) ценных бумагах получит «второе дыхание» и новую сферу приложения. Ведь его краеугольным камнем как раз и является постулат о точном отделении вопроса о *принадлежности* ценных бумаг и удостоверяемых ими прав от вопроса об их *осуществлении*: ценные бумаги (а вместе с ними и удостоверяемые ими права) *приобретаются и отчуждаются* по общим нормам о правах на движимые вещи, в то время как *осуществляются* они формально легитимированными предъявителями бумаг.

[2] Интересно, кстати, не понадобится ли трансформировать в связи с этим еще и понятие о юридических фактах? Не добавятся ли в него к традиционным «*фактам реальной действительности*» также и «факты», имевшие место в рамках... *технической* (*виртуальной*) *реальности*?

6. *Войниканис Е.А., Якушев М. В.* Информация. Собственность. Интернет: традиция и новеллы в современном праве. М., 2004.

7. *Герцева Е.Н., Гринкевич А.П.* Доменные споры. Судебная практика в России. М., 2014.

8. *Даниленков А.В.* Интернет-право. М., 2014.

9. *Дмитрик Н.А.* Осуществление субъективных гражданских прав с использованием сети Интернет. М., 2006.

10. *Дремлюга Р.И.* Интернет-преступность. Владивосток, 2008.

11. *Комаров А.А.* Интернет-мошенничество: проблемы детерминации и предупреждения. М., 2013.

12. Компьютер и Интернет в нотариальной практике: практ. пособие / отв. ред. Й. Беттендорф; пер. с нем.; предисл. В.В. Яркова. М., 2005.

13. *Корупаев А.Е.* Права человека в Интернете, киберпространстве и компания Google. М., 2011.

14. *Кудашкин Я.В.* Административно-правовое регулирование отношений в сети Интернет в РФ. Саранск, 2012.

15. *Лебедева Н.Н.* Право. Личность. Интернет. М., 2004.

16. *Луцкер А.П.* Авторское право в цифровых технологиях и СМИ. М., 2005.

17. *Минков А. М.* Рассмотрение споров о доменных именах в соответствии с процедурой UDRP. М., 2004.

18. *Миронова С.Н.* Использование возможностей сети Интернет при разрешении гражданско-правовых споров. М., 2010.

19. *Наумов В.Б.* Право и Интернет: очерки теории и практики. М., 2002.

20. *Незнамов А.В.* Особенности компетенции по рассмотрению Интернет-споров. М., 2011.

21. *Петровский С.В.* Интернет-услуги в российском праве. М., 2003.

22. Правовые аспекты использования Интернет-технологий / под ред. Д.В. Головерова, А.С. Кемрадж. М., 2002.

23. *Рассолов И.М.* Право и Интернет: теоретические проблемы. М., 2009.

24. *Рассолов И.М.* Интернет-право: учеб. пособие. М., 2012.

25. *Савельев А.И.* Договорное право 2.0: «умные» контракты как начало конца классического договорного права // Вестник гражданского права. 2016. № 3.

26. *Салиев И.Р.* Гражданско-правовое регулирование электронной торговли в сети Интернет. Тюмень, 2011.

27. *Сальникова Л.В.* Сделки в Интернет. Советует юрист. Ростов н/Д, 2006.

28. *Серго А.Г.* Доменные имена. М., 2006/2013.

29. *Серго А.Г.* Доменные имена в свете нового законодательства. М., 2010.

30. *Серго А.Г.* Интернет и право. М., 2003.

31. *Середа М.Ю., Середа В.Н.* Защита прав и свобод человека и гражданина в сети Интернет. Воронеж, 2013.

32. *Тедеев А.А.* Информационное право (право Интернета): учеб. пособие. М., 2005.

33. Телекоммуникационное законодательство: сб. / сост. Ю.В. Волков. Екатеринбург, 2006.

34. Трансформация авторского права в Интернете: зарубежные тенденции, бизнес-модели, рекомендации для России / под ред. И. Засурского, В. Харитонова. М., 2013.

35. *Чеботарева А.А.* Средства массовой информации в сети Интернет: проблемы юридической ответственности. Чита, 2009.

Е.А. Останина

ОСНОВАНИЕ ПРИСОЕДИНЕНИЯ К МНОГОПОЛЬЗОВАТЕЛЬСКОЙ ОНЛАЙН ИГРЕ – ДОГОВОР С УЧАСТИЕМ ПОТРЕБИТЕЛЕЙ

Аннотация. *Договоры по поводу массовых многопользовательских онлайн-игр характеризуются в качестве договоров присоединения. Отстаивается вывод, что участник игры является потребителем. Рассмотрена практика защиты потребителя, участвующего в многопользовательской онлайн-игре, сформированная в США, в Германии и в России.*

Ключевые слова: *многопользовательская онлайн-игра, потребитель, договор присоединения.*

Нет большей лжи, чем слова «Я прочитал условия лицензионного соглашения и согласен с ними». Большинство пользователей Интернета подписывают лицензионные договоры, не читая их.

Договоры между разработчиками и администраторами онлайн-игр (таких, как *World of Warcraft*, *World of Tanks* или *Second Life*) – с одной стороны и игроками, участниками таких игр, – с другой – тоже разработаны как договоры присоединения. Но эти договоры подвержены риску применения ст. 1062 ГК РФ.

Сложившаяся практика применения ст. 1062 ГК РФ к спорам между участниками онлайн-игр, а равно к спорам между организаторами таких игр и их участниками справедливо критикуется в цивилистической литературе, но, к сожалению, продолжается.

Влечет ли присоединение к онлайн-игре возникновение обязательства, распространяются ли на отношения между организатором игры и игроком нормы о договоре присоединения, является ли игрок экономически слабой стороной обязательства, нуждается ли он в повышенной защите и располагает ли он защитой – ответам на эти вопросы посвящена данная статья.

Прежде всего стоит оговорить этическую подоплеку проблемы. Во многих странах споры из-за массовых многопользовательских онлайн-игр (далее – *MMOG*) первоначально не рассматривались судами

по существу именно потому, что эти игры воспринимали как нечто заведомо ненужное и несерьезное.

Однако с развитием этого вида деятельности, по мере вовлечения в нее все большего количества людей и все больших денежных сумм отношение изменилось.

Теперь в литературе США, Южной Кореи и Китая отмечается, что оставить отношения из *MMOG* без регулирования означает выпустить джинна из бутылки: худшие стороны *MMOG* будут развиваться, лучшие останутся без поощрения[1].

В отечественной судебной практике наблюдается определенный «двойной стандарт» по отношению к *MMOG*. Когда речь идет об ответственности разработчиков за неуплату налогов, отношения разработчика *MMOG* с игроками характеризуют как отношения из смешанного договора, включающего в себя элементы лицензионного договора и договора возмездного оказания услуг.

Если же речь идет об отношениях между разработчиком игры и игроком, характеристика договора как смешанного, включающего в себя элементы договора возмездного оказания услуг, забывается и на первый план выводится понятие «игра».

Например, по одному из налоговых дел компания оспаривала доначисление ей налога, полагая, что заключает с гражданами лицензионные договоры. Суд, установив, что компания является разработчиком и администратором онлайн-игры, сделал вывод, что между компанией и гражданами заключен смешанный договор, включающий в себя элементы лицензионного договора и договора возмездного оказания услуг по организации игрового процесса. Поскольку услуги облагаются НДС, налог доначислен правильно[2].

Таким образом, в этом налоговом деле суд квалифицировал деятельность по организации *MMOG* как услугу.

По другому налоговому делу суд также пришел к выводу, что лицензионные соглашения о предоставлении доступа к многопользова-

[1] Yoon. Ung-gi, Real Money Trading in MMORPG Items From a Legal and Policy Perspective (December 13, 2004) // Journal of Korean Judicature. 2008 Vol. 1. P. 418–477. Available at SSRN: https://ssrn.com/abstract=1113327 or http://dx.doi.org/10.2139/ssrn.1113327; Methenitis, Mark, Internet Gambling Regulation Present and Future: Technology Outpaces Legislation as the MMORPG Problem Emerges (December 2005). Available at SSRN: https://ssrn.com/abstract=987056 or http://dx.doi.org/10.2139/ssrn.987056

[2] Постановление АС Московского округа от 18.06.2015 № Ф05-7093/2015 по делу № А40-91072/14.

тельской онлайн-игре содержат в себе положения как лицензионного договора, так и договора об оказании услуг[1].

Такой же подход используется в иных судебных актах по подобным налоговым спорам[2].

Совершенно иной подход используется в спорах из гражданских отношений.

Казалось бы, целесообразно признать и здесь организатора многопользовательской онлайн игры исполнителем по договору возмездного оказания услуг, а игрока – заказчиком. Но сам термин «игра» неуклонно приводит суды к выводу, что обеспеченное судебной защитой гражданско-правовое обязательство отсутствует, а гражданин не является потребителем.

По одному из дел участник *MMOG* обратился в суд с заявлением о взыскании неустойки вследствие неудовлетворения требований потребителя в связи с тем, что его игровой аккаунт был незаконно заблокирован разработчиком и администратором игры. Мировой суд применил к спору Закон РФ от 07.02.1992 № 2300-I (ред. от 03.07.2016) «О защите прав потребителей» (далее – Закон о защите прав потребителей), однако суд апелляционной инстанции это решение отменил, подчеркнув, что блокировка аккаунта была вызвана нарушением правил игры. Вопрос о том, нарушены ли правила игры, не подлежит рассмотрению в силу ст. 1062 ГК РФ, поэтому истец не только не имеет статуса потребителя, но и не располагает судебной защитой[3].

В другом споре между организатором *MMOG* и участником-игроком речь шла о незаконном, по мнению истца, действии по блокировке игрового аккаунта.

Из обстоятельств дела следовало, что пользователь заключил с ответчиком пользовательское соглашение. Правила игры определены приложением к этому соглашению. Поскольку блокировка аккаунта, по объяснениям ответчика, связана с нарушением истцом правил игры, суд сделал вывод о том, что «наличие либо отсутствие в действиях пользователя нарушений правил игры относятся к организации игрового

[1] Постановление АС Московского округа от 12.10.2015 № Ф05-13554/2015 по делу № А40-56211/14.

[2] Постановление АС Московского округа от 18.06.2015 № Ф05-7093/2015 по делу №А40-91072/14.

[3] Постановление Президиума Московского городского суда от 24.05.2013 по делу № 44г-45.

процесса, в связи с чем требования истца, связанные с участием в игре, в силу п. 1 ст. 1062 ГК РФ не подлежат судебной защите»[1].

За основанными на ст. 1062 ГК РФ решениями кроется молчаливая уверенность в том, что компьютерные игры вообще и многопользовательские онлайн игры в частности, как минимум – бесполезны, как максимум – вредны.

Между тем такая точка зрения не бесспорна. В литературе отмечаются и опасные, и полезные свойства *MMOG*.

Предельно обобщая все многообразие социологических и психологических изысканий по этому поводу[2], можно сказать, что опасность *MMOG* состоит в возможности привыкания и возникновения своеобразной зависимости. Полезное свойство *MMOG* состоит в приобретении нового опыта, усвоении навыков планирования, командной игры и общения[3].

С учетом соотношения позитивных и негативных сторон этого относительно нового общественного явления сложно не согласиться с тем, что отношения по поводу *MMOG* нуждаются в регулировании.

Что это за игры?

История многопользовательских игр берет начало в эпоху до возникновения Интернета. Предтечами *MMOG* можно считать настольные ролевые игры – с одной стороны и полевые ролевые игры – с другой.

Развитие стратегической мысли в военной практике неизбежно формировало различные формальные модели военных операций. До начала XX в. такие модели не были достоянием широкой публики, если не считать шахмат, но благодаря работам Герберта Уэллса идея была популяризована, а в книгах Гарри Гигакса и Джеффри Перрена в 1969 г. приняла современную форму фантастической настольной

[1] Определение Московского городского суда от 06.10.2011 по делу № 4г/1-8422.

[2] В частности: *Семенов Н.Б.* Виртуальные игровые практики в контексте преемственности и инноваций в культуре: автореф. дис. ... канд. социол. наук. Саратов, 2012; *Рыбалтович Д.Г.* Психологические особенности пользователей онлайн игр с различной степенью игровой аддикции: автореф. дис. ... канд. психолог. наук. СПб., 2012; *Антоненко А.А.* Интернет-зависимость подростков от компьютерных игр и онлайн-общения: клинико-психологические особенности и профилактика: автореф. дис. ... канд. психолог. наук. М., 2014; *Медведев Е.А.* Виртуальный мир как фактор социализации // Молодежь и общество на рубеже веков: тезисы и материалы конференции. М., 1998.

[3] *Медведев Е.А.* Субкультура участников ролевых игр и методы исследования ее воздействия на личност: автореф. дис. ... канд. социол. наук. М., 2004. С. 15.

ролевой игры. В настоящий момент, по данным «Индекса Ролевых Игр» (*The RPG Index*) количество когда-либо выпущенных книг по настольным ролевым играм составляет 13 030 названий, объединенных в 1473 собственно игр, и их количество постоянно растет[1].

Параллельно настольным, переплетаясь с ними, развивались игры полевые. В России история полевых игр имеет непосредственное отношение к регулярным праздникам на Бородинском поле, проходящим с 1987 г. Одним из основных событий этого праздника является театральная реконструкция Бородинского сражения. Позже военно-исторические клубы, десятками возникшие по всей стране, начали обращаться к другим темам, в том числе к фантастическим[2].

Предшественниками сетевых ролевых игр можно считать так называемые текстовые приключенческие игры, в которых игрок управляет представляющим его в игровом мире персонажем, отдавая письменные команды на естественном языке, используя клавиатурный ввод и получая ответы в виде художественного текста, описывающего игровой мир и произошедшие в нем изменения.

Все известные сетевые ролевые игры наследуют те или иные технические решения и концепции этого класса компьютерных игр, а сами они основаны на идеях, впервые разработанных в настольных ролевых играх.

Развитие технологии компьютерной графики вызвало к жизни графические стратегически-ролевые игры, созданные на основе идей, разработанных в настольных ролевых играх, и концепций, родившихся в традиционных однопользовательских играх, – например, такие известные сетевые игры, как *Ultima Online*, *Everquest*, ставшие необычайно популярными[3].

Возникновение жанра массовых многопользовательских онлайн-игр в его законченном, оформленном виде исследователи связывают с выпуском онлайн игры *Ultima Online* 30 сентября 1997 г.[4] Так или иначе именно *Ultima Online* прославила жанр.

MMOG представляют собой своеобразные виртуальные миры, где люди могут взаимодействовать друг с другом, в этих мирах имеют-

[1] *Медведев Е.А.* Субкультура участников ролевых игр и методы исследования ее воздействия на личност: автореф. дис. ... канд. социол. наук. М., 2004. С. 10.

[2] Там же.

[3] Там же. С. 11.

[4] См.: *Methenitis Mark*, Internet Gambling Regulation Present and Future: Technology Outpaces Legislation as the MMORPG Problem Emerges (December 2005). Available at SSRN: https://ssrn.com/abstract=987056 or http://dx.doi.org/10.2139/ssrn.987056

ся элементы (квесты, события), которые служат движению игрового сюжета и развитию создаваемых пользователями виртуальных персонажей. Теоретически эти онлайн-миры так же безграничны, как и реальный мир, практически же – они ограничены техническими возможностями разработчиков.

Эти игры часто имеют сиквелы, в которых многие элементы основной игры принимаются за исходное и улучшаются. Часто имеют место и сугубо технологические улучшения, например более совершенная графика[1].

MMOG начинается с сервера, который представляет собой мощный компьютер, подключенный к сети Интернет; это соединение требует намного больше траффика, чем любое домашнее подключение. На сервере содержится большая часть информации, касающейся игрового мира. Большинство игр имеют несколько серверов, часто в разных местах и в разных странах. Другая часть системы – игроки, чьи персональные компьютеры подключены к Интернету; лицензионное программное обеспечение позволяет игрокам взаимодействовать друг с другом и с сервером. Игроки оплачивают лицензии; оплата покрывает расходы, необходимые для содержания сервера[2].

Второй элемент системы – это персонажи, которые подразделяются на игровых и неигровых. Неигровые персонажи (часто в их роли выступают всевозможные владельцы оружейных магазинов и вестники, доставляющие задание) не подконтрольны ни одному из игроков. Игровые персонажи управляются игроком, собственно – это и есть «воплощение» игрока в данном онлайн-пространстве. Правила многих игр позволяют одному игроку управлять несколькими персонажами.

И третьим компонентом игры является имущество. В большинстве игр используются виртуальные аналоги движимых вещей и иного имущества, такие как внутриигровая валюта, оружие, техника, предметы экипировки и т.п.

Деньги в игровом мире работают так же, как деньги в реальном мире. Оборудование приобретается и продается. Особыми разновидностями предметов считаются предметы, позволяющие восстановить или приобрести дополнительные возможности и характеристики (будь

[1] *Methenitis Mark*. Internet Gambling Regulation Present and Future: Technology Outpaces Legislation as the MMORPG Problem Emerges (December 2005).

[2] Там же.

то какой-нибудь «волшебный эликсир» или «улучшенная система вентиляции моторного отсека»). Эти предметы, как правило, принимают форму продуктов питания, оборудования или лекарств[1].

В некоторых играх используется и такое имущество, которое по правилам игрового мира ассоциируется с недвижимостью. В некоторых играх можно купить «замок», «летающий остров» и даже «орбитальную судоверфь».

Конечно, у игроков нет права собственности на это имущество, потому что его не существует в реальном мире, но многие термины, характерные для владения и собственности, здесь все же используются[2].

Четвертый элемент этих игр – это различного рода столкновения игроков как с искусственными соперниками, так и друг с другом, будь то виртуальная дуэль на холодном оружии, виртуальная перестрелка на поле боя или партия за виртуальным карточным столом. Победа в таких столкновениях является, наверное, первоочередной задачей в любой из этих игр. Каждая игра имеет какой-то конфликт, который приводит в движение всю сюжетную линию, и этот конфликт всегда предполагает борьбу. Борьба является основным способом продвижения как в плане сюжета, так и в плане расширения внутриигровых возможностей.

В каждой игре разработаны свои символы, обозначающие этот процесс. Например, после того как противник побежден, игрок получает определенное количество очков опыта, часто сокращаемых как *EXP* (от англ. *Experience*). После того, как приобретено достаточно *EXP*, уровень персонажа увеличивается и становятся доступными новые возможности. Именно потому что это основной способ получения новых возможностей, игроки и проводят часы в борьбе друг с другом и искусственными противниками[3]. В каком-то смысле это имитация процесса борьбы и получения опыта, объективно недоступного в реальной жизни.

Другим результатом победы может быть то, что победитель по правилам игры получает деньги или предметы. Хотя, конечно, не совсем реалистично, что гигантский паук будет носить с собой кошелек, но в этой

[1] *Methenitis Mar.* Internet Gambling Regulation Present and Future: Technology Outpaces Legislation as the MMORPG Problem Emerges (December 2005). Available at SSRN: https://ssrn.com/abstract=987056 or http://dx.doi.org/10.2139/ssrn.987056.

[2] *Methenitis Mark*. Internet Gambling Regulation Present and Future: Technology Outpaces Legislation as the MMORPG Problem Emerges (December 2005).

[3] Ibidem.

отрасли приняты такие условности. Поэтому, для того чтобы прогрессировать, бой неизбежен (впрочем, порой разработчики некоторых игр в целях их популяризации проводят турниры, предполагающие вполне реальное и довольно существенное вознаграждение, однако это явление, именуемое «киберспорт», следует рассматривать отдельно).

Последним элементом является социальное взаимодействие, которое можно разделить на боевое взаимодействие и небоевое взаимодействие. Боевое взаимодействие – это либо столкновение игроков, либо, наоборот, взаимодействие игроков для победы над противником.

Небоевые взаимодействия могут принимать различные формы; игроки могут просто болтать о разных далеких от игры вопросах. Тем не менее для дальнейшего нашего анализа будет иметь принципиальное значение именно боевое взаимодействие, а именно тот его аспект, что игроки взаимодействуют, чтобы выиграть.

Кто в них играет?

Круг людей, вовлеченных в онлайн-игры, непрерывно расширяется. В первые годы малой доступности Интернета этот круг был искусственно сужен, но по мере того, как Интернет становится все более скоростным и все более доступным, популярность онлайн-игр все более возрастает. На пике своей популярности (в июле 2003 г.) *Ultima Online* насчитывала 250 тыс. абонентов, но и другие игры доказали, что 250 тыс. пользователей является сравнительно небольшим числом. Количество пользователей игры *Everquest* достигло приблизительно 450 тыс. Мир *Warcraft* доказал, что количество пользователей может быть еще больше. За один год эта игра приобрела более чем 4,5 млн пользователей. Тенденция состоит в том, что по мере появления все более совершенных компьютеров популярность *MMOG* все более возрастает[1].

Массовая пресса традиционно видит в участниках *MMOG* в основном несовершеннолетних. Между тем возраст опрошенных отнюдь этому предположению не соответствует[2].

Состав игроков столь же разнообразен, как население мира. В эти игры играют люди от среднего школьного до пенсионного возраста; студенты, менеджеры, врачи, юристы и военные. Единственное ог-

[1] *Methenitis Mark*. Internet Gambling Regulation Present and Future: Technology Outpaces Legislation as the MMORPG Problem Emerges (December 2005).

[2] *Медведев Е.А.* Субкультура участников ролевых игр и методы исследования ее воздействия на личность: автореф. дис. ... канд. социол. наук. С. 19.

раничение – у игрока должен быть компьютер, подключенный к Интернету[1].

Неподтвержденная официально статистика состоит в следующем. Средний возраст игрока – 25–26 лет, но 25% игроков – подростки. Примерно 50% игроков заняты полный рабочий день, более одной трети состоят в браке и почти четверть игроков – дети[2]. Женщины чуть меньше вовлечены в *MMOG*, чем мужчины, именно поэтому сегодня одной их актуальных задач для разработчиков *MMOG* являются игры, ориентированные на женскую аудиторию. То же касается и людей старшего возраста – в литературе отмечается, что эта целевая группа представляется перспективной для разработки новых вариантов игр[3].

В среднем 69% из опрошенных отечественными социологами респондентов отмечали, что они играют (или играли) на платных серверах, 72,5% опрошенных респондентов тратили реальные деньги (а не игровую валюту) в онлайн-игре на «прокачку» своего персонажа, дополнительные квесты[4].

Как это регулируется (анализ законодательства и судебной практики de lege lata)

Наиболее общий вопрос, который возникает в связи с правовым регулированием отношений по поводу *MMOG*, – это вопрос о подсудности и подведомственности возникающих из *MMOG* споров.

«Интернет стирает границы». Разработчик онлайн игры может находиться в одном государстве, владелец сервера – в другом, а игрок – в третьем. Какое же законодательство применятся при возникновении спора?

Этот вопрос не раз возникал при рассмотрении дел. Можно привести в качестве примера дело *Bragg v. Linden Research*, *Inc.*, рассмотренное в 2007 г. в Пенсильвании, и дело *Blizzard Entertaiment*, рассмотренное в Берлине, Германия, 2014 г.

---

[1] *Methenitis Mark*. Internet Gambling Regulation Present and Future: Technology Outpaces Legislation as the MMORPG Problem Emerges (December 2005). Available at SSRN: https://ssrn.com/abstract=987056 or http://dx.doi.org/10.2139/ssrn.987056).

[2] *Methenitis Mark*. Internet Gambling Regulation Present and Future: Technology Outpaces Legislation as the MMORPG Problem Emerges (December 2005).

[3] *Wiemeyer Josef*. Digital Spiele.K(ein) Themafür die Sportwissensvhaft? // Sportwiss (2009). 2009. Vol. 39, Issue 2. P. 120–128.39:120. Doi:10.1007/s12662-009-0034-2.

[4] *Рыбалтович Д.Г.* Указ. соч. С. 7.

В первом из дел один из ответчиков, выполняющий функции администратора *MMOG*, заявлял о том, что дело неподсудно суду штата Пенсильвания, поскольку он, ответчик, в этом штате не проживает. Суд не поддержал этот довод.

Во втором – речь шла о противоречии отдельных условий договора об *MMOG* гражданскому законодательству. Суд признал эти условия недействительными, но с любопытной оговоркой: запретить применять признанные недействительными условия к отношениям с участнием граждан, имеющих постоянное место жительства в Германии.

К числу более узких, но тоже, несомненно, важных вопросов относятся вопросы о том, насколько применимо к отношениям между организатором *MMOG* законодательство о защите прав потребителей, является ли такой договор договором присоединения. Здесь видятся полезными также два знаковых дела: дело *Bragg v. Linden Research, Inc*., 2007 г., США, Пенсильвания и дело *Blizzard Entertaiment*, 2014 г. Берлин, Германия. Рассмотрим их подробнее.

1. Дело *Braggv. Linden Research, Inc*., 2007, Пенсильвания[1]

В октябре 2006 г. Марк Брэгг подал в суд, чтобы взыскать стоимость земли, средств производства и продукции, а также личных вещей, которые были (по его утверждению) незаконно конфискованы ответчиком.

Истец представил веские доказательства, что имущество имелось у него до момента изъятия. Особенность дела состояла в том, что это имущество не было реальным.

Все это имущество было приобретено истцом в игре *Second Life*, популярной в США *MMOG*. Соответчиками была компания-разработчик и гражданин, выполняющий функции администратора игры.

Истец (Брэгг) играл в *Second Life* с 2005 г. В апреле 2006 г. Брэгг приобрел виртуальный «земельный участок» на аукционе, который проводился в рамках игры, но не соответствовал ее, игры, правилам. Кстати, приобрел он виртуальный земельный участок за 300 долл., что было примерно в 5 раз дешевле обычной цены.

По заявлению ответчика истец знал или должен был знать, что аукцион проводится с нарушениями.

Ответчик посчитал приобретение нарушениями правил игры и заблокировал аккаунт истца. Истец тем самым потерял возможность пользоваться всеми игровыми возможностями, за которые ранее были

[1] *Dougherty, Candidus, Bragg v. Linden*: Virtual Property Rights Litigation. E-Commerce Law & Policy, Vol. 9, No. 7, July 2007. Available at SSRN: https://ssrn.com/abstract=1092284

уплачены реальные деньги. Стороны разошлись в оценке сумм, вложенных в заблокированный аккаунт. Истец насчитал 8000 долл., ответчик – 590280.

При рассмотрении дела были проанализированы условия предоставления услуг. Установлено, что заключенный истцом и ответчиком (разработчиком игры) договор являлся договором присоединения – *click wrap agreement*.

Условия этого договора были изложены истцом. Ответчик присоединился к этому договору, кликнув мышью в установленной части диалогового окна. Суд особенно подчеркнул, что «встречного выражения воли» в этом договоре не было, условия были предложены игроку по принципу «принимай все или отказывайся» (*take it or leave it*).

Вместе с тем, несмотря на то что условия *click wrap* соглашений формулируются только одной стороной, они действительны, если другая сторона получила достаточные сведения об условиях соглашения и явно выразила намерение принять их. В этом деле договор присоединения был признан действительным в целом; но в договоре имелось условие о том, что все споры из данного договора должны быть рассмотрены в третейском суде; и это условие суд признал недействительным. По мнению суда, формулируя условия договора присоединения, ответчик слишком сильно нарушил разумный экономический баланс интересов сторон.

Суд привел несколько доводов, объясняя, почему считает третейскую оговорку недобросовестной и недействительной (а) как следует из обстоятельств дела, истец был лишен возможности обсуждать это условие, поскольку находился в неравных переговорных возможностях с ответчиком; (б) из обстоятельств дела следует, что разбирательство в третейском суде потребовало бы от истца куда больших расходов, чем предъявление иска по общим правилам гражданского судопроизводства. Поэтому право истца на справедливое рассмотрение дела было бы ограничено.

Дело разбиралось государственным (а не третейским) судом и закончилось мировым соглашением, по условиям которого ответчик уплатил истцу определенную сумму[1].

[1] См.: 487 F. Supp.2d 593 (2007) Marc BRAGG, Plaintiff, v. LINDEN RESEARCH, INC. and Philip Rosedale, Defendants. No. CIV.A.06 4925. United States District Court, E.D. Pennsylvania (https://h2o.law.harvard.edu/cases/4435).

May 30, 2007. Bragg v. Linden Lab (https://en.wikipedia.org/wiki/Bragg_v._Linden_Lab; Memorandum (http://www.paed.uscourts.gov/documents/opinions/07D0658P.pdf).

2. Дело *Blizzard Entertainment*, Берлин, Германия, 2014 г.

В январе 2014 г. Берлинский суд (*LandgerichtBerlin*) постановил, что некоторые условия типовых договоров компании *Blizzard Entertaiment* об использовании продукта *World of Warcraft* недействительны, поскольку нарушают права потребителя.

Объединение потребителей (*Verbraucherzentrale Bundesverbandt*) предъявило иск компании *Blizzard Entertaiment*, требуя запретить ответчику включать в договор условия, нарушающие права потребителей.

Иск был удовлетворен. Под угрозой выплаты штрафа в сумме 2500 тыс. евро ответчику было предписано не включать в договоры с потребителями, имеющими обычное место жительства в Федеративной Республике Германия[1], а в случаях, когда такие договоры заключены ранее, то не применять следующие условия:

(1) «Компания *Blizzard Entertainment* оставляет за собой право, по своему усмотрению, прекратить Ваш доступ к обслуживанию или удалить учетную запись, если Ваши заказы не могут быть оплачены посредством указанной Вами кредитной карты».

(2) акцептуя настоящее соглашение, Вы соглашаетесь с тем, чтобы возместить компании *Blizzard Entertainment* все расходы и издержки, связанные с обслуживанием Вашего игрового аккаунта, включая судебные сборы и оплаты банковских операций;

(3) *Blizzard Entertainment* оставляет за собой право изменять все содержащиеся в настоящем соглашении условия в любое время и по своему собственному усмотрению. В целях совершенствования игрового опыта, а также в целях защиты от мошенников компания *Blizzard Entertainment* оставляет за собой право менять методы доступа, функции, время выделения ресурсов. Компания имеет право изменять требования к программному обеспечению или оборудованию, необходимым для использования *World of Warcraft*. Компания имеет право также в одностороннем порядке менять плату за *World of Warcraft* или основы ее определения;

(4) Компания *Blizzard Entertainment* обязана уведомить пользователя о таких изменениях, и может, по своему усмотрению, выбрать способ уведомления: почтой, электронной почтой или посредством всплывающих уведомлений.

[1] http://www.damm-legal.de/lg-saarbruecken-gratis-onlinespiel-mit-kostenpflichtigen-ueber-die-telefonrechnung-abgerechneten-zusatzfeatures-verstost-gegen-die-guten-sitten-1-38-bgb-wenn-altersverifikation-fehlt/

Любое дальнейшее использование *World of Warcraft* в течение одного месяца после уведомления считается согласием пользователя с изменением договора»[1].

В основание судебного решения положены нормы ГГУ об общих условиях сделок. В свое время эти нормы были включены в ГГУ именно в целях защиты интересов потребителя от несправедливых условий договоров присоединения.

В частности, признавая недействительным условие, согласно которому компания *Blizzard Entertainment* имеет право заблокировать доступ игрока к игре или аннулировать игровой аккаунт, если списание с кредитной карты игрока оказывается невозможным, суд обращает внимание на то, что § 314 ГГУ позволяет стороне при наличии серьезного основания расторгнуть длящиеся обязательственные отношения; но данный пункт договора не предполагает выяснения причин невозможности списания, а потому не позволяет установить, имеются ли серьезные основания для расторжения договора. Суд соглашается с доводами истца, что данное условие позволяет ответчику заблокировать аккаунт истца даже в том случае, когда невозможность списания была вызвана ошибкой в оформлении счета, допущенной самой компанией.

Признавая недействительным условие о праве компании в одностороннем порядке менять плату, суд отмечает, что это условие противоречит первому предложению абзаца первого § 307 ГГУ: «...положения общих условий сделок недействительны, если вопреки требованиям доброй совести они ставят контрагента стороны, использующей общие положения, в чрезвычайно невыгодное положение». Суд отметил, что хотя компания и объясняет свое право одностороннего изменения условий договора, защитой от мошенничества, но само это право практически неограниченно. В частности, не ограничено право компании менять характеристики программного обеспечения и оборудования, необходимого для доступа к *World of Warcraft*.

Наконец, условие об одностороннем изменении цены в потребительском договоре, несомненно, требует более надежных ориентиров, чем простая декларация об улучшении качестве и о борьбе с мошенниками.

Даже признавая, что компьютерная игра нуждается в постоянном улучшении, суд все же обращает внимание на то, что право компании

[1] https://www.telemedicus.info/urteile/Internetrecht/1451-LG-Berlin-Az-15-O-30012-Kuendigungsrecht-und-Preisanpassung-in-MMORPG-AGB-World-of-Warcraft.html

в одностороннем порядке изменять условия договора с потребителем не соответствует доброй совести.

Также недобросовестными суд признал и условия о порядке уведомления потребителя, поскольку право компании уведомлять потребителя посредством всплывающего окна на сайте означает, что потребитель не получит уведомление, если он не заходит на сайт в течение месяца, а по истечении месяца после изменения новые правила игры вступят в силу[1].

Суд оценивает это право компании в соответствии с п. 5 § 308 ГГУ и делает вывод о том, что предоставленное договором компании право самостоятельно выбирать способ уведомления предоставляет потребителю слишком мало гарантий получения такого уведомления, а потому нарушает права потребителя.

Из рассмотренных примеров с очевидностью следует, что отношения по поводу *MMOG* можно и нужно рассматривать в качестве потребительских, когда одна сторона отношений – организация, предоставляющая услуги в качестве вида своей деятельности, а другая сторона приобретает эти услуги для целей, не связанных с предпринимательской деятельностью.

В российском гражданском законодательстве нет специальных норм, регулирующих отношения по поводу *MMOG*. Само по себе такое отсутствие норм вряд ли можно считать недостатком нашего гражданского права. Нормы российского обязательственного права вполне успешно могут быть применены для регулирования отношений по поводу *MMOG*.

Значительно более серьезную проблему представляет собой нежелание российских судов рассматривать споры по поводу онлайн-игр всерьез.

Между тем в отношениях между онлайн-игроками и организаторами онлайн-игр есть по меньшей мере один аспект, несомненно заслуживающий внимания. Это защита прав несовершеннолетних.

Защита несовершеннолетних

Поскольку около четверти игроков – дети, а в силу своего небольшого житейского опыта несовершеннолетние участники *MMOG* на-

[1] https://www.telemedicus.info/urteile/Internetrecht/1451-LG-Berlin-Az-15-O-30012-Kuendigungsrecht-und-Preisanpassung-in-MMORPG-AGB-World-of-Warcraft.html.

иболее подвержены риску необдуманных вложений в «виртуальное имущество», отношения с участием несовершеннолетних, безусловно, заслуживают регулирования.

По одному из дел, рассмотренных судом Саарбрюккена[1], суд постановил, что бесплатные онлайн игры с оплатой дополнительных возможностей через телефонный счет противны добрым нравам (§ 138 ГГУ), поскольку не предусматривают проверку возраста несовершеннолетнего.

Из обстоятельств дела следовало, что 13-летний сын заявителя играл в онлайн-игру «Гладиатор – герой Рима». Эта игра может быть установлена бесплатно, но для того, чтобы повысить возможности персонажа, приобретаются «навыки». Эти «навыки» приобретаются за виртуальную валюту, а виртуальную валюту, в свою очередь, можно приобрести за реальные деньги. Среди систем оплаты имеется система оплаты посредством оплаты телефонного звонка на определенный номер.

Эту схему оплаты использовал 13-летний сын истца, в результате чего истцу был предъявлен телефонный счет с дополнительной оплатой в сумме 2 818 47 евро.

Суд установил, что рассматриваемая игра является особенно привлекательной для детей и подростков. Несмотря на то что ответчик ссылался на отсутствие у игры такой целевой аудитории, как несовершеннолетние, суд отметил, что ответчик должен был понимать, что игра адресована в том числе и несовершеннолетним, не полностью дееспособным гражданам.

Кстати, в доказательство того, что игра особенно привлекательная для детей, был проведен изящный филологический анализ используемых в игре фраз и речевых оборотов.

Поскольку очевидно, что в игре может принять участие и несовершеннолетний, ответчик обязан был позаботиться о проверке возраста того, с кем он заключает договор. То, что в отношения по оплате «навыков» ответчик непосредственно с несовершеннолетним не вступал, а использовал посредничество телефонного оператора, не уменьшило, а напротив, увеличило уверенность суда в том, что ответчик действовал недобросовестно. Суд пришел к выводу, что ответчик сознательно эксплуатировал незрелость и неопытность несовершеннолетнего, сначала предоставив несовершеннолетнему возможность играть бесплатно, а за-

[1] LG Saarbrücken, Urteilvom 22.06.2011, Az.: 10 S 60/10 (URL: https://www.kanzlei.biz/22-06-2011-lg-saarbruecken-10-s-60-10;https://dejure.org/dienste/vernetzung/rechtsprechung?Text=10%20S%2060/10 (дата обращения: 16.01.2017).

тем, когда несовершеннолетний был увлечен азартом игры, предоставив легкую возможность тратить отцовские деньги на оплату «навыков».

Кто с открытыми глазами ведет дела таким образом, что использует несовершеннолетних для возложения чрезмерных обязанностей на их родителей, тот нарушает добрые нравы, отмечается в судебном решении (*LGSaarbrücken*, *Urteilvom* 22.06.2011.Az.: 10 S 60/10)[1].

Игры в рабочее время. *MMOG* как вид предпринимательской деятельности

Одна из особенностей рассматриваемых онлайн-игр состоит в том, что игроки вступают между собой в соревнование. Игроки-граждане заинтересованы состязаться с гражданами. Своеобразной проблемой стал бизнес, суть которого хорошо поясняет еще одно рассмотренное в США дело – дело *Black Snow v. Mythic* (2002), Калифорния[2].

Компания *Black Snow* открыла отделение в Тихуане, где почасовая плата значительно меньше, чем в США. Там эта компания нанимала мексиканских рабочих с небольшой квалификацией или безо всякой квалификации и поручила этим рабочим часами играть в «Темные века Камелота» (*Dark Age of Camelot*). Рабочие эти выиграли множество внутриигровых предметов, которые затем компания продала за реальные деньги.

Когда разработчик игры, компания *Mythic Interactive*, обнаружила это нарушение и заблокировала аккаунт компании *Black Snow*, последняя еще и предъявила иск, обвиняя разработчиков в «недобросовестной деловой практике».

Представитель истца заявил, что ответчик действовал недобросовестно, ограничивая возможность передавать внутриигровые предметы. «Имеет ли игрок право на свое время, или же право на его время принадлежит ответчику? Разве не является это несправедливым, что ответчик помешал истцу продавать предметы, заработанные его собственным временем и за его истца счет?»[3]

---

[1] URL: https://www.kanzlei.biz/22-06-2011-lg-saarbruecken-10-s-60-10; https://dejure.org/dienste/vernetzung/rechtsprechung?Text=10%20S%2060/10 (дата обращения: 16.01.2016).

[2] BlackSnow Interactive v Mythic Entertainment Inc, No 02-00112 (C.D. Calif.) [2002].

[3] Цит. по: *Lastowka Greg and Hunter Dan*. The Laws of the Virtual Worlds. California Law Review, Forthcoming. Available at SSRN: https://ssrn.com/abstract=402860 or http://dx.doi.org/10.2139/ssrn.402860

Впрочем, процесс не был доведен до конца ввиду ликвидации компании *Black Snow*[1].

В деле *Hernandez v. Internet Gaming Entertainment*, 2007, Флорида[2] вопрос был рассмотрен с противоположной стороны.

Иск был заявлен одним из игроков *World of Warcraft* против юридического лица, усадившего своих низкооплачиваемых сотрудников добывать внутриигровое имущество и продававшего это внутриигровое имущество за реальные деньги.

Истец был возмущен тем, что ответчик, сделав участие в *World of Warcraft* видом предпринимательской деятельности, мешает другим игрокам (физическим лицам) получать от игры удовольствие.

Истец утверждал, что ответчик действует в противоречии с условиями лицензионного соглашения с конечным пользователем и правилами использования игры *World of Warcraft*, которыми установлено, что пользователь не имеет права продавать предметы за реальные деньги вне виртуального мира.

Истец утверждал, что *IGE* продавал внутриигровые предметы, причем в таком количестве, что создал ощутимый экономический вред для «честных игроков», поскольку снижал ценность их усилий, и ставил их персонажей в невыгодные условия, поскольку они не готовы приобретать ценные предметы через таких самозваных посредников. Этот иск был заявлен в качестве коллективного.

К слову сказать, во всех соглашениях по поводу *MMOG* сегодня содержится заверение: «Настоящим Пользователь заверяет, что является физическим лицом».

Заканчивая обзор законодательства об *MMOG de lege lata*, хотелось бы привести цитату из одной из англоязычных статей, посвященных исследуемой проблеме: «При том, что возникающие по поводу *MMOG* экономические отношения практически не урегулированы, потенциал для злоупотреблений открывается просто невероятный. Так же, как любая отрасль с большим количеством не отслеживаемых денег, сфера *MMOG* создает почву для злоупотреблений. Возможность злоупотреб-

[1] *Balkin Jack M.* Virtual Liberty: Freedom to Design and Freedom to Play in Virtual Worlds. Virginia Law Review, Vol. 90, No. 8, p. 2043, 2004; Yale Law School, Public Law Working Paper No. 74. Available at SSRN: https://ssrn.com/abstract=555683.

[2] Hernandez v. Internet Gaming Entertainment, U.S. Dist. Ct. Southern District of Florida, Case No:07-CIV-21403-COHN/SELTZER [2007].

лений еще более усиливается вследствие анонимности, свойственной Интернет»[1].

Правовое регулирование отношений по поводу *MMOG de lege ferenda*

Необходимость развития законодательства, а главное – судебной практики по поводу *MMOG*, представляется очевидной.

О направлениях совершенствования законодательства и (или) судебной практики можно спорить. Ряд авторов предлагают конкретизировать содержание ст. 1062 ГК РФ, указав в ней, что судебной защите не подлежат требования только из азартной игры, а не из всякой игры.

Так, Ю.В. Багно обосновывает необходимость введения в ГК РФ понятия «азартная игра» в качестве альтернативы уже закрепленного в нем термина «игра», поскольку использование в рамках гражданского права понятия «игра» является чересчур широким и отдаленным от законодательных предписаний[2].

Также П.В. Павленко делает вывод о необходимости «замены в ГК РФ словосочетания «игры и пари» на «азартные игры и пари», так как словосочетание «игры и пари», употребляемое законодателем в гл. 58 ГК РФ, является слишком широким и далеко не во всех случаях подлежит правовому регулированию (например, развлекательные игры с детьми в домашних условиях)»[3].

Таким образом, Ю.В. Багно и П.В. Павленко предлагают дополнить ст. 1062 ГК РФ словом «азартные».

В.В. Архипов, наоборот, считает, что такое изменение ст. 1062 ГК РФ привело бы к «несколько абсурдным» выводам: «Допустим, игроки в тот же *World of Warcraft* договорились об определенном варианте распределения добычи, полученной в результате победы над драконом *Deathwing*. Лидер рейда отказался распределять добычу данным образом и забрал все себе. Игроки обратились в суд общей юрисдикции с требованием о понуждении лидера рейда к распределению добычи

[1] *Methenitis Mark*. Internet Gambling Regulation Present and Future: Technology Outpaces Legislation as the MMORPG Problem Emerges (December 2005). P. 17.

[2] *Багно Ю.В.* Гражданско-правовое регулирование отношений, возникающих из игр и пари: автореф. дис. ... канд. юрид. наук. Краснодар, 2004. С. 9.

[3] *Павленко П.В.* Гражданско-правовое регулирование игр, пари и смежных с ними институтов гражданского права (сравнительный аспект): автореф. дис. ... канд. юрид. наук. М., 2009. С. 12.

в соответствии с изначальной договоренностью, с утверждением, что она (договоренность) представляет собой непоименованный гражданско-правовой договор и подлежит судебной защите, поскольку ст. 1062 ГК РФ распространяется теперь только на азартные игры и пари»[1].

Можно согласиться с тем, что само по себе добавление слова «азартные» в ст. 1062 ГК РФ проблемы не решит. Требуется телеологическое толкование ст. 1062 ГК РФ.

В частности, можно признать общепризнанным, что собственно игровая деятельность правом регулироваться не должна. Право не должно регулировать, как убивать монстров.

В конце концов, привлекательность многих *MMOG* для потребителя в том и состоит, что в онлайн-игре можно быть разбойником с большой дороги, воином-наемником с соответствующими этому ремеслу нравами и привычками, тираном, строящим свою империю, и т.д.

Например, игра *EVE online* известна своим экономическим эффектом для своих игроков в реальном мире. Эта космическая *MMOG* позволяет геймерам приобщиться к множеству профессий, включая горную добычу и пиратство. В результате за долгие годы появились большие корпорации, имеющие значительные средства в эквиваленте реального мира. На серверах игры происходит достаточно много преступлений и сомнительных действий, включая грабежи и разрушение корпораций. В таком случае вокруг этого появляется множество денег, что делает подобные вещи весьма прибыльными. Однажды один из игроков принял неверное решение, что привело к гигантским финансовым потерям. Этот геймер, пожелавший остаться анонимным, решил перевезти на корабле средств на сумму больше 6422 реальных долларов. Средства в основном были в виде чертежей, позволяющих производить определенное количество внутриигровых товаров и потому крайне ценных. Космический корабль, который должен был перевозить этот груз, был маленьким слабым судном, но игрок решил, что если он встретится с неприятелем, то сможет легко от него удрать. Но случилось так, что корабль не смог. И после того, как судно с чертежами вошло на вражескую территорию, оно было уничтожено вместе со всем грузом[2].

---

[1] *Архипов В.В.* Виртуальная собственность: системные правовые проблемы в контексте развития индустрии компьютерных игр // Закон. 2014. № 9. С. 69–90.

[2] Игрок EVE online лишился 6000 долларов // Сайт мир nvidia (URL: http://nvworld.ru/news/eve-online-player-lost-6k-bucks (дата обращения: 02.01.2017).

Такое внутриигровое уничтожение виртуального имущества, несомненно, не должно стать поводом для судебного разбирательства в реальном мире, так как оно входит в правила игры.

Большинство исследователей считают перспективным использование теста «магического круга» Б.Т. Дюранске[1].

Как пишет В.В. Архипов, этот термин был позаимствован Б.Т. Дюранске у Й. Хейзинги, известного голландского исследователя роли игр в культуре, автора классического труда *Homo Ludens* («Человек играющий», 1938). Суть его заключается в том, что пространство игры отделено от реального пространства неким магическим кругом, действия внутри и вне которого не должны зависеть друг от друга. Сам тест выражается в следующем высказывании: «Деятельность, имеющая место в виртуальном мире, подчиняется праву реального мира в том случае, если пользователь, участвующий в данной деятельности, во время ее осуществления разумно осознает или должен разумно осознавать, что она влечет последствия для реального мира»[2]. Б.Т. Дюранске предлагает использовать этот тест в качестве процессуальной теории для применения в американском суде, но в целом его логика может быть применима и в других правовых системах[3].

Как представляется, в дискуссии о применении ст. 1062 ГК РФ все спорящие правы. Правила ст. 1062 ГК РФ о том, что обязательства из игр и пари не обеспечены судебной защитой, действительно были продиктованы прежде всего отрицательным отношением общества к азартным играм. И также верно, что право на самом деле не должно регулировать ни процесс игры в футбол, ни процесс игры в покер, ни процесс игры в *World of Tanks*, ни другие подобные игровые процессы.

Состоится изменение ст. 1062 ГК РФ или нет, главное, чтобы установленный ею запрет не толковался слишком расширительно. Неправильно, когда без судебной защиты остается требование участника, связанное с незаконной блокировкой аккаунта, так как это требование выходит далеко за пределы «магического круга».

---

[1] *Савельев А.И.* Правовая природа виртуальных объектов, приобретаемых за реальные деньги в многопользовательских играх // Вестник гражданского права. 2014. № 1. С. 127–150; *Архипов В.В.* Виртуальная собственность: системные правовые проблемы в контексте развития индустрии компьютерных игр // Закон. 2014. № 9. С. 69–90.

[2] *Дюранске Б.Т., Кейн Ш.Ф.* Виртуальные миры, реальные проблемы // Известия высших учебных заведений. Правоведение. 2013. № 2 (цит. по: *Архипов В.В.* Указ. соч. С. 69–90).

[3] Там же.

Продолжая аналогию с футболом, незаконная блокировка аккаунта игрока – это примерно то же, что не пустить болельщика, купившего билет, на футбольный матч, – действие, очевидно дающее право на иск.

При этом сегодняшняя проблема отечественной судебной практики состоит именно в том, что установленное ст. 1062 ГК РФ ограничение толкуется слишком расширительно.

В частности, по обстоятельствам нескольких дел потребителю отказали в иске, связанном с незаконной блокировкой аккаунта, ссылаясь на ст. 1062 ГК РФ.

Так, по обстоятельствам одного из дел[1] истец требовал взыскать с организатора онлайн игры деньги, потраченные на дополнительные игровые возможности, в связи с тем, что после оплаты этих возможностей игровой аккаунт был заблокирован. «По информации ответчика, блокирование аккаунта истца администратором игры производилось по причине нарушения П. правил игры. По утверждению истца, каких-либо нарушений игрового процесса он не допускал. Анализ возникших между сторонами правоотношений, приведенных выше требований закона, условий пользовательского соглашения позволяет сделать вывод о том, что наличие либо отсутствие в действиях пользователя нарушения правил игры относится к организации игрового процесса, а поэтому заявленные П. требования, как связанные с участием в игре, в силу п. 1 ст. 1062 ГК РФ судебной защите не подлежат» – отмечается в судебном акте.

Таким образом, одной лишь ссылки ответчика на нарушение истцом правил игры оказалось достаточно, чтобы суд применил ст. 1062 ГК РФ и даже не стал выяснять, было ли нарушение.

По другому делу конфликт также возник в связи с тем, что ответчик заблокировал аккаунт истца по причине допущенных нарушений, и сделано это было непосредственно после «покупки» истцом дополнительных возможностей. Истец заявляет, что нарушений не допускал. «Анализ возникших между сторонами правоотношений позволяет сделать вывод о том, что наличие либо отсутствие в действиях пользователя нарушения правил игры относится к организации игрового процесса, в связи с чем заявленные П. исковые требования, как связанные с участием в игре, в силу п. 1 ст. 1062 ГК РФ судебной защите не подлежат»[2].

[1] Постановление Президиума Московского городского суда от 24.05.2013 по делу № 44г-45.

[2] Определение Московского городского суда от 06.05.2013 № 4г/1-1017. Такое же рассуждение имеется в иных судебных актах: Определение Московского городского су-

Конечно, право не должно регулировать, «как правильно забивать гол». Но если судья взял принадлежащий игроку мяч и ушел с ним, разве лишен игрок возможности предъявить виндикационный иск?

Логика этого судебного акта видится весьма спорной.

Далее, по двум другим делам потребители также заявляли требования о возврате денег, потраченных на дополнительные игровые возможности после незаконной, по их мнению, блокировки аккаунта. Примечательно, что блокировка аккаунта произошла тогда, когда игрок еще не смог воспользоваться оплаченными игровыми возможностями.

Эти дела[1] примечательны тем, что суд признал, что участник игры являлся потребителем. Организатор же игры в этих делах ссылался на то, что блокировка была необходима для того, чтобы обеспечить участие в игре другим пользователям.

И несмотря на то, что участник игры правильно, на мой взгляд, был признан в этих делах потребителем, суд даже не попытается применить ни ст. 18 Закона о защите прав потребителей, ни ст. 310 ГК РФ.

Напротив, в судебных актах отмечается, что «блокирование аккаунта истца администратором игры производилось по той причине, что использование истцом дополнительных платных сервисов могло привести к сбою игрового процесса, что могло повлечь невозможность для других пользователей продолжать игру, что явилось бы нарушением их интересов».

Нельзя не отметить, что это довольно спорный принудительный альтруизм. Если ответчик считает необходимым не предоставить потребителю оплаченную им услугу для того, чтобы иметь возможность предоставить другим потребителям услуги не оплаченные, нельзя ли вернуть истцу хотя бы потраченные деньги?

Вместо этого суд ссылается на условия пользовательского соглашения: «Учитывая что, по условиям Пользовательского соглашения, а также Правилам игры ООО «Геймшок» имело право отключить платные сервисы истца, включая свойства игровых предметов, с целью соблюдения баланса интересов пользователей в бесплатной онлайн-игре, судебная коллегия полагает, что суд обоснованно пришел к выводу

да от 06.10.2011 по делу № 4г/1-8422; Постановление Президиума Московского городского суда от 24.05.2013 по делу № 44г-45.

[1] Апелляционное определение Московского городского суда от 14.07.2015 по делу № 33-24464/2015; Определение Московского городского суда от 16.11.2015 № 4г/6-11858/2015.

об отказе в удовлетворении заявленных истцом требований в полном объеме»[1].

С сожалением приходится констатировать, что требование о признании этого условия недействительным не было предъявлено истцом.

Можно напомнить, что в берлинском деле *Blizzard Entertainmen* (2014) аналогичное условие было признано недействительным.

Далее в анализируемом отечественном судебном акте совершенно необоснованно подчеркивается бесплатный характер участия в игре: «...в заключенном между сторонами Пользовательском соглашении отсутствует условие о выплате пользователю игры вознаграждения, участие в игре является бесплатным»[2].

Довод суда о том, что истец имел возможность ознакомиться с пользовательским соглашением и узнать о праве коммерческой организации в одностороннем порядке изменить условия предоставления услуг[3], тоже неубедителен.

Сопоставление этих трех дел с делом *Blizzard Entertainment* (2014) приводит к неутешительному выводу, что российские участники многопользовательских онлайн игр защищены меньше, чем их немецкие собратья. Не решен даже вопрос о признании граждан, принимающих участие в *MMOG*, потребителями.

Размышляя о необходимости изменить эту ситуацию, конечно, хотелось бы подчеркнуть, что следует соблюдать баланс интересов сторон и избегать возложения на организатора игр одних лишь обязанностей. В конце концов, затраты на разработку онлайн-игр тоже должны окупаться. Однако и существующее положение вещей вряд ли заслуживает сохранения.

Договоры присоединения чреваты нарушением интересов присоединившейся стороны. Это общеизвестно. В сфере *MMOG* используются именно договоры присоединения.

В других, более привычных сферах использования договоров присоединения, в частности в банковской деятельности, в лизинговой деятельности, российской судебной практикой накоплен большой опыт оценки справедливости договорных условий. Почему бы не использовать этот опыт в новой для отечественной судебной практики сфере?

---

[1] Апелляционное определение Московского городского суда от 14.07.2015 по делу № 33-24464/2015.

[2] Там же.

[3] Определение Московского городского суда от 16.11.2015 № 4г/6-11858/2015.

Первое, что нужно сделать для того, чтобы урегулировать отношения по поводу *MMOG*, – это отказаться от чрезмерно широкого применения ст. 1062 ГК РФ. Норма ст. 1062 должна применяться лишь в том случае, когда конфликт является частью игры и не связан с предоставлением или отказом от предоставления услуги потребителю.

Второе: представляется необходимым распространить действие Закона о защите прав потребителей на отношения между организатором игры и пользователем.

Приведенное выше решение по делу *Blizzard Entertainment* (2014) показывает, что по крайней мере в одном случае такое распространение не встретило никаких доктринальных препятствий.

А.И. Савельев предлагает «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]. Он обращает внимание, что легальная дефиниция термина «потребитель» указывает на того, кто приобретает имущество (работы, услуги) именно на основании возмездного договора[2].

Не отрицая верности этого общего вывода, хотелось бы уточнить его применительно к особенностям *MMOG*. Большая часть этих игр на самом деле игры бесплатные, но эта «бесплатность» весьма ограниченна. Она направлена на то, чтобы вовлечь пользователя в виртуальный мир, продемонстрировать ему имеющиеся в этом виртуальном мире возможности и мотивировать приобретение внутриигровых предметов или навыков за реальные деньги.

Бесплатная часть игры поэтому может рассматриваться как определенное преддоговорное отношение, которое, по крайней мере для организатора игры, призвано предшествовать заключению возмездных договоров.

Поэтому и на того пользователя, который вступает в *MMOG* бесплатно, видится целесообразным распространить правила Закона о защите прав потребителей[3] (или по крайней мере те из правил, которые касаются права потребителя на информацию).

В связи с тем, что отношения между организатором игры и пользователем можно признать потребительскими отношениями, а норму

[1] *Савельев А.И.* Электронная коммерция в России и за рубежом: правовое регулирование. 2-е изд. М.: Статут, 2016 (СПС «КонсультантПлюс»).

[2] Там же.

[3] СЗ РФ. 1996. № 3. Ст. 140.

ст. 1062 ГК РФ применимой только при отказе разрешать внутриигровые конфликты, но не конфликты между организатором онлайн игры и ее участником, следует отметить, что ряд общих норм российского гражданского права успешно могут быть использованы для защиты прав участника *MMOG*.

1. Третейские оговорки: оговорки о том, что споры из *MMOG* могут рассматриваться только и исключительно в третейском суде и не подведомственны судам общей юрисдикции, следует толковать как норму, ограничивающую доступ к правосудию, а потому недействительную на основании ст. 10 ГК РФ.

2. Коммерческая организация вправе отказаться от договора с потребителем только в случаях, предусмотренных законом (ст. 310 ГК РФ).

Право коммерческой организации в одностороннем порядке менять условия договора декларируется практически в каждом пользовательском соглашении практически в каждой *MMOG*.

Так, в п. 6.1.1 пользовательского соглашения с компанией *Wargaming* отмечается, что организатор игры вправе «в любое время в одностороннем порядке ограничивать, расширять, дополнять, модифицировать и иным образом изменять Игровые ресурсы, включая любые элементы и части Игр, без предварительного уведомления Пользователя, в том числе путем изменения Ключевых документов».

«Модификация Игровых ресурсов и их элементов может осуществляться посредством создания и установки новых частей программного обеспечения (патчей). Их целью может являться, например, усовершенствование или изменение игрового процесса (геймплея) либо добавление в Игру новых возможностей («*features*»), что может привести к удалению или приостановлению доступа к определенным Игровым элементам. Пользователь понимает и настоящим признает, что данные действия являются неотъемлемой частью процесса создания Игры и функционирования Игровых ресурсов, а также дает согласие на совершение данных действий *Wargaming* без предварительного уведомления Пользователя»[1].

Вместе с тем согласно ст. 310 ГК РФ 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 пре-

[1] http://legal.ru.wargaming.net/ru/eula/

доставлено договором лишь стороне, не осуществляющей предпринимательской деятельности.

Таким образом, «игрок» может от договора отказаться, а организатор игры – нет.

При этом телеологическое толкование ст. 310 ГК РФ позволяет сделать вывод о том, что коммерческая организация вправе изменять договор, если это изменение исключительно в пользу потребителя.

Поэтому условия договора могут изменяться либо по соглашению сторон, либо на свой риск коммерческой организацией, при этом коммерческая организация должна быть готова доказать, что такое изменение предоставляет пользователю новые возможности, блага, преимущества.

Кстати, можно утверждать, что не всякое изменение контента следует считать изменением условий договора, поскольку «уровень выносливости орка» или «дальнобойность советского танка Т-34», очевидно, нельзя считать условиями пользовательского соглашения.

Условия же, подобные п. 6 Пользовательского соглашения с компанией *Wargaming*, согласно которому «*Wargaming* вправе... прекратить доступ Пользователя к Игровым ресурсам, включая Аккаунт и Игры, в соответствии с настоящим Соглашением, в частности, при нарушении Пользователем условий Соглашения или Ключевых документов. *При реализации данного права Wargaming не обязан предоставлять Пользователю доказательства, свидетельствующие о нарушении Пользователем условий Соглашения, в результате которого Пользователю был прекращен или ограничен доступ*»[1] (курсив мой. – *Е.А.*), явно противоречат ст. 310 ГК РФ.

3. Квалификация обязательства между организатором игры и пользователем в качестве потребительского означает еще и то, что организатор игры обязан рассматривать имущественные претензии пользователя в сроки, установленные Законом о защите прав потребителя. А пользователь, в свою очередь, имеет право требовать взыскания неустойки за неисполнение правомерных требований потребителя.

4. Наконец, всякий договор между организатором *MMOG* и пользователем является договором присоединения.

Поэтому пользователь может ссылаться на недействительность недобросовестных условий договора согласно ст. 10 и 168 ГК РФ и использовать правило толкования *contra proferentem* при неясности условий пользовательского соглашения.

[1] http://legal.ru.wargaming.net/ru/eula/

В целом перспективы применения Закона о защите прав потребителей и норм ГК РФ о договорах и обязательствах к договорам между организаторами *MMOG* и участниками кажутся весьма привлекательными.

Разумеется, если кто-то из отечественных юридических лиц последует дурному примеру компании *Black Snow* и сделает зарабатывание «виртуального имущества» видом предпринимательской деятельности, такие отношения не следует признавать потребительскими.

Правовая природа договора между организатором *MMOG* и пользователем

Как было сказано выше, налоговые органы обычно квалифицируют отношения между организатором *MMOG* и пользователем как договор возмездного оказания услуг.

По природе осуществляемой коммерческой организацией деятельности этот договор на самом деле ближе всего к договору возмездного оказания услуг. Деятельность разработчика/организатора не имеет овеществленного результата, полезный эффект этой деятельности неотделим от самой по себе деятельности.

В литературе отмечается, что характеристика *MMOG* как договора возмездного оказания услуг не в интересах потребителя.

Так, А.И. Савельев пишет, что в случае, когда предоставление внутриигровых объектов рассматривается пользовательским соглашением в качестве услуги, услуга считается оказанной в момент «зачисления» таких ценностей на аккаунт пользователя[1].

Нельзя не отметить, что квалификация договора и момент, с которого услуга считается предоставленной, – это все же совершенно разные вопросы.

Действительно, многие договоры *MMOG* предусматривают, что «услуги в виде получения и использования дополнительных возможностей, которые Пользователь получает за плату, считаются оказанными в момент зачисления внутриигровых ценностей на Учетную Запись Пользователя»[2].

---

[1] *Савельев А.И.* Правовая природа виртуальных объектов, приобретаемых за реальные деньги в многопользовательских играх // Вестник гражданского права. 2014. № 1. С. 127–150.

[2] Пункт 10.3 Пользовательского соглашения *WorldofTanks*, компании *Wargaming* (версия от 16.06.2016) (http://legal.ru.wargaming.net/ru/eula/).

Однако эта формулировка всего лишь одна из возможных в договоре возмездного оказания услуг. Она действительно наиболее выгодна для организатора *MMOG*, а пользователь не имеет возможности обсуждать это условие, присоединяясь ко всему договору в целом.

Однако это лишь означает, что имеет смысл обсуждать действительность данного условия в контексте Постановления Пленума ВАС РФ «О свободе договора и ее пределах»[1]. Вполне возможно, данное условие следует считать «явно обременительным» и «нарушающим существенным образом баланс интересов сторон» (п. 10 Постановления Пленума).

Но в любом случае данное условие не составляет достаточной причины отказаться от квалификации договора в качестве договора возмездного оказания услуг.

Пределы договорного регулирования

Договорного регулирования тем не менее недостаточно.

Нормы обязательственного права эффективно могут урегулировать отношения между организатором *MMOG* и ее участником.

Но два, три участника или две тысячи участников, скажем, того же *World of Tanks* в соглашения между собой не вступали. Поэтому возникает потребность сконструировать правоотношения, приближенные к абсолютным. При этом используется аналогия с правом собственности не потому, что виртуальные возможности кто-то на самом деле отождествляет с вещами, а потому, что такая аналогия кажется простой и полезной.

Один из исследователей, *Joshua Fairfield*, отмечает, в частности, что договоры бессильны управлять столь обширными сообществами, которые возникают в отношении каждой *MMOG*, обладающей популярностью[2]. Договорное право берет на себя непосильную задачу управлять отношениями внутри огромного общества. Составители договоров пытаются подражать таким институтам, как право собственности или деликтное право, но получается плохо. И не потому, что договоры плохо написаны, а потому, что договоры вообще не предназначены регули-

[1] О свободе договора и ее пределах см.: Постановление Пленума ВАС РФ от 14.03.2014 № 16 // Вестник ВАС РФ. 2014. № 5.

[2] *Fairfield Joshua*. Anti-Social Contracts: The Contractual Governance of Virtual Worlds (July 2007) // McGill Law Journal. Vol. 53, 2008; Washington & Lee Legal Studies Paper. No. 2007-20. Available at SSRN: https://ssrn.com/abstract=1002997

ровать отношения внутри обширной, неоднородной и постоянно изменяющейся группы людей[1]. Например, договоры плохо защищают вложения в «виртуальное имущество» (примером чему являются ситуации взлома аккаунтов и «хищения» полученных в ходе игры предметов). «Кодексы поведения», которые используются наряду с контрактами, создают чудесные нормы, аналогичные деликтному праву, но потерпевший в случае нарушения использовать их не может[2].

Контракты хороши, когда двое договариваются о будущем своем поведении, но для таких огромных сообществ такие контракты вряд ли работают. *Joshua Fairfield* считает, что контракт по природе своей не может урегулировать отношения внутри интернет-сообщества[3].

Для развития отношений внутри этого сообщества требуются нормы публичного права. Кроме того, нормы деликтного права и нормы о праве собственности могут быть модифицированы для регулирования отношений внутри интернет-сообществ[4].

Особенно широко распространена аналогия с правом собственности в странах Азии – Южной Корее, Китае.

Так, например, в деле *See Bragg v. Linden Research* истец обратился с иском к организатору онлайн игр. По мнению истца, организатор плохо обеспечил защиту своего программного обеспечения. В результате аккаунт истца был взломан, заработанное истцом «виртуальное имущество» было похищено. Суд установил, что недостаточная защита сервера ответчика стала причиной кражи. Примечательно, что истец ссылался на то, что виртуальное имущество было заработано им, его «временем, мудростью, деньгами»[5].

Но «ассоциативная цепочка» в праве – не всегда самый удачный выход из сложной ситуации.

А.И. Савельев приводит убедительные доводы против использования проприетарной концепции в отношении внутриигровых предметов и игровых персонажей. Он отмечает, что (1) «объектом права собственности в системе координат российского вещного права могут

[1] *Fairfield Joshua*. Anti-Social Contracts: The Contractual Governance of Virtual Worlds (July 2007) // McGill Law Journal. Vol. 53, 2008; Washington & Lee Legal Studies Paper. No. 2007-20. Available at SSRN: https://ssrn.com/abstract=1002997

[2] Там же.

[3] Там же.

[4] Там же.

[5] https://www.newscientist.com/article/dn4510-gamer-wins-back-virtual-booty-in-court-battle/

быть только вещи, причем индивидуально-определенные, поэтому виртуальные объекты формально не могут регламентироваться нормами о праве собственности ввиду их явно выраженного нематериального характера», (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 оно существует. Складывается 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[1].

Приведенные доводы можно дополнить следующим небольшим соображением.

Действительно, распространение на «виртуальное имущество» некоторых норм о праве собственности более серьезно защитило бы потребителя. Но эти же нормы возложили бы на организатора онлайн игры довольно тяжелые обязанности поддерживать виртуальный мир в более или менее неизменном состоянии.

Это означало бы и невозможность когда-нибудь просто отключить сервер.

При этом онлайн игры довольно быстро устаревают. Представим себе консерватора, который любит играть в *World of Tanks*, хочет играть в *World of Tanks* и тогда, когда никто другой уже не играет в *World of Tanks*, а все переключились на более совершенный аналог. Действительно ли разработчики (организаторы) этой онлайн игры обязаны поддерживать функционирование виртуального мира бесконечно, притом что обслуживание сервера требует затрат?

Подобного рода проблемы уже возникали применительно к тем *MMOG*, которые были разработаны первыми (а соответственно первыми и устарели). Пользуясь льготными (сформулированными ими же) условиями пользовательских соглашений, организаторы этих устаревших онлайн игр перевели пользователей на более совершенные «платформы».

[1] *Савельев А.И.* Правовая природа виртуальных объектов, приобретаемых за реальные деньги в многопользовательских играх // Вестник гражданского права. 2014. № 1. С. 127–150.

Так, в пользовательском соглашении одной из популярных игр содержится условие о том, что «*Blizzard Entertainment* может по собственному усмотрению предлагать тем или иным пользователям перенос их персонажей из перенаселенного «Исходного» игрового мира в «Новый»»[1].

При этом в том же пункте отмечается, что не все персонажи, льготы и возможности переносятся.

Вряд ли стоит возлагать на разработчика и организатора онлайн игр явно невыполнимые обязанности.

Кроме того, нет достаточных оснований характеризовать право на виртуальное имущество как абсолютное правоотношение. В абсолютном правоотношении управомоченному противостоит весь мир.

В отношении виртуального имущества, снабженных дополнительными возможностями персонажей и тому подобных отношениях управомоченному противостоит сообщество других игроков, которое может быть более или менее обширным (так, количество пользователей *World of Tanks* в 2016 г. составляло, по сведениям РБК, 110 млн), но все же не равно всему человечеству[2].

Всегда рядом может оказаться человек, не знающий и не обязанный знать, что такое *MMOG* и виртуальное имущество. И если поздним вечером задержавшийся в офисе менеджер очень близко подошел к приобретению желаемого акционного приза, но внезапно монтер выключил в офисе электричество, не получится взыскать с монтера упущенную выгоду.

Поэтому аналогия с правом собственности пока остается, на мой взгляд, таким же условным сравнением, как и характеристика Интернета в качестве пространства.

Вместе с тем проблема остается, и она состоит в том, что отношения между пользователями никак не урегулированы ни договором (пользователи между собой договором не связаны), ни законодательством.

В этой части кажется перспективным использование норм деликтного права, с той лишь обязательной поправкой, что действие, предположительно оцениваемое как деликт, должно находиться за рамками игры. Так, если корабль с ценным грузом в игре *EVEonline* был ограблен пиратами, то возможность нападения пиратов пред-

[1] Пользовательское соглашениеWorld of Warcraft: http://eu.blizzard.com/ru-ru/company/legal/wow_tou

[2] http://www.rbc.ru/newspaper/2016/05/11/572c7edd9a7947089d1f050c

усмотрена содержанием этой игры. Поэтому, несмотря на то, что владелец груза платил за этот груз реальными деньгами, деликт все же отсутствует.

Но если пользователь *N* взломал аккаунт пользователя Z и «похитил» виртуальное «имущество», это действие безусловно можно оценивать в качестве противоправного.

При характеристике действия в качестве деликта придется, однако, доказывать, что действие причинило вред имуществу или личности потерпевшего (ст. 1064 ГК РФ).

Причиняет ли вред хищение «виртуального имущества»? Очевидно, что да, поскольку для достижения аналогичного результата игроку придется потратить время и (или) реальные деньги. Является ли такой вред имущественным? Очевидно, что да, особенно в том случае, когда достижение прогресса, аналогичного тому, что был до правонарушения, требует вложения реальных, а не игровых денег.

MMOG и защита прав несовершеннолетних

В заключение хотелось бы рассмотреть проблему защиты прав несовершеннолетних в сфере *MMOG*. Выше было приведено очень удачное, на мой взгляд, решение суда Саарбрюккена, в котором сделка по покупке «особых навыков персонажа», совершенная несовершеннолетним, была признана недействительной.

В российском гражданском праве тоже есть правила о недействительности сделки, совершенной несовершеннолетними (ст. 26, 28 ГК РФ), а в Законе о рекламе – требования к рекламе, установленные для защиты прав несовершеннолетних. Но в ситуации участия в *MMOG* все это плохо применяется.

Во-первых, многие *MMOG* по своему содержанию, оформлению, расположению рекламы о них адресованы несовершеннолетним.

Во-вторых, в любом пользовательском соглашении содержится правило, согласно которому пользователь заявляет о том, что достиг возраста 18 лет и является дееспособным.

В-третьих, многие *MMOG* практикуютпродажи игровых возможностей и «виртуального имущества» путем направления sms на определенный номер.

SMS-приобретения «виртуальных мечей» и «виртуальных танков» несовершеннолетними, несомненно, случаются. Но в опубликованной судебной практике не нашлось ни оного дела, в котором такие прио-

бретения пытались бы оспаривать. Причиной этого предположительно являются проблемы в доказывании. Очень затруднительно доказать, что соответствующее sms-сообщение направил несовершеннолетний, а не более взрослый член семьи.

Вопрос защиты несовершеннолетних в этой части является предметом публично-правового регулирования.

Федеральный закон от 29.12.2010 № 436-ФЗ (с изм. от 29.06.2015) «О защите детей от информации, причиняющей вред их здоровью и развитию» вводит градацию информационной продукции (ст. 7–10), запрещает распространять среди детей информацию, отрицающую семейные ценности или обосновывающую или оправдывающую допустимость насилия и (или) жестокости (ст. 5). Но эти запреты ничего не добавляют в исследуемую сферу. Большинство *MMOG* не декларируются как адресованные подросткам, даже если они на самом деле адресованы подросткам, и в части защиты несовершеннолетних от необдуманных приобретений виртуального имущества ничего не добавляется.

Возможно, когда-нибудь, когда этот вопрос станет предметом внимания законодателя, данный Закон будет дополнен нормой, запрещающей в *MMOG* реализовывать виртуальное имущество и дополнительные игровые возможности любым способом, не предполагающим проверку личности покупателя. Хотя такая мера может несколько снизить доход разработчиков онлайн игр, она может способствовать защите прав несовершеннолетнего.

Пока при существующем состоянии законодательства контроль над тем, в какие игры играет ребенок и какое имущество он для этого покупает, остается на 100% вопросом ответственности и риска родителей.

Таким образом, в результате проведенного исследования было показано, что договоры между гражданами и организаторами *MMOG* отвечают всем признакам потребительских договоров и являются при этом договорами присоединения. Действующее гражданское законодательство и практика его применения содержат несколько очень полезных средств и способов защиты потребителя как экономически слабой стороны обязательства.

Эти средства и способы стоит использовать и в регулировании отношений по поводу *MMOG*. От такого использования виртуальные миры не станут беднее, но выходящие из виртуального мира в мир реальный граждане станут более защищенными.

Пристатейный библиографический список:

1. *Balkin Jack M.* Virtual Liberty: Freedom to Design and Freedom to Play in Virtual Worlds. Virginia Law Review, Vol. 90, No. 8. P. 2043, 2004; Yale Law School, Public Law Working Paper No. 74. Available at SSRN: https://ssrn.com/abstract=555683

2. Blizzard Entertainment // https://www.telemedicus.info/urteile/Internetrecht/1451-LG-Berlin-Az-15-O-30012-Kuendigungsrecht-und-Preisanpassung-in-MMORPG-AGB-World-of-Warcraft.html

3. Blizzard Entertainment // https://www.telemedicus.info/urteile/Internetrecht/1451-LG-Berlin-Az-15-O-30012-Kuendigungsrecht-und-Preisanpassung-in-MMORPG-AGB-World-of-Warcraft.html

4. Bragg v. Linden Lab // https://en.wikipedia.org/wiki/Bragg_v._Linden_Lab; Memorandum // http://www.paed.uscourts.gov/documents/opinions/07D0658P.pdf

5. Dougherty, Candidus, Bragg v. Linden: Virtual Property Rights Litigation. E-Commerce Law & Policy, Vol. 9, No. 7. July 2007. Available at SSRN: https://ssrn.com/abstract=1092284

6. *Fairfield Joshua.* Anti-Social Contracts: The Contractual Governance of Virtual Worlds (July 2007) // McGill Law Journal, Vol. 53. 2008; Washington & Lee Legal Studies Paper No. 2007-20. Available at SSRN: https://ssrn.com/abstract=1002997

7. *Lastowka Greg and Hunter Da.* The Laws of the Virtual Worlds. California Law Review, Forthcoming. Available at SSRN: https://ssrn.com/abstract=402860 or http://dx.doi.org/10.2139/ssrn.402860

8. LG Saarbrücken Urteilvom 22.06.2011 //https://dejure.org/dienste/vernetzung/rechtsprechung?Text=10%20S%2060/10

9. LG Saarbrücken, Urteilvom 22.06.2011 (URL: https://www.kanzlei.biz/22-06-2011-lg-saarbruecken-10-s-60-10).

10. Marc BRAGG, Plaintiff, v. LINDEN RESEARCH, INC. and Philip Rosedale, Defendants. No. CIV.A.06 4925. United States District Court, E.D. Pennsylvania (https://h2o.law.harvard.edu/cases/4435).

11. *Methenitis Mark.* Internet Gambling Regulation Present and Future: Technology Outpaces Legislation as the MMORPG Problem Emerges (December 2005). Available at SSRN: https://ssrn.com/abstract=987056 or http://dx.doi.org/10.2139/ssrn.987056

12. *Yoon Ung-gi.* Real Money Trading in MMORPG Items From a Legal and Policy Perspective (December 13, 2004) // Journal of Korean Judicature. Vol. 1. P. 418–477. 2008. Available at SSRN: https://ssrn.com/abstract=1113327 or http://dx.doi.org/10.2139/ssrn.1113327

13. *Антоненко А.А.* Интернет-зависимость подростков от компьютерных игр и онлайн-общения: клинико-психологические особенности и профилактика: автореф. дис. ... канд. психолог. наук. М., 2014.

14. *Архипов В.В.* Виртуальная собственность: системные правовые проблемы в контексте развития индустрии компьютерных игр // Закон. 2014. № 9.

15. *Багно Ю.В.* Гражданско-правовое регулирование отношений, возникающих из игр и пари: автореф. дис. ... канд. юрид. наук. Краснодар, 2004.

16. Игрок EVEonline лишился 6000 долларов // Сайт мир nvidia (URL: http://nvworld.ru/news/eve-online-player-lost-6k-bucks (дата обращения: 02.01.2017).

17. *Медведев Е.А.* Виртуальный мир как фактор социализации // Молодежь и общество на рубеже веков: тезисы и материалы конференции. М., 1998.

18. *Медведев Е.А.* Субкультура участников ролевых игр и методы исследования ее воздействия на личность: автореф. дис. ... канд. социол. наук. М, 2004.

19. *Павленко П.В.* Гражданско-правовое регулирование игр, пари и смежных с ними институтов гражданского права (сравнительный аспект): автореф. дис. ... канд. юрид. наук. М., 2009.

20. *Рыбалтович Д.Г.* Псхилогические особенности пользователей онлайн игр с различной степенью игровой аддикции: автореф. дис. ... канд. психол. наук. СПб., 2012.

21. *Савельев А.И.* Правовая природа виртуальных объектов, приобретаемых за реальные деньги в многопользовательских играх // Вестник гражданского права. 2014. № 1.

22. *Савельев А.И.* Электронная коммерция в России и за рубежом: правовое регулирование. 2-е изд. М.: Статут, 2016.

23. *Семенов Н.Б.* Виртуальные игровые практики в контексте преемственности и инноваций в культуре: автореф. дис. ... канд. социол. наук. Саратов, 2012.

А.А. Богустов

ЭЛЕКТРОННАЯ ФОРМА ДОГОВОРА В НАЦИОНАЛЬНОМ ПРАВЕ СТРАН – ЧЛЕНОВ ЕС (НА ПРИМЕРЕ ЗАКОНОДАТЕЛЬСТВА ПОЛЬШИ)

Аннотация. *В статье рассматриваются особенности регулирования электронных договоров правом Польши. Делается вывод, что регулирование порядка заключения и исполнения договоров, выраженных в электронной форме, отражает основные тенденции развития современного договорного права. К их числу относится дифференциация правового регулирования в зависимости от особенностей субъектного состава и предмета договора, а также ограничение принципа свободы договора в интересах защиты потребителя как экономически более слабой стороны.*

Ключевые слова: *электронный договор, свобода договора, оферта, потребитель.*

Одним из факторов, оказывающих влияние на развитие гражданского права, в последние десятилетия является развитие науки и техники. Прогресс в этих областях привел к изменениям в системе объектов гражданских прав, вещных прав, в праве интеллектуальной собственности и даже семейном праве. Не остается в стороне от этого процесса и обязательственное право. В частности, широкое внедрение информационных технологий во все сферы жизни породило необходимость регламентации договоров, выраженных в электронной форме.

Определенный опыт правового регулирования данной группы отношений накоплен в праве государств – членов ЕС. Его анализ позволяет выяснить господствующие подходы к регулированию данной группы отношений, которые могут быть восприняты в национальном законодательстве постсоветских стран.

В качестве примера можно обратиться к национальному законодательству Польши, на формирование которого в рассматриваемой нами сфере решающее воздействие оказали положения европейского права. Например, Директива Европейского парламента и ЕС 2000/31/ЕС

от 08.06.2000 об электронной торговле[1] легла в основу Закона Польши от 14.02.2003[2], внесшего изменения в ГК Польши[3]. В частности, в него была включена ст. 66[1], посвященная порядку заключения договора в электронной форме.

Упомянутая выше Директива 2000/31/ЕС и Директива Европейского парламента и ЕС 98/27/ЕС от 19.05.1998 «Предписания о защите интересов потребителей»[4] выступили источниками для принятия Закона Польши «Об оказании услуг электронным способом»[5]. Закон Польши «Об электронной подписи»[6] реализует положения Директивы Европейского парламента и ЕС 1999/93/ЕС от 13.12.1999 «Об основах законодательства Сообщества в сфере электронных подписей»[7]. Закон «Об охране отдельных прав потребителей и ответственности за ущерб, причиненный опасными продуктами»[8], инкорпорирует ряд актов европейского права, в том числе Директиву Европейского парламента и ЕС 97/7/ЕС от 20.05.2000 «О защите потребителей в отношении дистанционных договоров»[9].

Организационную основу существования электронных договоров создает Закон «Об оказании услуг электронным способом», который определяет обязанности исполнителей, основания освобождения их

[1] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce) (URL: http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:32000L0031).

[2] Ustawa o zmianie ustawy – Kodeks cywilny oraz niektyrych innych ustaw. 14 lutego 2003 r. // Dziennik Ustaw. 2003. Nr. 49. poz. 408.

[3] Kodeks Cywilny. 23 kwietnia 1964 r. // Dziennik Ustaw. 1964. Nr. 16. poz. 93, ze zm.

[4] Directive 98/27/EC of the European Parliament and of the Council of 19 May 1998 on injunctions for the protection of consumers' interests (URL: http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:31998L0027.

[5] Ustawa o świadczeniu usług drogą elektroniczną. 18 lipca 2002 r. // Dziennik Ustaw. 2002. Nr. 144. poz. 1204. Tekst jedn. Dz. U. z 2016 r. poz. 1030, 1579.

[6] Ustawa o podpisie elektronicznym.18 września 2001 r. // Dziennik Ustaw. 2001. Nr. 130. poz. 1450. Tekst jedn. Dz. U. z 2013 r. poz. 262, 2014 r. poz. 1662, z 2015 r. poz. 1893.

[7] Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures (URL: http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:31999L0093).

[8] Ustawa o ochronie niektórych praw konsumentów oraz o odpowiedzialności za szkodę wyrządzoną przez produkt niebezpieczny. 2 marca 2000 r. // Dziennik Ustaw. 2000. Nr. 22. poz. 271. Tekst jedn. Dz. U. z 2012 r. poz. 1225.

[9] Directive 97/7/EC of the European Parliament and of the Council of 20 May 1997 on the protection of consumers in respect of distance contracts (URL: http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:31997L0007).

от ответственности и принципы охраны личных данных заказчиков таких услуг.

Возможность заключения договора в электронной форме впервые была введена в польское право с момента принятия Закона «Об электронной подписи». Он дополнил ГК Польши (§ 2 ст. 78) положением о том, что волеизъявление, выраженное в электронной форме, подтвержденное достоверной электронной подписью, имеет равное значение с волеизъявлением, выраженным в письменной форме. То есть электронная и письменная формы сделки были приравнены по своим правовым последствиям.

Как было указано выше, порядок заключения договора в электронной форме урегулирован ГК Польши. При этом необходимо учитывать, что эти правила несколько отступают от общих положений о моменте вступления оферты в силу. В литературе высказывается мнение, что он зависит от того, «направлена ли оферта индивидуально определенному адресату либо неопределенному кругу адресатов (*ad incertas personas*). В первом случае оферта обязывает с момента возникновения у адресата возможности ознакомиться с ее содержанием (§ 1 ст. 61 ГК). А оферты, направленные *ad incertas personas,* обязывают со времени их совершения: они не требуют особого получения от оферента их адресатом»[1].

Применяя это положение к электронным договорам, польское законодательство устанавливает два порядка заключения таких соглашений. Из анализа § 2 ст. 61 ГК Польши можно сделать вывод, что выраженное в электронной форме волеизъявление, направленное определенному лицу, вступает в силу с момента поступления его в средство электронной коммуникации адресата таким способом, что у последнего возникает возможность ознакомиться с содержанием оферты. То есть в данном случае на оферту, выраженную в электронной форме (например, при помощи электронной почты), распространяются общие правила о предложении заключить договор.

Иная ситуация складывается, когда предложение заключить договор в электронной форме адресуется неопределенному кругу лиц. В соответствии с § 1 ст. 66^1 ГК Польши в отличие от общего порядка вступления предложения заключить договор в силу такая оферта связывает сделавшее ее лицо, только если адресат незамедлительно подтвердит ее получение. При этом такое подтверждение «не является

[1] *Radwański Z.* Prawo cywilne – część ogólna. Warszawa, 2004. S. 293.

волеизъявлением, направленным на принятие оферты, а лишь свидетельствует о ее получении»[1].

В случае направления оферты в электронной форме неопределенному кругу лиц законодательство устанавливает для предпринимателя обязанность до момента заключения договора предоставить другой стороне информацию «однозначным и понятным способом» (§ 2 ст. 66^1 ГК). Она должна содержать сведения о техническом порядке заключения договора в электронной форме, правовых последствиях подтверждения получения оферты адресатом, приемах и способах фиксации содержания заключенного договора и обеспечения предпринимателем доступа к нему контрагента, технических средствах и методах поиска и исправления ошибок во вводимых данных, языках, используемых для заключения договора, применимых кодексах этики и их доступности в электронной форме.

Обязанность предоставления подобной дополнительной информации существует у предпринимателя и в том случае, когда он приглашает другую сторону вести переговоры, делать оферты, заключать договор иным способом.

Возложение на предпринимателя таких обязанностей при заключении договора с использованием средств информационных технологий выступает в настоящее время в качестве одной из тенденций развития договорного права. Об этом свидетельствует тот факт, что положения аналогичного содержания включены и в Модельные правила европейского частного права (ст. II – 3:105 *DCFR*)[2].

Представляется, что установление обязанности предоставления предпринимателем информации связано со стремлением защитить интересы потребителя путем устранения неравенства преддоговорных позиций сторон. Так, из § 4 ст. 66^1 ГК следует, что в отношениях с потребителем у предпринимателя она носит императивный характер, а в отношениях между предпринимателями она существует, только если это установлено соглашением сторон.

Обязанность предоставления информации выступает проявлением нескольких взаимосвязанных тенденций развития современного зарубежного договорного права. С одной стороны, она является одним из проявлений ограничения принципа свободы договора, выражающегося и в обязанности относиться с уважением к партнеру по договору,

[1] *Radwański Z.* Prawo cywilne – część ogólna. Warszawa, 2004. S. 294.

[2] Модельные правила европейского частного права. М.: Статут, 2013.

обязанности информировать и предупреждать его. Эта обязанность «основана на трезвом, а потому и убедительном расчете, что служит справедливому распределению договорных рисков между сторонами и способствует увеличению как их прибыли, так и общественного богатства в целом»[1]. В свою очередь, в отношениях с потребителями обязанность информирования приводит к усилению требований к формальности договора. Цель в данном случае заключается в том, чтобы «нуждающийся в защите партнер по договору до или в момент его заключения в письменной форме получил как можно больше необходимой ему информации»[2].

Еще одним направлением правового регулирования соглашений в электронной форме является их регламентация в качестве особой разновидности дистанционных договоров. В соответствии со ст. 6 Закона об охране отдельных прав потребителей и ответственности за ущерб, причиненный опасными продуктами ими являются договоры, заключенные с потребителем без одновременного присутствия обеих сторон с использованием средств дистанционного взаимодействия, в частности печатных либо электронных формуляров заказа как адресованного, так и не адресованного конкретному лицу, серийных писем в печатной либо электронной форме, рекламы с отпечатанным бланком заказа в прессе, электронной рекламы, каталогов, телефона, телефакса, радио, телевидения, устройств автоматического вызова, видеофонов, видеотекста, электронной почты либо иных средств электронной коммуникации, если контрагентом потребителя является предприниматель, организовавший подобным образом свою деятельность.

Можно сделать вывод, что в данном случае правовое регулирование направлено не на установление особых правил закрепления волеизъявления сторон в электронной форме, а на обеспечение защиты прав потребителя при заключении им дистанционного договора.

Свобода договора в классическом понимании этого принципа имеет последствием обязательность договора для участников: «Заключившие договор связаны его условиями как законом. Должник не может отступать от своих обязанностей. Отмена договора может быть совершена только с согласия всех его участников»[3]. Однако в современных усло-

[1] *Цвайгерт К., Кетц Х.* Введение в сравнительное правоведение в сфере частного права. Т. 2. М.: Междунар. отношения, 1998. С. 19.

[2] Там же. С. 78–79.

[3] *Морандьер Л.Ж.* Гражданское право Франции. Т. 2. М.: Изд-во иностранной литры, 1960. С. 203.

виях действующее законодательство зачастую корректирует действие данного принципа в целях защиты потребителя как экономически более слабой стороны. Это выражается в предоставлении ему при определенных условиях возможности одностороннего отказа от ранее заключенного договора. Указанный процесс находит отражение и в регулировании польским правом дистанционных договоров. В соответствии со ст. 7 Закона «Об охране отдельных прав потребителей и ответственности за ущерб, причиненный опасными продуктами» заключивший дистанционный договор потребитель может от него отказаться без указания причин, заявив об этом в письменной форме в течение десяти дней. При этом возможность отказа не может быть обусловлена выплатой потребителем отступного. В случае отказа договор считается незаключенным, а потребитель освобождается от всех обязательств. У сторон возникает обязанность возвратить все полученное по договору в неизменном виде с учетом нормального износа. Возврат должен быть произведен не позднее 14 дней с момента отказа от договора. При этом, если потребитель осуществил предоплату каких-либо сумм, они должны быть возвращены с уплатой процентов, начисляемых с момента осуществления платежа.

Упомянутый выше 10-дневный срок для отказа от договора начинает течь с момента передачи вещи, а если договор предусматривает оказание услуги – то со дня ее оказания. Срок для отказа от договора может быть увеличен до трех месяцев с момента передачи вещи либо оказания услуги в случае непредставления потребителю необходимой информации (ч. 2 ст. 10 Закона «Об охране отдельных прав потребителей и ответственности за ущерб, причиненный опасными продуктами»).

Право на отказ от договора направлено на защиту потребителя в ситуациях, когда сделка совершается в условиях, не дающих ему в полной мере сформировать волю заключение договора, осознать сущность принятых на себя обязательств заключения договора и последствий данного соглашения. В связи с этим реализация права на отказ от дистанционного договора не является чем-то уникальным и лишь выражает общую тенденцию усиления правовой охраны интересов потребителей. Например, во многом сходный порядок отказа предусмотрен ст. 2–5 Закона «Об охране отдельных прав потребителей и ответственности за ущерб, причиненный опасными продуктами» в отношении договора, заключенного вне места постоянной деятельности предпринимателя («договора, заключенного на пороге дома»).

Предоставление столь широких прав потребителю на отказ от договора вызывает необходимость одновременно обеспечить и устойчивость коммерческого оборота. Достижению этой цели служит определение случаев невозможности отказа от дистанционного договора. В соответствии со ст. 10 Закона «Об охране отдельных прав потребителей и ответственности за ущерб, причиненный опасными продуктами» отказ по общему правилу невозможен, если услуги с согласия потребителя оказаны ему до истечения срока для отказа, потребителем повреждена оригинальная упаковка аудио-, видеозаписей и носителей информации, цена либо вознаграждение по договору зависит от изменения курса на финансовом рынке и т.д.

На защиту интересов потребителя направлено императивное правило о запрете возложения на него обязанностей по предоплате товаров и услуг. Кроме того, в содержание дистанционного договора включается указание на место и способ предъявления рекламации, которые должны не создавать чрезмерных трудностей и расходов для потребителей.

Дистанционный договор в соответствии со ст. 8 анализируемого Закона может быть заключен на определенный и неопределенный срок. Действие срочного договора ограничено одним годом, а при указании более длительного срока считается, что он заключен на неопределенный срок. Неопределенность срока договора предоставляет возможность в любой момент без объяснения причин отказаться от него, по общему правилу предупредив другую сторону за один месяц.

Еще одним правилом, имеющим целью защиту прав потребителей, является установление предельных сроков исполнения предпринимателем обязанностей по договору. В соответствии со ст. 12 Закона «Об охране отдельных прав потребителей и ответственности за ущерб, причиненный опасными продуктами» предприниматель обязан, если иное не установлено соглашением сторон, исполнить дистанционный договор в течение 30 дней с момента согласия потребителя на его заключение. Если исполнение договора невозможно в связи с тем, что его объект недоступен, предприниматель обязан немедленно, но не позднее 30 дней с момента заключения договора уведомить об этом потребителя и возвратить полученную от него денежную сумму в полном объеме.

Если это установлено соглашением сторон, предприниматель в случае хотя бы временной невозможности исполнения обязательства

имеет право предоставить взамен объект того же назначения, качества и цены, проинформировав письменно потребителя о принадлежащем ему праве отказаться как от принятия такого исполнения, так и от договора в целом.

В литературе справедливо отмечается, что тенденцией развития современного законодательства является дифференциация договоров в зависимости от их субъектного состава, которая «зачастую переплетается с дифференциацией правового регулирования в зависимости от особенностей предмета договора»[1]. Это положение в полной мере применимо к регулированию рассматриваемой нами группы отношений в польском праве. Так, среди соглашений, заключаемых между предпринимателями и потребителями, в особую группу выделяются дистанционные договоры, в том числе существующие и в электронной форме. Из правил, установленных для последней категории, делаются исключения для дистанционных договоров в сфере финансовых услуг, в отношении которых действует особый правовой режим (ст. 16^{a}–17 Закона «Об охране отдельных прав потребителей и ответственности за ущерб, причиненный опасными продуктами»).

В Законе «Об охране отдельных прав потребителей и ответственности за ущерб, причиненный опасными продуктами» получают дальнейшее развитие предписания ГК о праве на получение информации потребителем при заключении договора. В соответствии со ст. 9 Закона не позднее совершения предложения заключить договор предприниматель обязан сообщить ему «одновременно, в понятной и легкой для прочтения форме» официальные данные о себе, существенных свойствах и предмете исполнения, цене и всех составляющих ее элементах, включая налоги и пошлины, опорядке и способе ее оплаты и т.д. Кроме того, на предпринимателя возлагается обязанность письменно подтвердить потребителю указанную информацию не позднее начала исполнения договора.

Однако, говоря об установлении как ГК, так и Законом «Об охране отдельных прав потребителей и ответственности за ущерб, причиненный опасными продуктами» обязанности предоставления информации, следует обратить внимание на то, что ее неисполнение практически не влечет негативных последствий для предпринимателя. Едва ли не единственным последствием этого является упоминавшееся выше

[1] *Кулагин М.И.* Предпринимательство и право: опыт Запада // *Кулагин М И.* Избранные труды. М.: Статут,1997. С. 262.

продление срока, в течение которого потребитель может отказаться от договора. В этом проявляется общая тенденция развития современного договорного права, которая состоит в том, что «вопрос о санкциях в случаях нарушения обязательства о предоставлении информации решается законодателем зачастую неполно, иногда слишком сложно, а иногда и вообще не решается»[1].

На основании проведенного в настоящей статье исследования можно сделать вывод, что регулирование порядка заключения и исполнения договоров, выраженных в электронной форме, отражает основные тенденции развития современного договорного права. К их числу относится дифференциация правового регулирования в зависимости от особенностей субъектного состава (установление особых правил заключения договоров между предпринимателями и потребителями, между предпринимателями, а также между лицами, не осуществляющими предпринимательскую деятельность) и предмета договора (выделение в отдельную группу регулирования договоров по оказанию финансовых услуг). Важным направлением развития современного права, проявляющимся в регулировании электронных договоров, выступает ограничение принципа свободы договора в интересах защиты потребителя как экономически более слабой стороны.

Пристатейный библиографический список:

1. *Кулагин М.И.* Предпринимательство и право: опыт Запада // *Кулагин М.И.* Избранные труды. М.: Статут,1997.

2. Модельные правила европейского частного права. М.: Статут, 2013. – 989 с.

3. *Морандьер Л.Ж.* Гражданское право Франции. Т. 2. М.: Изд-во иностранной лит-ры, 1960. – 728 с.

4. *Цвайгерт К., Кетц, Х.* Введение в сравнительное правоведение в сфере частного права. Т. 2: Договор. Неосновательное обогащение. Деликт. М.: Международные отношения, 1998. – 512 с.

5. Directive 97/7/EC of the European Parliament and of the Council of 20 May 1997 on the protection of consumers in respect of distance contracts (URL: http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:31997L0007 (дата доступа: 20.03.2017)).

[1] *Цвайгерт К., Кетц Х.* Указ. соч. С. 79.

6. Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures (URL: http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:31999L0093 (дата доступа: 20.03.2017)).

7. Directive 98/27/EC of the European Parliament and of the Council of 19 May 1998 on injunctions for the protection of consumers' interests (URL: http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:31998L0027 (дата доступа: 20.03.2017)).

8. Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce) (URL: http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:32000L0031 (дата доступа: 20.03.2017)).

9. Kodeks Cywilny. 23 kwietnia 1964 r. // Dziennik Ustaw. 1964. Nr. 16. – poz. 93, ze zm.

10. *Radwański Z.* Prawo cywilne – część ogólna. Warszawa: C.H. Beck, 2004. – 361 s.

11. Ustawa o ochronie niektórych praw konsumentów oraz o odpowiedzialności za szkodę wyrządzoną przez produkt niebezpieczny. 2 marca 2000 r. // Dziennik Ustaw. 2000. Nr 22. – poz. 271. t.j. Dz. U. z 2012 r. poz. 1225.

12. Ustawa o podpisie elektronicznym.18 września 2001 r. // Dziennik Ustaw. 2001. Nr 130. – poz. 1450. t.j. Dz. U. z 2013 r. poz. 262, 2014 r. poz. 1662, z 2015 r. poz. 1893.

13. Ustawa o świadczeniu usług drogą elektroniczną. 18 lipca 2002 r. // Dziennik Ustaw. 2002. Nr. 144. – poz. 1204. t.j. Dz. U. z 2016 r. poz. 1030, 1579.

14. Ustawa o zmianie ustawy – Kodeks cywilny oraz niektyrych innych ustaw. 14 lutego 2003 r. // Dziennik Ustaw. 2003. Nr. 49. – poz.408.

О.П. Печеный

ВЛИЯНИЕ ИНТЕРНЕТ-СРЕДЫ НА СДЕЛКИ О РАСПОРЯЖЕНИИ ИМУЩЕСТВОМ НА СЛУЧАЙ СМЕРТИ ФИЗИЧЕСКОГО ЛИЦА

Аннотация. *В статье анализируются особенности влияния цифровой среды на наследственные отношения. Освещены проблемы распоряжений на случай смерти и определения их форм. Затрагиваются проблемы распоряжения цифровыми активами на случай смерти. Проводится анализ действующего законодательства об электронной коммерции, соответствующих директив Европейского союза. Исследуется возможность использования электронной цифровой подписи в сфере наследования.*

Ключевые слова: *наследство, интернет-среда, наследственное право, электронная цифровая подпись.*

В настоящее время цифровые технологии дополняют, а порой и серьезно «теснят» классические гражданско-правовые формы. В глобальном аспекте речь идет не о единичных электронных сделках, а о виртуальной реальности, объединяющей традиционные гражданские правоотношения, обремененные «электронным» элементом, отношения по поводу объектов, создаваемых и функционирующих в виртуальном пространстве, отношения по поводу доступа в социальные сети. Виртуальная реальность заняла особое место в жизни современного человека – она является не только средой общения, глобальной системой поиска информации или информационной платформой нового уровня, она способна как отображать действительность, так и преображать ее[1].

Под влиянием виртуальной реальности в ином, «преображенном», виде перед нами предстают все социальные явления, включая и само право, и его отдельные институты. В свете этого перспективной задачей юридической науки должен стать анализ влияния виртуальной среды

[1] Цит. по: *Пожидаева И.* Симулякрность как основа манипулятивного дискурса блога: лингвофилософский аспект // Studia linguistica. 2012. Вып. 6 (2). С. 347.

на те или иные правовые явления, выявление изменения последних вследствие воздействия этой среды.

В отношении сделок и договоров, заключаемых с помощью электронных средств связи, необходимо определить их место в традиционной системе сделок, выявить их характерные черты и переосмыслить особенности их заключения и расторжения[1]. В отношении сферы наследственного права, включая распоряжения на случай смерти, часть из которых может быть отнесена к сделкам, следует концептуально определиться в части возможности их существования в электронной форме или составления с применением элементов цифровой среды. В настоящее момент в силу строго личного характера распоряжений на случай смерти однозначно положительный ответ вряд ли возможен.

При этом нельзя оставить без внимания и то, что под влиянием социально-демографических и иных факторов изменяется потребность общества в определенных механизмах наследственного права, включая квазинаследственные распоряжения на случай смерти. Е.Ю. Петров отмечает, что с ростом продолжительности жизни, со старением населения следует стимулировать дарения, учитываемые при разделе наследства, пожизненные ренты, прижизненные фонды и другие механизмы, позволяющие передавать имущество «авансом»[2]. Все указанные механизмы, включающие и распоряжения на случай смерти, могут формироваться под воздействием цифрового формата и элементов цифровой среды.

Сегодня существенное значение имеет вопрос о возможности физического лица распорядиться на случай смерти «*цифровыми активами*», под которыми мы понимаем определенную совокупность неимущественных благ, персональных данных, информацию о наследодателе (аккаунты, пароли доступа к социальным сетям, файлообменникам, электронным «кошелькам», банковским счетам и т.д.). В обычном, нотариально удостоверенном завещании такая информация в силу ее изменчивости и иных факторов вряд ли уместна.

В современной практике можно встретить различные подходы к решению проблемы завещательного распоряжения цифровыми активами.

---

[1] Харьковская цивилистическая школа: о договоре / И.В. Спасибо-Фатеева, О.П. Печеный, В.И. Крат и др.; под общ. ред. И.В. Спасибо-Фатеевой. Харьков: Право, 2017. С. 142.

[2] *Петров Е.* В защиту реформы наследственного права (https://zakon.ru/blog/2016/12/25/v_zaschitu_reformy_nasledstvennogo_prava).

Например, компания *Legacy Locker* в подтверждение регистрации пользователя на сайте компании и оплаты услуг предоставляет клиенту две клубные карты, одну из которых он может передать близкому человеку с тем, чтобы тот в случае смерти клиента мог связаться с администрацией сайта и получить доступ к цифровому наследству умершего.

Зарегистрированные пользователи социальной сети *Facebook* имеют возможность определить, кто будет управлять их страницей после смерти, что можно приравнять к распоряжению на случай смерти. Пользователю сети как наследодателю доступны три опции: автоматическое удаление аккаунта, превращение профиля в так называемую страницу памяти и завещание аккаунта конкретному лицу[1].

В обозначенных случаях по сути речь идет о распоряжении неимущественными благами физического лица на случай смерти, что в некоторой мере не согласуется с законодательными нормами (ч. 2 и 3 ст. 1112 ГК РФ; п. 1 ч. 1 ст. 1219 ГК Украины) и доктриной наследственного права, отрицающей возможность включения в состав наследства благ неимущественного характера. Но распоряжение «цифровыми активами» на случай смерти нуждается в теоретическом обосновании и законодательном закреплении, например, это может найти выражение в создании отдельного завещательного распоряжения «цифровыми активами», сходного с завещательным распоряжением вкладчика банку, другим финансовым распоряжением.

Регламентация всех групп отношений, формирующихся в виртуальном пространстве, в современных постсоветских государствах, в том числе и Украине, явно недостаточна, практика требует разработки работающих правовых моделей в этой сфере. С учетом потребностей оборота влияние цифровой среды ощущают классические гражданско-правовые формы.

Так, стороны нередко прибегают к технической фиксации порядка заключения обычной сделки, и, например, в нотариальной практике по соглашению сторон используется видеозапись процесса заключения и нотариального удостоверения сделки. Особенно это востребовано для завещаний, которые после смерти завещателя нередко становятся предметом судебных споров. Законодательство в этой части явно отстает, так как вовсе не регламентирует фиксацию процесса заключения

[1] *Степанов В.* Facebook разрешил пользователям завещать собственные аккаунты (https://tjournal.ru/p/fb-afterdeath).

и нотариального удостоверения завещания (равно, как и любой иной сделки). Этот пробел, безусловно, необходимо восполнить.

В развитие сказанного следует подчеркнуть, что и цифровая фиксация процесса совершения и нотариального удостоверения сделки должна получить доказательственное значение в суде, в частности, по делам о признании такой сделки недействительной. Использование цифровых технологий для подтверждения сделок в существующих формах должно стать одним из направлений влияния цифровой среды на традиционные гражданско-правовые отношения.

Другим направлением, которое также нуждается в более подробной регламентации, является *электронная коммерция*[1], обороты которой существенно растут и в европейских, и в национальных масштабах. Сейчас только в Германии оборот е-бизнеса составляет 21,5 млрд евро, а при ожидаемом годовом росте оборота более чем на 10% прогнозы продаж в течение следующих двух лет оцениваются в 28,4 млрд евро в год[2].

В странах Европейского союза вопросам электронной коммерции и ее законодательной регламентации уделяется значительное внимание. К примеру, в Германии в 2014 г. вступили в силу новые правила электронной коммерции, которые реализуют Директиву прав потребителей (Директива 2011/83/ЕС).

Особое внимание привлекает Директива 2000/31/ЕС Европейского парламента и Совета ЕС «О некоторых правовых аспектах информационных услуг на внутреннем рынке, в частности, об электронной коммерции (Директива об электронной коммерции)», на основании и с учетом положений которой был разработан и принят Закон Украины от 03.09.2015 № 675-VIII «Об электронной коммерции»[3] (далее – Закон об электронной коммерции). При этом отдельные положения указанного законодательного акта буквально и некритично воспроизводят Директиву, что нарушает сложившиеся подходы в технике нормотворчества и усложняет правоприменение.

---

[1] Считается, что электронная коммерция возникла в 60-е гг. XX в., когда было разрешено бронировать авиабилеты. В современных российских и украинских реалиях электронная коммерция востребована в первую очередь как средство экономии и оптимизации издержек бизнеса и потребителей в условиях кризиса.

[2] *Барабаш И.* Правила электронной коммерции в Германии // Сборник статей о праве Германии. Вып. № 1 (www.drjv.org).

[3] Проект Закона был внесен в парламент группой народных депутатов различной политической принадлежности в 2013 г., но стал законом только осенью 2015 г. и вступил в силу 30.09.2015.

Сфера действия Закона об электронной коммерции определена как *отношения в сфере электронной коммерции при совершении электронных сделок*. При этом еще в пояснительных документах к законопроекту была отмечена неточность терминологии, используемой в названии и тексте Закона. Так, поскольку Закон в целом направлен на регулирование электронной торговли, правильнее использовать термин «электронная торговля» вместо термина «электронная коммерция», который заимствован из Директивы 2000/31/ЕС. Законодательство об электронной коммерции предполагает более широкую сферу действия, которая охватывает не только торговлю с использованием интернет-ресурсов, но и предоставление услуг, возможность подключения к глобальным сетям и все другие виды деятельности, сделки в сфере которых в той или иной степени связаны с виртуальным пространством.

В Законе об электронной коммерции сформулированы определения ряда используемых в нем терминов, многие из которых достаточно размыты. Так, широко известное на бытовом уровне понятие «интернет-магазин» определяется как *средство* для предоставления или реализации товара, работы или услуги путем совершения электронной сделки. Однако сложно понять, что охватывается понятием «средство» – понимается под этим, к примеру, интернет-сайт или доменное имя и какова его правовая связь с продавцом или производителем товара.

Закон об электронной коммерции определяет сферы, на которые его действие не распространяется. В частности, он не применяется к сделкам, подлежащим нотариальному удостоверению и государственной регистрации, а также к сделкам, которые регулируют семейные правоотношения. Из смысла указанных положений Закона следует, что правила об электронной коммерции неприменимы к завещаниям и другим распоряжениям на случай смерти, хотя это не означает, что цифровая среда не влияет на сферу наследственного права в целом.

В первую очередь такое влияние может быть обусловлено использованием цифровой подписи и других идентификаторов субъектов наследственных правоотношений. При этом нельзя не учитывать, что идентификация в любом случае условна и не является стопроцентной. В исследованиях (К. Спирелли[1], Н.А. Дмитрик[2]) выделяют несколько

[1] *Spyrelli Christina*. Electronic Signatures: A Transatlantic Bridge? An EU and US Legal Approach Towards Electronic Authentication // The Journal of Information, Law and Technology. 2002. N 2. P. 7

[2] *Дмитрик Н.А.* Осуществление субъективных гражданских прав с использованием сети Интернет. М.: Волтерс Клувер, 2006. С. 108.

подходов к правовому регулированию использования электронных подписей, наиболее удачным из которых следует признать классификацию по «технологическому» критерию, в зависимости от способа создания цифровой подписи и ее юридического значения.

Называют три основных подхода к правовому регулированию использования электронных подписей:

(1) *минималистский* – признание правового значения электронных подписей и электронных документов путем устранения из законодательства норм, препятствующих их использованию; введение принципа «технологической нейтральности» — отсутствие привязки законодательства к какой-либо технологии формирования электронной подписи (например, Акт об электронных подписях США, 2000 г.);

(2) *максималистский* – признание преимущественно только электронных цифровых подписей, привязка к технологии открытого ключа, использование сертифицирующих центров и пр.;

(3) *смешанный* (представляет собой гибрид первых двух) – признание на законодательном уровне всех видов электронных подписей, как используемых, так и тех, которые возникнут в будущем.

При этом законодательством гарантируется определенный уровень документов, подписанных с помощью «усиленной» электронной подписи.

Как правило, усиленными являются подписи, использующие технологию открытого ключа. Электронная цифровая подпись может использоваться физическими лицами как аналог собственноручной подписи для предоставления электронному документу юридической силы. Юридическая сила электронного документа, подписанного электронной цифровой подписью, соответствует юридической силе документа на бумажном носителе, с собственноручной подписью управомоченного лица.

С технической точки зрения электронная цифровая подпись представляет собой результат хэш-функции, результат которой не повторяется для разных исходных данных, причем по ним исходную информацию восстановить нельзя. Можно сравнить хэш-функцию с архивированием, в результате чего получается краткая последовательность единиц информации (байт), с невозможностью восстановить исходные данные из такого «архива».

Отсюда следует, что использование электронной цифровой подписи как компьютерного файла, созданного в результате хэширования, доступно любому лицу, имеющему ключ к нему, а не только владельцу

электронной цифровой подписи. Это является основным препятствием к распространению и электронной цифровой подписи, и вообще цифровых форм на сферу наследственного права, предполагающих неразрывную связь с личностью субъектов. Нельзя отрицать того, что в ближайшем будущем техническая сторона электронной подписи будет усовершенствована, с доведением возможности идентификации ее владельца до максимума, что и обусловит дальнейшее открытие наследственно-правовых форм для интернет-среды.

Пристатейный библиографический список:

1. *Пожидаева И.* Симулякрность как основа манипулятивного дискурса блога: лингвофилософский аспект // Studia linguistica. 2012. Вып. 6 (2).

2. Харьковская цивилистическая школа: о договоре / И.В. Спасибо-Фатеева, О.П. Печеный, В.И. Крат и др.; под общ. ред. И.В. Спасибо-Фатеевой. Харьков: Право, 2017.

3. *Петров Е. В* защиту реформы наследственного права (https://zakon.ru/blog/2016/12/25/v_zaschitu_reformy_nasledstvennogo_prava).

4. *Степанов В.* Facebook разрешил пользователям завещать собственные аккаунты (https://tjournal.ru/p/fb-afterdeath).

5. *Барабаш И.* Правила электронной коммерции в Германии // Сборник статей о праве Германии. Вып. № 1 (www.drjv.org).

6. *Spyrelli Christina*. Electronic Signatures: A Transatlantic Bridge? An EU and US Legal Approach Towards Electronic Authentication // The Journal of Information, Law and Technology. 2002. N 2.

7. *Дмитрик Н.А.* Осуществление субъективных гражданских прав с использованием сети Интернет. М.: Волтерс Клувер, 2006.

О.В. Тимошенко

CLICK-WRAP И BROWSE-WRAP СОГЛАШЕНИЯ: НОВЫЙ УРОВЕНЬ ЭВОЛЮЦИИ ДОГОВОРНОГО ПРАВА В СЕТИ ИНТЕРНЕТ

Аннотация. *Данная статья посвящена анализу вопросов, связанных с правовой природой click-wrap и browse-wrap соглашений. Автор постаралась определить, являются ли эти соглашения договорами, каковы нюансы их совершения и какие проблемы могут возникнуть при создании текста подобных соглашений. Эти вопросы рассматриваются с учетом законодательства, доктрины и зарубежной судебной практики.*

Ключевые слова: *click-wrap соглашения, browse-wrap соглашения, Интернет, договор, пользователь, веб-сайт.*

1. Общая характеристика *click-wrap* и *browse-wrap* соглашений

Под *click-wrap* соглашением понимается соглашение, заключаемое в электронном виде посредством щелчка мышью одной из сторон по кнопке *I accept* («я согласен»), сопровождающей текст такого соглашения. Обычно оно содержит информацию о пределах разрешенного пользования, запрещает декомпиляцию или указывает на применяемый закон или юрисдикцию и т.д. Путем заключения *click-wrap* соглашений пользователь может создать учетную запись, загрузить программное обеспечение или выполнить онлайн-транзакцию и т.д.; владельцы сайтов, в свою очередь, предупреждают пользователя о том, что программное обеспечение защищено авторским правом, прямо отказываются от подразумеваемых гарантий и т.д.

Впервые действительность таких соглашений подтвердил суд США в деле *Hotmail Corp. v. Vans Money Pie, Inc.*[1], в котором подобное соглашение о порядке пользования почтовым ящиком на сайте *hotmail.com* было признано действительным. Договор, заключенный посредством

[1] No. C-98 JW PVT ENE, C98-20064JV, (N.D. Cal Apr. 1998).

щелчка мышью, имеет юридическую силу в Англии[1], Италии[2], Франции[3] и ряде других стран.

Ситуация, когда условия договора доступны для ознакомления по ссылке на веб-сайте, но от пользователя не требуется выражать согласие с его условиями в явной форме, подпадает под понятие *browse-wrap* соглашения[4]. В этом случае соглашение заключается самим фактом использования веб-сайта, на котором непосредственно размещены (например, внизу веб-страницы) гиперссылки на условия, на основании которых предлагается использование основной страницы, программы, онлайн-сервиса. Таким образом, пользователь соглашается с условиями, аналогичными положениям *click-wrap* соглашений (а также, например, с порядком представления заявлений о нарушении авторских прав, с запретом на коммерческое использование размещенной на сайте информации) поскольку просмотр или иное использование веб-сайта уже предполагает выражение согласия с этими условиями.

В обеспечении ознакомления пользователей с условиями *click-wrap* или *browses-wrap* соглашений заинтересован владелец сайта – он устанавливает правила и ограничения, фиксируя их в так называемом пользовательском соглашении. Например, условия пользовательского соглашения веб-сайта *eBay* содержат пояснение: «eBay не является традиционным организатором аукциона». Это объясняется так: «eBay – это торговая площадка, дающая пользователям возможность предлагать, продавать и покупать практически любые товары в самых разных местах и форматах цены. Фактический договор продажи заключается непосредственно между продавцом и покупателем».

2. Правовая характеристика *click-wrap* и *browse-wrap* соглашений

В доктрине *click-wrap* и *browse-wrap* соглашения без каких-либо оговорок признаются договорами, в том смысле, в котором его понимает

[1] *Reed C., Angel J.* Computer Law: The Law and Regulation of Information Technology. Oxford University Press. 2007. P. 106. В английской доктрине часто обсуждается дело *Beta Computers* (*Europe*) *Ltd v. Adobe Systems* (*Europe*) *Ltd* (1996. S.L.T. 604).

[2] Giudicedi pace di Partanna n. 15/2002, case N 206/2001 R.G.A.C. (http://www.ricer-agiuridica.com/sentenze/index.php?num=868).

[3] См. ст. 1369-4, 1369-5 ФГК, посвященные процессу заключения договора в электронной форме (введены в действие Ордонансом от 16.06.2005 № 2005-674).

[4] А.И. Савельев говорит о «концепции *browse-wrap*» (*Савельев А.И.* Электронная коммерция в России и за рубежом: правовое регулирование: учеб. пособие. М.: Статут, 2014. С. 117).

и российское гражданское право (п. 1 ст. 420 ГК РФ «Договором признается соглашение двух или нескольких лиц об установлении, изменении или прекращении гражданских прав и обязанностей»). Иногда их относят к договорам *sui generis*[1], а зачастую совсем не квалифицируют, ограничиваясь лишь указанием на их договорную сущность[2].

Попробуем дать правовую характеристику рассматриваемым соглашениям.

Даже при поверхностном анализе *click-wrap* и *browse-wrap* соглашений становится очевидно, что они обычно являются безвозмездными: в случае с *click-wrap* соглашениями после нажатия пользователем кнопки «я согласен» он без взимания какой-либо платы или иного предоставления получает доступ к пользованию веб-страницей; в случае с *browse-wrap* соглашениями для пользования веб-сайтом не требуется даже предварительного согласия. Можно ли признать рассматриваемые соглашения реальными, учитывая, что они возникают с момента получения пользователем доступа к пользованию веб-сайтом (веб-страницей)?

По всей видимости, *click-wrap* и *browse-wrap* соглашения нельзя причислить к группе безвозмездных договоров, в число которых входят договоры дарения и безвозмездного пользования имуществом. Это связано с тем, что объектом и договора дарения[3], и договора безвозмездного пользования (договора ссуды)[4] является вещь – материальный предмет. Между тем пользование веб-сайтом (даже с учетом возможного извлечения пользователем его полезных свойств в самых различных формах – изучение контента, копирование информации, распространение данных и т.д.) не может пониматься как пользование вещью.

---

[1] См.: *Савельев А.И.* Электронная коммерция в России и за рубежом: правовое регулирование. С. 2.

[2] См.: *Гаврилов Э.П.* Какие изменения предлагается внести в главу 70 ГК РФ «Авторское право»? // Патенты и лицензии. 2012. № 1; *Samons M.* Click-Wrap Agreement Held Enforceable // N.Y.L.J. 1998; *Lim Y.F.* Cyberspace law Commentaries and Materials, 2nd ed. Oxford, 2007.

[3] По договору дарения одна сторона (даритель) безвозмездно передает или обязуется передать другой стороне (одаряемому) вещь в собственность (п. 1 ст. 572 ГК РФ).

[4] По договору безвозмездного пользования (договору ссуды) одна сторона (ссудодатель) обязуется передать или передает вещь в безвозмездное временное пользование другой стороне (ссудополучателю), а последняя обязуется вернуть ту же вещь в том состоянии, в каком она ее получила, с учетом нормального износа или в состоянии, обусловленном договором (п. 1 ст. 689 ГК РФ).

Можно ли признать рассматриваемые соглашения реальными, учитывая, что они возникают с момента получения пользователем доступа к пользованию веб-сайтом (веб-страницей)? Думается, что положительный ответ на этот вопрос будет обоснованным. Пользователь и собственник веб-страницы не просто приобретают права и обязанности одномоментно с тем, как пользователь нажимает клавишу «я согласен», но в целом смысл такого договора состоит в получении пользователем доступа к веб-странице в момент достижения согласия сторонами.

Развивая сказанное, следует уделить внимание предложению А. Абдуджалилова о необходимости введения в обязательственное право понятия «безвозмездное оказание услуг» именно по отношению к договорам в сети Интернет[1]. Названный автор, в частности. написал: «Определение обязательства по безвозмездному оказанию услуг в Интернете формулируется как гражданское правоотношение в виртуальном пространстве Интернета, в силу которого одно лицо – пользователь имеет право требовать от другого лица – компании совершения какого-либо действия (предоставления услуг), а компания имеет право требовать от пользователя совершения определенного действия (регистрации) и воздержания от совершения какого-либо действия, противоречащего общей концепции компании»[2].

По нашему мнению, данная идея имеет право на существование. В ее подтверждение можно привести следующий пример. Компания *Uber* предоставляет услуги по договору, который можно квалифицировать как близкий к агентскому договору. На веб-сайте компании *uber.com* есть ссылка на «Условия и положения», в которых содержатся условия договорных отношений, и «Общая концепция компании», содержащая требования, соблюдение которых компания может потребовать от пользователя; пользователь, в свою очередь, получает доступ к услугам, предоставляемым *Uber*'ом.

В то же время нельзя не учитывать, что не всегда на веб-сайтах предоставляются какие-либо услуги. Примером могут служить различные

[1] Возможность заключения безвозмездного договора оказания услуг подтверждается судебной практикой (см.: постановление ФАС Уральского округа от 19.10.2010 № Ф09-8056/10-С5 по делу № А50-331/2010; определение ВАС РФ от 16.07.2010 № ВАС-9448/10 по делу № А50-20807/2009)

[2] *Абдуджалилов А.* Правовая характеристика договоров, заключаемых в Интернете // Журнал российского права. 2016. № 2. С. 81. В своей работе А. Абдуджалилов определяет такие договоры, как консенсуальные.

веб-страницы, на которых правообладатель результатов интеллектуальной собственности размещает авторские произведения, базы данных и пр. В этом случае действия пользователя, получившего доступ к веб-сайту, подчиняются уже положениям не только обязательственного права, но и законодательства об интеллектуальной собственности (часть четвертая ГК РФ). Следовательно, предложенная А. Абдуджалиловым конструкция «безвозмездного оказания услуг» будет работать не во всех случаях.

Нельзя принять точку зрения и тех авторов, которые считают *click-wrap* и *browse-wrap*-соглашения договорами *sui generis*. Например, А.И. Савельев, относящий рассматриваемые соглашения к договорам *sui generis*, определяет их так: «Под click-wrap-соглашением понимается соглашение, заключаемое в электронном виде посредством щелчка мышью одной из сторон по клавише «я согласен», сопровождающей текст такого соглашения», «Browse-wrap-соглашения, принимаемые путем просмотра веб-сайта»[1]. Но анализ этих определений позволяет заключить, что речь идет не об особом виде договора, а об ином способе его заключения. И здесь следует вспомнить очень точное замечание А.В. Зажигалкина: «Особый вид контракта определяется его предметом, а не методом заключения»[2].

С учетом изложенного можно сделать вывод, что сущность *click-wrap* и *browse-wrap*-соглашения выражается в новом способе его заключения – в электронной форме. Одна из сторон – владелец сайта формулирует условия, а пользователь принимает эти условия целиком соответственно путем клика или просмотра веб-страницы с гиперссылкой на условия соглашения.

3. Проблемы заключения *click-wrap* и *browse-wrap* соглашений

Российское право не содержит специальных положений, посвященных *click-wrap* и *browse-wrap* соглашениям – они подчиняются общим положениям о порядке заключения договоров.

Рассматриваемые соглашения имеют все существенные признаки договора присоединения (ст. 428 ГК РФ): владелец веб-сайта определяет положения договора, к которому пользователь присоединяется,

[1] *Савельев А.И.* Электронная коммерция в России и за рубежом: правовое регулирование. С. 184.

[2] *Зажигалкин А.В.* Международно-правовое регулирование электронной торговли: дис. ... канд. юрид. наук. СПб., 2005. С. 126.

выражая свое согласие со всеми условиями договора. Преимущества договора присоединения проявляются и здесь: вместо того, чтобы обременять себя, заключая каждый раз договор с индивидуальными условиями для каждого пользователя, компании – владельцы сайта – создают единое для всех соглашение, к которому любой пользователь может «присоединиться».

Click-wrap и *browse-wrap*-соглашения удобны и для пользователей, предпочитающих простоту и оперативность при использовании Интернета и не желающих тратить время и усилия на согласование условий использования веб-сайтов[1]. Таким образом, условия *click-wrap*- и *browse-wrap*-соглашений редко становятся предметом реального изучения со стороны пользователей. Например, согласно исследованию, проведенному в США, среднестатистический американец должен затратить приблизительно 201 час, в стоимостном выражении составляющих в среднем 3534 долл., на одно только чтение политики конфиденциальности, размещенных на веб-сайтах, которые он посещает[2].

В связи с этим актуальным становится вопрос о равенстве возможностей сторон такого договора – владельца веб-сайта и пользователя. Этот вопрос возникает в связи с тем, что потребитель, как правило, является слабой стороной по отношению к владельцу веб-сайта, в качестве которого в большинстве случаев выступает лицо, профессионально занимающееся предпринимательской деятельностью. Владелец веб-сайта, действуя в собственных интересах, может использовать недобросовестные приемы (мелкий шрифт, чрезмерно длинные предложения, узкоспециальные термины и т.д.) или расположить кнопку «я согласен» в начале текста соглашения, что исключит разумную возможность предварительного ознакомления пользователя с условиями. Также есть риск, что владелец сайта закрепит за собой право на одностороннее изменение условий договора, исключит для пользователя возможность отказаться от совершения сделки и др.

В качестве возражений против юридической силы *click-wrap* соглашений указывают и на неопределенность субъектного состава

[1] Toedt III D.C. Browse-wrap agreements for Web site terms of service might or might not be enforceable [Electronic resource] (URL:http://www.oncontracts.com/browse-wrap-agreement-enforceability).

[2] См.: *McDonald M., Cranor L.* The Cost of Reading Privacy Policies // A Journal of Law and Policy. 2008. N 540. P. 562.

такого договора (личности контрагента), да и самой информации о факте заключения договора[1]. Но как показывает анализ гражданского законодательства, названный недостаток не является чем-то принципиально новым – существуют договоры, которые считаются заключенными и юридически действительными и в отсутствие такой явно выраженной определенности: купля-продажа товаров с использованием автоматов; договоры дистанционной купли-продажи товаров и т.д. При возникновении необходимости есть возможность установить компанию – владельца сайта. Хотя нельзя не согласиться с существованием проблемы с установлением личности контрагента – пользователя: в сети Интернет он может указать не свое настоящее имя, а использовать псевдонимом (*nickname*), действовать анонимно или не быть дееспособным на заключение сделок. Таким образом, в виртуальном пространстве практически нельзя достоверно определить субъекта права, за исключением случаев его прямого волеизъявления, выраженного в электронной подписи, или сущности конкретных отношений[2].

Безусловно, круг проблем, возникающих при использовании рассматриваемых соглашений, не ограничивается вышеперечисленными. Для преодоления этих и иных проблем применительно *click-wrap*-соглашениям А.И. Савельев предлагает соблюдать следующие правила:

– пользователю должна быть обеспечена возможность предварительного ознакомления с условиями такого договора до того момента, как договор будет считаться заключенным;

– пользователь должен иметь возможность отказаться от принятия его условий и от совершения сделки;

– 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;

– должна быть предусмотрена обязанность обеспечивать наличие специальных средств для исправления ошибок, допущенных при вводе;

– должна быть обеспечена возможность распечатать и сохранить соглашение;

---

[1] *Витко В.С.* Гражданско-правовая природа лицензионного договора. М.: Статут, 2011. С. 290.

[2] *Дашян М.С.* Право информационных магистралей. Law of InformationHighways // Вопросы правового регулирования в сфере Интернет. 2007.

– должно быть надлежащее уведомление о любых изменениях условий договора[1].

Подобные выводы сформированы зарубежной судебной практикой.

Так, одним из решений, наиболее часто упоминаемым при рассмотрении вопросов, связанных с юридической силой *click-wrap*-соглашений, является решение по делу *Caspi v. Microsoft Network LLC*[2]. По мнению суда, существенных различий между условиями на бумажном носителе и на электронном носителе нет, а у пользователей есть потенциальная возможность предварительно ознакомиться с условиями договора.

Примечательно, что для подтверждения согласия некоторые владельцы веб-сайтов стали использовать «двойное подтверждение». Так, при рассмотрении дела о признании действительным *click-wrap* соглашения американский суд пришел к выводу, что если правообладатель веб-сайта предусмотрел двойное подтверждение условий соглашения, то пользователь не может «жаловаться, что он не видел, не читал и т.д.», поскольку он «фактически «подписал» соглашение путем нажатия клавиши «я согласен» не один, а два раза»[3].

Что касается заключения *browse-wrap* соглашений, то здесь для владельца сайта усложняется доказывание того факта, что пользователь ознакомился с условиями соглашения до начала использования веб-страницы и согласился с ними. Это связано с тем, что стандартное поведение, характерное для большинства пользователей, – как можно скорее перейти к странице с интересующим их контентом, не «тратя время» на ознакомление с условиями, на которые сделана ссылка мелким шрифтом где-то внизу сайта.

Американские суды при рассмотрении дел с конструкцией *browse-wrap*-соглашения отмечали, что ссылка на условия договора, которая располагается внизу страницы сайта, является неочевидным фактом для посетителя, и он не может считаться связанным подобным до-

[1] *Савельев А.И.* Электронная коммерция в России и за рубежом: правовое регулирование. С. 115–116, 148. Что касается *browse-wrap*-соглашений, то А.И. Савельев ограничивается лишь указанием на то, что если веб-сайт обладает коммерческой ценностью, то предпринимателям лучше предусмотреть заключение такого соглашения в форме *click-wrap* (см. там же. С. 121).

[2] 732 A.2d 528, 529 (N.J. Super. Ct. App. Div. 1999).

[3] Groff v. America Online, Inc., File No. C. A. No. PC 97-0331, 1998 W L 307001 (RI Superior Court, May 27, 1998).

говором[1]. Более того, американские суды говорят о недействительности подобных соглашений, если кнопка «ознакомьтесь и примите лицензионные условия использования программы до ее загрузки и использования» расположена на экране ниже кнопки «загрузить» и требует прокручивания страницы[2]. Аналогичные решения можно найти и в практике немецких судов[3].

Примечательно, что американский суд признает юридическую силу *browse-wrap*-соглашений в том случае, если на сайте есть заметная синяя гиперссылка, содержащая условия соглашения. В одном из таких дел суд сослался на визуальный эффект, подразумевая, что разумное лицо должно было обратить внимание на синюю гиперссылку: человек при использовании компьютера быстро узнает, что больше информации можно получить, нажав именно на нее[4].

Признание юридической силы за *browse-wrap* соглашениями встречается в практике судов Канады[5] и Голландии[6], где особый статус пользователя (предпринимателя или профессионала в сфере использования интернет-контента) подразумевает, что те знают о существовании ссылок на условия использования основной веб-страницы, и следовательно, обязаны ознакомиться с ними. В подобных случаях в обоснование решений суда идут ссылки 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[7].

Уникальным является решение американского суда по делу *Register.com, Inc. v. Verio, Inc.*[8]. Проблема заключалась в том, что условия предоставления сервиса появлялись уже после того, как запрос был сделан и данные получены. Ответчик многократно (систематически) использовал данный сервис, и условия *browse-wrap* соглашения были ему

[1] 54 USPQ 2d 1344 (C.D. Cal. 2000).

[2] 150 F. Supp. 2d 585 (SDNY 2001).

[3] Oberlandesgericht Hamburg. N 3 U 168/00. 13.06.2002.

[4] Hubbert v. Dell Corp., 835 N.E. 2d 113 (Ill. App. Ct. 2005).

[5] The Canadian Real Estate Association v. Sutton Real Estate Services Inc., (Québec) Québec. Netwise v. NTS Computers.

[6] 5 December 2002. Computerrecht 2003/02. P. 149.

[7] *Савельев А.И.* Электронная коммерция в России и за рубежом: правовое регулирование. С. 121.

[8] 356 F.3d 393 (nd 2 Cir. 2004).

известны уже после первого запроса. Это, по мнению суда, позволяло говорить о возникновении обязательств между истцом и ответчиком, возникших из *browse-wrap*-соглашения.

Заключение

По нашему мнению, обеспечит защиту прав обеих сторон соблюдение следующих правил:

1. Условия соглашения должны быть приемлемы, исполнимы и справедливы. Эти требования обусловливаются прежде всего тем, что *click-wrap*- и *browse-wrap*-соглашения заключаются по модели договора присоединения. Следовательно, предлагающей соглашение стороне (владельцу веб-сайта) нужно учитывать, что в соответствии с п. 2 ст. 428 ГК РФ пользователь может потребовать расторжения или изменения соглашения, если оно хотя и не противоречит закону и иным правовым актам, но лишает пользователя прав, обычно предоставляемых по соглашениям такого вида, исключает или ограничивает ответственность владельца сайта за нарушение обязательств либо содержит другие явно обременительные для пользователя условия, которые он исходя из своих разумно понимаемых интересов не принял бы при наличии у него возможности участвовать в определении условий соглашения.

2. При разработке текстов *click-wrap*- и *browse-wrap*-соглашений следует использовать максимально четкие и ясные формулировки, которые позволят сделать эти соглашения простыми и доступными для понимания пользователями.

3. Особый акцент необходимо сделать на отношении размещения кнопки «я согласен» или гиперссылки на условия соглашения. Применительно к *click-wra*- соглашениям: необходимо располагать клавишу «я согласен» в конце текста такого соглашения, чтоб не исключать разумную возможность предварительного ознакомления пользователя с условиями (но не ниже, чем, например, клавиша «загрузить», чтобы не требовалось прокручивание страницы). Применительно к *browse-wrap* соглашениям: размещение «Условий использования» или «Политики конфиденциальности» и др. должно отображаться на видном месте, а не по краям веб-страницы, сверху или снизу, причем гиперссылки должны выделяться, быть яркими (желательно синими, поскольку, как указывалось выше, разумный пользователь понимает, что больше информации можно получить, нажав на синюю гиперссылку).

Изложенное в случае судебного спора повысит шансы на признание юридически действительным заключенного соглашения, позволит защитить сторону, права которой были нарушены.

Завершая настоящую статью, хотелось бы отметить, что в отличие от весьма подробно регламентируемых правом договоров реального мира – купли-продажи. поставки, аренды и т.п., договоры, заключаемые в сети Интернет, находятся только в начале пути. При этом если *click-wrap* соглашения хотя и порождают немало вопросов, но в целом вписываются в концепцию договорного права, то *browse-wrap* соглашения являются куда более дискуссионным правовым явлением.

С учетом этого использование позитивного опыта тех стран, в которых уже достаточно развито регулирование *e-commerce*, позволит эффективно решать вопросы, возникающие в связи с заключением *click-wrap*- и *browse-wrap* соглашений. Но нужно учитывать, что действенность законодательных формулировок, используемых в США и в европейских странах в сфере интернет-пространства, обусловливается длительным социально-экономическим развитием и правоприменительной практикой. Поэтому, как отмечается многими учеными, заимствование зарубежных правовых институтов, хотя доказавших свою эффективность на практике, требует критического осмысления и тщательной проработки при введении в отечественное право.

Пристатейный библиографический список:

1. *Савельев А.И.* Электронная коммерция в России и за рубежом: правовое регулирование: учеб. пособие. М.: Статут, 2014.

2. *Гаврилов Э.П.* Какие изменения предлагается внести в главу 70 ГК РФ «Авторское право»? // Патенты и лицензии. 2012. № 1.

3. *Samons M.* Click-Wrap Agreement Held Enforceable // N.Y.L.J. 1998, *Lim Y.F.* Cyberspace law Commentaries and Materials, 2nd ed, Oxford, 2007.

4. *Абдуджалилов А.* Правовая характеристика договоров, заключаемых в Интернете // Журнал российского права. 2016. № 2.

5. *Зажигалкин А.В.* Международно-правовое регулирование электронной торговли: дис. ... канд. юрид. наук. СПб., 2005.

6. Toedt III D.C. Browse-wrap agreements for Web site terms of service might or might not be enforceable (URL:http://www.oncontracts.com/browse-wrap-agreement-enforceability).

7. *McDonald M., Cranor L.* The Cost of Reading Privacy Policies // A Journal of Law and Policy. 2008. N 540.

8. *Витко В.С.* Гражданско-правовая природа лицензионного договора. М.: Статут, 2011.

9. *Дашян М.С.* Право информационных магистралей. Law of Information Highways // Вопросы правового регулирования в сфере Интернет. 2007.

М.Е. Черемисинова

СОЦИАЛЬНАЯ ИНТЕРНЕТ-СЕТЬ В КАЧЕСТВЕ СУБЪЕКТА ПРАВООТНОШЕНИЙ

Аннотация. *Статья посвящена правовым аспектам формирования правового статуса участников социальных интернет-сетей, а также владельцев интернет-ресурсов. Выявляются потенциальные правовые риски, сопутствующие использованию интернет-сетей. Социальная интернет-сеть рассматривается как сложная общественная структура, являющаяся предметом исследования философской, социальной и правовой науки. Такой подход позволяет вести поиск средств правового регулирования отношений, складывающихся при использовании социальных интернет-сетей, с учетом социальной обусловленности правовых механизмов, технологической, пространственной специфики самих ресурсов.*

Ключевые слова: *социальная интернет-сеть, правовой статус участников, саморегулирование, пользовательское соглашение, ограничения прав субъектов интернет-отношений.*

Выбор темы обусловлен популярностью социальных интернет-сетей, их стремительным распространением, а также включенностью в общественные, политические и международные процессы. Немаловажны в связи с этим и прогнозы относительно развития Интернета в целом: в частности, существует мнение, что изменения Глобальной сети будут происходить в направлении формирования «Гигантского глобального графа»[1] (*GGG*), который придет на смену Всемирной паутине (*WWW*). Такой граф (сеть) в отличие от сети, объединяющей компьютеры и документы, соединит между собой людей и, основываясь на семантических технологиях, предоставит пользователям сервисы более высокого класса[2].

[1] Понятие «граф» в математике используется для обозначения сети (подробнее об этом см.: *Губанов Д.А., Новиков Д.А., Чхартишвили А.Г.* Социальные сети: модели информационного влияния, управления и противоборства. М., 2010).

[2] *Тихомиров А.А., Труфанов А.И.* Сверхсложные сети: новые модели интерпретации социально-экономических и биосоциальных процессов // Труды Института государства и права Российской академии наук. 2011. № 6.

1. В социологической науке еще до появления Интернета социальные сети изучались как взаимосвязи между людьми. Причем в социальной философии понятие «социальная сеть» имеет несколько значений.

О социальных отношениях, обладающих сетевой структурой, писал еще в 1903 г. Г. Зиммель, анализируя процессы влияния урбанизации на формообразования различных типов взаимодействия между людьми[1]. В это же время Г. Спенсер выдвинул схожую теорию социального взаимодействия[2]. В 1930-х гг. Я. Морено использовал понятие «социальная сеть» для обозначения групповых отношений[3]. Этот термин был закреплен в 1954 г. социологом Дж. Барнсом в работе «Классы и собрания в норвежском островном приходе»[4] – исследователь использовал это понятие для обозначения типов связей, возникающих в малых группах (племенах, семьях), и социальных категорий (например, пол, этническая принадлежность). На сегодняшний день социальные сети принято понимать как нерегулируемые социальные структуры[5].

В виртуальной среде процесс формирования социальных сетей подчинен несколько иным правилам, поэтому вопрос об их правовом регулировании может быть рассмотрен при помощи анализа механизмов присоединения к этим сетям пользователей (и граждан, и организаций). Учитывая, что в дальнейшем анализу будут подвергнуты только социальные интернет-сети, для их обозначения будет использоваться привычное сокращение «соцсети».

2. Прежде всего рассмотрения требует вопрос о соотношении содержания понятий соцсети и ее сайта.

Законодательное определение понятия сайта содержится в Законе об информации – под ним понимается «совокупность программ для электронных вычислительных машин и иной информации, содержащейся в информационной системе, доступ к которой обеспечивается посредством информационно-телекоммуникационной сети «Интернет» по доменным именам и (или) по сетевым адресам, позволяющим идентифицировать сайты в сети «Интернет»». Ключевые моменты в этом определении – (1) содержание (информация); (2) технические

[1] *Зиммель Г.* Большие города и духовная жизнь // Логос. 2002. № 3, 4. С. 20–27.

[2] *Спенсер Г.* Личность и государство. Челябинск, 2007. С. 39–44.

[3] *Морено Я.* Социометрия: Экспериментальный метод и наука об обществе. М., 2001.

[4] *Barnes J.* Class and Committees in a Norwegian Island Parish // Human Relations. 1954. P. 11–17.

[5] *Boyd D.M., Ellison N.B.* Social Network Sites: Definition, History, and Scholarship / Danah M. Boyd, Nicole B. Ellison // Journal of Computer-Mediated Communication. 2008. N 13.

(программные) средства; (3) наличие доменного имени и (или) (4) сетевого адреса[1].

Для выявления содержания такого сложного общественного явления, как соцсеть, придется опираться на другие понятия. Среди них:

1) владелец сайта соцсети – как правило, им является юридическое лицо, предлагающее определенный набор телекоммуникационных сервисов неограниченному кругу лиц. От имени этого юридического лица выступает администрация соцсети;

2) пользователи соцсети, связанные «виртуальными» общественными отношениями[2];

3) собственно технологическая платформа, предоставляющая возможность информационного обмена, ведения бизнеса, развития маркетинга, формирования общественных объединений, отдыха и развлечения и т.д.

Сказанное со всей очевидностью демонстрирует то, что сайт соцсети и сама соцсеть – явления, не совпадающие, хотя и взаимообусловленные.

Примечателен тот факт, что сайт соцсети создается для осуществления взаимодействия его пользователей. Но другие сайты, несмотря на предоставление пользователям возможности выразить собственное мнение, характеризуются обычно односторонней подачей информации – основную тематику формирует владелец сайта (или разработчик). Вследствие этого блокирование «обычного» сайта без судебного постановления[3] может ограничить информационные права определенного числа пользователей. Блокирование же соцсети

[1] В законодательстве иногда встречается термин «интернет-ресурс», понятие которого не раскрывается (см., например: Указ Президента РФ от 12.05.2009 № 537 «О Стратегии национальной безопасности Российской Федерации до 2020 года», постановление Правительства РФ от 07.02.2011 № 61 «О Федеральной целевой программе развития образования на 2011–2015 годы»). Этот термин широко используется в нормативных правовых актах различных ведомств.

[2] Соцсеть рассматривают как разновидность сверхсложных связей, которая, по мнению некоторых авторов, удачно интерпретирует социальные явления, в том числе человеческие отношения, «расслаивая их на необходимый спектр формальных и неформальных компонент, и может послужить основой для дальнейшего детального описания, анализа и подготовки управляющих решений с учетом неоднородности элементов и связей изучаемых систем» (*Тихомиров А.А., Труфанов А.И.* Указ. соч. С. 169).

[3] ФЗ от 28.12.2013 № 398-ФЗ «О внесении изменений в Федеральный закон «Об информации, информационных технологиях и о защите информации»» предполагает взаимодействие провайдера хостинга (или иного лица, обеспечивающего размещение в сети Интернет, информационного ресурса, содержащего противоправную информа-

приведет помимо ограничения информационных прав к парализации огромного числа межперсональных, деловых, образовательных и иных отношений.

Еще один аспект функционирования такого явления, как соцсеть, – это присутствие у сайта сети признаков средства массовой информации, что признается исследователями философской науки и журналистских кругов.

Первоначальным предназначением интернет-сервисов соцсетей, по мнению Л.А. Браславец, было установление связей между пользователями, а также публикация информации. Вместе с тем информация, публикуемая пользователями в соцсетях, в достаточно короткие сроки вышла за рамки личностно ориентированной, например в освещении терактов в Нью-Йорке 11.09.2001 пользователи соцсетей приняли активнейшее участие. В настоящее время практически каждое общественно значимое событие находит отклик в публикациях, размещаемых в соцсетях – это явление получило у западных исследователей название «гражданская журналистика»[1].

В исследовании, проведенном А.М. Лещенко, утверждается, что «социальные сети сопоставимы в современной социокультурной ситуации со средствами массовой коммуникации, так как они выполняют все функции средств массовых коммуникаций»[2].

цию) с владельцем ресурса для оперативного удаления противоправного контента и восстановление работы сайта при содействии владельца ресурса.

[1] *Браславец Л.А.* Интернет-сервисы социальных сетей в современной системе средств массовой информации. Воронеж, 2010.

[2] Автор пишет: «По критерию периодичности, доступности, финансовому критерию сетевая коммуникация является наиболее эффективной в современном коммуникативном пространстве. Традиционные средства массовой коммуникации выступают в качестве центров, сначала аккумулирующих информацию, затем ее сортирующих и распространяющих. Социальные сети характеризуются потенциально бесконечным числом независимых центров аккумуляции и распространения информации, что определяет ее глобальность, демократичность, но и бесконтрольность. Эти характеристики закладывают новые смысловые конструкты в организации коммуникативного пространства современного общества» (*Лещенко А.М.* Социальные сети как механизм конструирования коммуникации в современном обществе: автореф. дис. ... канд. филос. наук. Пятигорск, 2011). Автор в своей работе использует термин «средства массовой коммуникации», который хотя и не определен точно на законодательном уровне, содержится во многих нормативных правовых актах (например, в Законе об информации, информационных технологиях и о защите информации», ФЗ от 29.12.1994 № 77-ФЗ «Об обязательном экземпляре документов», Указе Президента РФ от 12.03.2007 № 320 «О Федеральной службе по надзору в сфере массовых коммуникаций, связи и охраны культурного наследия») и сопутствует термину «средства массовой информации».

По мнению Л.К. Терещенко, имеются определенные основания для применения понятия «средства массовой информации» к интернет-сайтам (под которыми понимаются и, безусловно, и сайты соцсетей). Однако, на ее взгляд, большая часть сайтов слабо «вписывается» в законодательство о средствах массовой информации. И это, несмотря на то, что в 2011 г. в Закон РФ от 27.12.1991 № 2124-I «О средствах массовой информации» были внесены изменения: в него было введено понятие «сетевое издание», под которым понимается сайт в сети Интернет, зарегистрированный в качестве средства массовой информации[1].

Таким образом, сайт соцсети (но, бесспорно, не сама соцсеть) может быть отнесен к средствам массовой информации при соблюдении условия о регистрации (добровольной) в качестве сетевого издания.

3. Первый шаг для присоединения к соцсети – это регистрация пользователя.

Наиболее популярные соцсети (такие как *Facebook*, «ВКонтакте», *Linkedin*) требуют при регистрации указания достоверных сведений о пользователе – на ресурсах, старающихся поддерживать свою репутацию, анонимность не приветствуется, а иногда и прямо запрещается. Вопросы персональных данных и компетентного суда, на рассмотрение которого могут быть переданы возникающие споры, решаются в пользовательских соглашениях по-разному.

Например, в пользовательском соглашении *Facebook* предусмотрен пункт, в соответствии с которым пользователь сети предоставляет владельцам ресурса неэксклюзивную, подлежащую переводу, безвозмездную международную лицензию на использование своего *IP*-контента, который он размещает или создает с помощью *Facebook*. Этот пункт позволяет соцсети транслировать в другие профили или на сторонние сайты, интегрировавшие так называемый социальный плагин (*like*), все фото, видео, обновления статусов и т.д. При этом пользователь сети соглашается с тем, что его персональная информация будет перенаправлена в США и обработана там, и эти персональные данные выходят из-под юрисдикции государства, в котором проживает пользователь. В то же время любые претензии или споры, возникающие в результате действия пользовательского соглашения или в связи с ним либо с *Facebook*, будут разрешаться исключительно в Окружном суде США Северного округа штата Калифорния или

[1] *Терещенко Л.К.* Модернизация информационных отношений и информационного законодательства: монография / Ин-т законодательства и сравнительного правоведения при Правительстве РФ. М., 2013. С. 183–184.

в федеральном суде, находящемся в округе Сан-Матео. Кроме того, регистрируясь в *Facebook,* пользователь дает свое согласие на подчинение индивидуальной юрисдикции указанных судов для проведения судебных разбирательств по всем претензиям. Действие соглашения, а также любые претензии, которые могут возникнуть между пользователем и соцсетью, регулируются законами штата Калифорния без учета коллизионных норм законодательства[1].

В соответствии с пользовательским соглашением *LinkedIn* пользователь соцсети предоставляет информацию на свой страх и риск и сам несет ответственность за достоверность и актуальность сведений, указанных в своем профиле. Место рассмотрения судебных дел, к участию в которых может быть привлечена администрация *LinkedIn*, – Северная Ирландия.

В пользовательском соглашении «ВКонтакте» устанавливается, что все споры, стороной в которых выступит администрация сайта, рассматриваются по законодательству Российской Федерации.

Правомерность подобных условий пользовательского соглашения вызывает обоснованные сомнения у тех пользователей соцсетей, для которых затруднительно найти возможность принять участие в судебном разбирательстве за пределами своей страны, так как «среднестатистическому гражданину это явно не под силу» (причем не только в России, но и в странах Европы).

Помимо указанного в некоторых пользовательских соглашениях есть условие, оговаривающее возраст пользователя (физического лица). Например, в пользовательском соглашении «ВКонтакте» установлено, что пользователем этой соцсети может выступать физическое лицо, достигшее возраста, допустимого для акцепта этих правил и обладающее соответствующими полномочиями. А в *LinkedIn* возраст пользователей четко определен[2].

Не затрагивая всех тонкостей пользовательского соглашения (многие условия которого вызывают серьезные возражения), можно

[1] URL: https://ru-ru.facebook.com/legal/terms

[2] Минимальный возраст равен (a) 18 годам для граждан Китайской Народной Республики, (b) 16 годам для граждан Нидерландов, (c) 14 годам для граждан США, Канады, Германии, Испании, Австралии и Южной Кореи и (d) 13 годам для граждан всех остальных стран. Однако если в законе указано, что для предоставления компанией *LinkedIn* услуг (в том числе при сборе, хранении и использовании информации в соответствии с политикой конфиденциальности) участник должен быть старше указанного возраста, тогда в качестве минимального возраста должен использоваться возраст, указанный в законе. Услуги не предназначены для предоставления детям младше 13 лет.

заключить, что присоединение к соцсети возможно только при соблюдении пользователем четко обозначенных требований владельца сайта соцсети.

4. Итак, с пользователем соцсети заключается соглашение, которое может рассматриваться как договор присоединения (например, в договоре соцсети «ВКонтакте» это четко установлено), в соответствии с условиями этого соглашения в обмен на личную информацию пользователю предлагается набор сервисов.

Надо специально отметить, что договор присоединения нередко применяется во взаимоотношениях коммерческой организации с гражданином и предполагает определение организацией условий договора в стандартных формах. Как и в случае с публичным договором, конструкция договора присоединения не рассчитана исключительно на регулирование заключения договора с участием граждан-потребителей, но в большинстве случаев применяется именно к таким отношениям[1].

В связи со сказанным весьма интересен вопрос о том, является ли пользователь соцсети потребителем, когда пользуется сервисами, которые предлагаются ресурсом соцсети.

На наш взгляд, правильнее было бы говорить не о пользователе соцсети, а о ее участнике. Это объясняется тем, что ценность соцсети определяется в значительной мере той информацией, которую человек (либо организация) размещает при создании своего профиля и при дальнейшем участии в «жизни» соцсети, а не только теми сервисами, которые предлагает пользователю сайт соцсети. Иными словами, формирование и информационное наполнение самого сайта соцсети осуществляются при непосредственном участии именно пользователей – как раз они формируют основные информационные потоки, непрерывно взаимодействуя между собой.

Итак, функционирование соцсети обеспечивают и владелец сайта соцсети, и многочисленная армия участников (пользователей соцсети), включающая граждан, организации, государственные органы и должностных лиц. Это, в свою очередь, позволяет заключить, что отношения владельца ресурса и участников характеризуются скорее как сотрудничество, нежели как предоставление и потребление услуг.

По мнению Е.А. Лавренчук, это сотрудничество принципиально нового типа – «своего рода соработничества, человека с техносоци-

[1] *Кирилловых А.А.* Защита прав потребителей: вопросы правового регулирования. М.: Деловой двор, 2012.

альным объектом, их коэволюцией. Объект нисколько не менее активный строитель системы отношений (сети), чем включенный в его функционирование субъект»[1].

Данное утверждение, основанное на философском исследовании, акцентирует внимание еще на одном важном элементе соцсети, упомянутом ранее, – технологической платформе, программном обеспечении. Речь идет о технологическом функционале, который обеспечивает участникам (пользователям соцсети) возможность общения и в отношении которого в пользовательском соглашении, например, «ВКонтакте» установлено следующее: «Администрация сохраняет за собой право в любое время изменять оформление Сайта, его содержание, список сервисов, изменять или дополнять используемые скрипты, программное обеспечение и другие объекты, используемые или хранящиеся на Сайте, любые серверные приложения в любое время с предварительным уведомлением или без такового» (п. 7.4).

5. Отношения внутри социальной сети не всегда соответствуют требованиям законодательства – нередки и правонарушения.

Некоторая часть правонарушений, совершаемых в соцсетях (как и в Интернете вообще), подпадает под регулирование соответствующего отраслевого законодательства – норм КоАП, УК РФ и пр. Но, несмотря на активное развитие отечественного законодательства, его эффективность в части пресечения интернет-нарушений остается недостаточной. Например, несмотря на активно ведущуюся борьбу в сети Интернет, по-прежнему существуют торренты с незаконным контентом (сервисы обмена информацией в Интернете, от англ. *torrent* – «стремительный поток»).

С одной стороны, это объясняется развитием информационных технологий, способствующих мгновенному распространению информации, с другой – неприспособленностью действующих процедурных механизмов и ресурсов к скорости интернет-процессов, на преодоление которой направлены ФЗ от 28.12.2013 № 398-ФЗ и ФЗ от 01.07.2017 № 156-ФЗ.

С учетом сказанного интерес вызывают управленческие механизмы, создаваемые в самих соцсетях.

Уже при первом ознакомлении с пользовательским соглашением, которое обозначено как «юридически обязательное» (его правила

[1] *Лавренчук Е.А.* Аутопойезис социальных сетей в интернет-пространстве: дис. ... канд. филос. наук. М., 2011.

должны быть приняты «безоговорочно»), четко усматривается контролирующая функция администрации соцсети за деятельностью пользователей и значительное число вопросов, решение которых остается «на усмотрение» администрации сайта[1].

Например, администрация соцсети оставляет за собой право (но не принимает на себя обязанность) просматривать аккаунты пользователей или страницы групп и сообществ на наличие запрещенного контента и блокировать их, если «по личному мнению администрации» контент не соответствует правовым или этическим нормам, которые имеют значение для репутации соцсети.

Закономерно было бы решать в пользовательских соглашениях и вопросы ответственности администрации. Но здесь, как правило, устанавливается ограничение ответственности, в том числе за сбои в работе и потерю информации, за последствия изменения функционала и т.п. И это при том, что подобные проблемы вовсе не редки, например, в марте 2012 г. ошибка программного обеспечения *Facebook* на 30 минут открыла все электронные адреса пользователей, а в мае того же года брешь в системе безопасности позволила с помощью примитивного трюка читать приватные сообщения пользователей, а потом была выявлена недоработка, позволяющая хакерам легко внедряться в профили[2].

В итоге последствия сбоев программно-технического функционала остаются в сфере риска самих пользователей[3]. Например, из-за системной ошибки рекламодателям[4] были переданы не только ано-

[1] Существование такой иерархии в соцсети подтверждают работы К. Фритьоф, Ф. Хайек и А. Хиршман, в которых установлено, что социальные сети играют ключевую роль в координации властных взаимоотношений, реализующихся в рамках организаций (см. об этом: *Лавренчук Е.А.* Аутопойезис социальных сетей в интернет-пространстве: автореф. дис. ... канд. юрид. наук. М., 2011).

[2] *Штайншаден Я.* Социальная сеть. Феномен Facebook. М., 2011. С. 204.

[3] В юридической литературе было высказано предложение об установлении гражданско-правовой ответственности сложных программных продуктов, причем сложный программный продукт рассматривается как источник повышенной опасности, т.е. его владелец (разработчик) несет ответственность независимо от наличия своей вины (см.: *Крыжановская А.А.* Гражданско-правовая ответственность за вред, причиненный в связи с использованием сложных программных продуктов: научно-практическое исследование. М., 2010.)

[4] Речь идет о таргетировании (или целевой рекламе), которое заключается в предоставлении социальной интернет-сетью рекламодателям данных со всех страниц определенной целевой группы (по выбору рекламодателя), предварительно обработав эти данные и сделав их анонимными.

нимные данные, но и имена пользователей *Facebook*, которые должны были быть скрыты, что является грубым нарушением законодательства о персональных данных.

В то же время нельзя не признавать, что владелец сайта соцсети не может отвечать за все правонарушения, допускаемые в соцсети, учитывая огромное количество участников, отслеживание их неправомерного поведения является крайне сложной и затратной задачей, а кроме того, возлагает на владельца ресурса несвойственную ему публичную функцию. Поэтому ответственность за неправомерные действия групп и сообществ, в которые объединяются пользователи соцсети, должна возлагаться на самих пользователей соцсети (участников).

6. Подводя итоги, следует признать, что владельцы ресурса и участники соцсети, используя устройства и сервисы, образуют сложную общественную, информационную, техническую и экономическую систему. С правовой точки зрения эта система не является самостоятельным субъектом права и не подпадает под какой-либо из существующих правовых режимов.

По мнению исследователей, аксиологический статус соцсетей в современном информационном обществе обусловлен тем, что они, с одной стороны, являются вынужденным, компенсационным механизмом, формирующимся в условиях неэффективности государства и других социальных институтов; с другой – представляют собой универсальный социальный механизм, осуществляющий свои функции в условиях состояния относительной социальной и групповой солидарности и дополняющий в этом качестве иные социальные институты[1].

В связи со сказанным целесообразно установление такого правового регулирования[2] соцсети, который:

1) будет предусматривать взаимную ответственность владельцев ресурса и пользователей соцсети в рамках самостоятельного правового режима;

---

[1] Подробнее об этом см.: *Реутов Е.В., Колпина Л.В., Реутова М.Н., Бояринова И.В.* Социальные сети в региональном сообществе: монография. Белгород: КОНСТАНТА, 2011.

[2] Ю.А. Тихомиров подчеркивает, что в новейших теоретических исследованиях правовое регулирование рассматривается как процесс упорядочения общественных отношений при помощи как спонтанно формируемых в обществе норм права, так и правовых предписаний, устанавливаемых государством в нормативных правовых актах (*Тихомиров Ю.А.* Правовое регулирование: теория и практика. М., 2010. С. 25).

2) позволит сохранить инициативу пользователей, присоединяющихся к соцсети, реализуемую с помощью институтов саморегулирования, которые уже разработаны и применяются (модерация, администрирование).

При этом необходимо учитывать и такие составляющие функционирования соцсети, как возможности технического воздействия на процессы и отношения, возникающие между ее участниками, а также экономические преимущества, которые могут быть извлечены из предоставления ресурса миллионам пользователей.

Пристатейный библиографический список:

1. *Губанов Д.А., Новиков Д.А., Чхартишвили А.Г.* Социальные сети: модели информационного влияния, управления и противоборства. М., 2010.

2. *Тихомиров А.А., Труфанов А.И.* Сверхсложные сети: новые модели интерпретации социально-экономических и биосоциальных процессов // Труды Института государства и права Российской академии наук. 2011. № 6.

3. *Зиммель Г.* Большие города и духовная жизнь // Логос. 2002. № 3–4.

4. *Спенсер Г.* Личность и государство. Челябинск, 2007.

5. *Морено Я.* Социометрия: Экспериментальный метод и наука об обществе. М., 2001.

6. *Barnes J.* Class and Committees in a Norwegian Island Parish // Human Relations. 1954.

7. *Boyd D.M., Ellison N.*B. Social Network Sites: Definition, History, and Scholarship / Danah M. Boyd, Nicole B. Ellison // Journal of Computer-Mediated Communication. 2008. N 13.

8. *Штайншаден Я.* Социальная сеть. Феномен Facebook. М., 2011.

9. *Лавренчук Е.А.* Аутопойезис социальных сетей в интернет-пространстве: автореф. дис. ... канд. юрид. наук. М., 2011.

10. *Браславец Л.А.* Интернет-сервисы социальных сетей в современной системе средств массовой информации. Воронеж, 2010.

11. *Лещенко А.М.* Социальные сети как механизм конструирования коммуникации в современном обществе: автореф. дис. ... канд. филос. наук. Пятигорск, 2011.

12. *Терещенко Л.К.* Модернизация информационных отношений и информационного законодательства: монография / Институт зако-

нодательства и сравнительного правоведения при Правительстве РФ. М., 2013.

13. *Кирилловых А.А.* Защита прав потребителей: вопросы правового регулирования. М.: Деловой двор, 2012.

14. *Крыжановская А.А.* Гражданско-правовая ответственность за вред, причиненный в связи с использованием сложных программных продуктов: науч.-практ. исслед. М., 2010.

15. *Тихомиров Ю.А.* Правовое регулирование: теория и практика. М., 2010.

16. *Реутов Е.В., Колпина Л.В., Реутова М.Н., Бояринова И.В.* Социальные сети в региональном сообществе: монография. Белгород: КОНСТАНТА, 2011.

Н.С. Еманова

ЭЛЕКТРОННАЯ ТОРГОВЛЯ В СОЦИАЛЬНЫХ СЕТЯХ: АКТУАЛЬНЫЕ ВОПРОСЫ

Аннотация. *В статье исследуется вопрос о правовых гарантиях, предоставляемых покупателю интернет-магазином в социальной сети, а также способы защиты покупателем своих прав в социальной сети.*

Ключевые слова: *торговля, электронная торговля, социальная сеть, VKontakte, Facebook*.

В современном мире социальные интернет-сети (далее – соцсети) стали неотъемлемой частью жизни людей: по данным исследовательской компании *TNS*, в России соцсетями пользуется 99,7% всей среднесуточной интернет-аудитории[1]. Что же представляют собой соцсети и в чем их предназначение?

Понятие «социальная сеть» продолжительное время исследовалось в основном социологами, которые понимали под ними реальные взаимосвязи людей друг с другом[2].

Развитие информационных технологий привело к появлению социальных связей «нового формата» – социальных интернет-сетей[3], за которыми стали усматривать несколько иное значение. В современных социологических исследованиях соцсеть рассматривают как веб-сервис или виртуальную коммуникацию, позволяющие реализовать определенные мотивации индивида, например возможность определять дистанцию в отношениях с другими индивидами, не пе-

[1] Россия занимает пятое место по количеству пользователей этих ресурсов (см., например: Федеральная антимонопольная служба проверит заработки социальных сетей (URL: http://ppt.ru/news/114927 (дата обращения: 15.05.2015)), ФАС проверит социальные сети (URL: http://bodytut.ru/фас-проверит-социальные-сети/ (дата обращения: 11.06.2016)).

[2] Родоначальником их исследования считается Георг Зиммель (см. об этом: *Кашин В.В.* Формальная социология Георга Зиммеля // Вестник ОГУ. 2008. № 7. С. 4–11).

[3] М.В. Егоров пишет: «Динамика развития общества сопровождается трансформацией социальных связей, связанной с интенсификацией социальных процессов» (*Егоров М.В.* Механизмы сетевой самоорганизации социального пространства: дис. ... канд. соц. наук. Ставрополь, 2016. С. 3).

ресекая границу желаемого сближения[1]. А, например, Д.М. Бойд и Н.Б. Эллисон, характеризуя соцсети, пишут, что это «сетевые услуги, которые позволяют частным лицам: 1) строить общественные или полуобщественные профили в пределах ограничений, наложенных системой, 2) определять список других пользователей, с которыми они могут сообщаться и делиться информацией, 3) просматривать и связывать их список контактов с другими, созданными пользователями внутри системы»[2].

Вместе с тем нельзя не замечать, что если еще пару лет назад прямое предназначение соцсетей усматривалось в обеспечении возможностей для общения людей по всему миру, и никто не видел за ними торговый потенциал, то сейчас ситуация принципиально поменялась. Соцсети сегодня – это онлайн-подобие рынка, где можно купить все что угодно.

Электронная торговля в соцсетях – явление достаточно новое, поэтому ни в одном из нормативных правовых актов такое явление, как «торговля в социальной сети», не получило необходимого регулирования[3].

На наш взгляд, поскольку розничная купля-продажа товаров в соцсетях осуществляется в интернет-пространстве, то ее следует рассматривать как разновидность дистанционной продажи. Следовательно,

[1] См., например: *Алексаньян Н.К.* Сетевизация современного общества // Гуманитарные, социально-экономические и общественные науки. 2012. № 1, 2. С. 34–37; *Саенко Л.А., Егоров М.В.* Сетевое общество в контексте современных социальных трансформаций // Дискуссия. 2014. № 7(48). С. 88–93; *Тисрон С.* Новые социальные сети в интернете // Психотропы. 2011. № 17 (2). С. 99–118; *Ефимов Е.Г.* Социальные группы как объект исследования социальных интернет-сетей // Известия ВолгГТУ. 2012. № 11 (8). С. 64–66; *Архангельская А.С., Архангельская И.Б.* Социальные сети как площадка для бизнес-коммуникаций // Вестник ННГУ. 2013. № 4(2). С. 186–189; *Зайонц В.В.* Социологические подходы к исследованию виртуальных социальных сетей // Молодой ученый. 2010. № 4. С. 266–271; *Ефимов Е.Г.* Социология социальных интернет-сетей (историко-теоретические аспекты) // Исторические, философские, политические и юридические науки, культурология и искусствоведение // Вопросы теории и практики. 2013. № 9–1(35). С. 47–50; *Алексеенко Е.А.* Особенности электронной торговли в социальных сетях // Общество: социология, психология, педагогика. 2012. № 3. С. 33–38.

[2] *Бойд Д.М., Эллисон Н.Б.* Социальные интернет-сети: дефиниция, история, образование // Журнал компьютерных технологий. 2008. № 13. С. 210–230.

[3] Примечательно, что в публикациях электронная торговля иногда определяется так: «...интеграция инструментов коммерции в интерфейс страниц брендов в социальных сетях. Также это различные инструменты для распространения своего опыта общения с брендом по своим «друзьям» Делаем продажи через социальные сети» (URL: http://www.likeni.ru/analytics/123881/ (дата обращения: 19.09.2015)).

возникающие правоотношения подпадают под регулирование положений о дистанционных продажах, содержащихся в ст. 497 ГК РФ («Продажа товара по образцам и дистанционный способ продажи товаров»), Законе РФ от 07.02.1992 № 2300-I «О защите прав потребителей», Правилах продажи товаров дистанционным способом, утвержденных Постановлением Правительства РФ от 27.09.2007 № 612 (далее – Правила продажи).

Однако развитие такого явления, как соцсети, приводит к появлению новых видов электронной торговли. И вот уже говорят о VK-commerce (торговля в соцсети «ВКонтакте» и *FB-commerce* (торговля в соцсети *Facebook*)[1].

Анализ контента значительного числа групп в соцсетях позволяет сделать вывод о том, что многие из них специализируются на продаже товаров. Такие группы позиционируют себя как интернет-магазины. Но их деятельность не во всех случаях соответствует нормам, содержащимся в упомянутых выше нормативных правовых актах. Более того, несовершенство правового регулирования некоторых вопросов в законодательстве, равно как и недостаточная осведомленность потребителей, недобросоветно используется «владельцами» таких «интернет-магазинов» в целях получения максимальной прибыли в ущерб интересам потребителей.

Первым хотелось бы разобрать вопрос о субъектах электронной торговли в соцсетях.

Занятие торговлей относится к предпринимательской деятельности. Согласно абз. 3 п. 1 ст. 2 ГК РФ предпринимательской является самостоятельная, осуществляемая на свой риск деятельность, направленная на систематическое получение прибыли от пользования имуществом, продажи товаров, выполнения работ или оказания услуг лицами, зарегистрированными в этом качестве в установленном законом порядке.

Следовательно, для осуществления торговой деятельности в соцсети необходимо либо создание юридического лица, обладающего правом заниматься коммерческой деятельностью (ст. 50 ГК РФ), либо регистрация физического лица в качестве индивидуального предпринимателя (ст. 23 ГК РФ).

Несоблюдение этого требования может повлечь для гражданина административную (ст. 14.1 КоАП РФ) или уголовную ответствен-

[1] Можно ли продавать в социальных сетях? (URL: http://www.likeni.ru/interviews/mozhno-li-prodavat-v-sotsialnykh-setyakh/ (дата обращения: 24.03.2017)).

ность (ст. 171 УК РФ); несоблюдение требований о постановке на учет в налоговый орган влечет также и налоговую ответственность (ст. 116 НК РФ). Кроме того, как верно отмечает В.В. Кванина, «сделки физических лиц, не зарегистрированных в качестве индивидуальных предпринимателей, совершенные при осуществлении предпринимательской деятельности, должны рассматриваться в качестве ничтожных»[1].

Как показал проведенный анализ, многие так называемые интернет-магазины в соцсетях не считают обязательным соблюдать упомянутые нормы при осуществлении своей деятельности. Так, лишь 37 из 300 интернет-магазинов, представленных в соцсети «ВКонтакте», соблюдают названные требования действующего законодательства; остальные же осуществляют продажу товаров, как правило, без регистрации продавца в качестве индивидуального предпринимателя (без образования юридического лица).

Таким образом, основная масса продавцов в соцсетях занимается незаконным предпринимательством. При этом из 100 опрошенных продавцов, занимающихся электронной торговлей в соцсетях, лишь 28 знают о незаконности своей деятельности, что, впрочем, не мешает им продолжать этим заниматься. Примечательно, что и основная масса покупателей нелегальных интернет-магазинов не подозревает о незаконности их торговой деятельности: по результатам опроса, из 187 покупателей только 19 знают, каким требованиям должен соответствовать интернет-магазин в соцсети.

В развитие сказанного выше следует обратить внимание на то, что каждая соцсеть разрабатывает собственное пользовательское соглашение, которым может либо разрешать, либо запрещать осуществление определенной деятельности, в том числе торговой.

В связи с этим примечательно, что, например, в соцсети «ВКонтакте» до 2016 г. не предусматривалось ее использование в качестве платформы для электронной торговли[2]. Согласно п. 5.11 и 5.13. 1 пользовательского соглашения соцсети «ВКонтакте» пользователи были вправе создавать персональную страницу только в некоммерческих целях, а сообщество могло быть использовано только для продвижения товаров, но не для их продажи. Ситуация изменилась с начала 2016 г.:

[1] *Кванина В.В.* Понятие и признаки предпринимательской деятельности // Вестник Южно-Уральского государственного университета. Серия «Право». 2004. № 11 (40). Вып. 5. С. 129–140.

[2] Социальная коммерция. Год после RIW-2012 (URL: http://www.buxle.ru/2013/socialnaya-kommerciya-god-posle-riw-2012/ (дата обращения: 24.03.2017)).

теперь в соцсети «ВКонтакте» легализована продажа товаров через данную соцсеть[1].

В то же время соцсеть *Facebook* заняла такую позицию гораздо раньше. Так, пользовательским соглашением соцсети *Facebook* не запрещаются коммерческие операции, а начиная с мая 2011 г. развивается система совершения сделок через эту соцсеть[2]. Кроме того, разработано и работает в соцсети *Facebook* приложение «*CS – Cart Store*», созданное для автоматического создания интернет-магазина в рамках соцсети. Как отмечает Дженис Динер, *ASOS* стал первым полностью интегрированным в соцсеть Facebook магазином Европы[3].

При этом достаточно известные компании используют соцсети не для продажи, а именно для продвижения товаров, давая при этом ссылку на интернет-магазин, «расположенный» вне этой соцсети[4]. Например, в соцсети *Facebook* это магазины Dolce & Gabbana[5] и «Сердце океана»[6], а в соцсети «ВКонтакте» – магазин «Найфл»[7].

Еще одним значимым аспектом рассматриваемой темы является проблема предоставления продавцом недостоверной или неполной информации о товаре потребителю (покупателю).

В соответствии с п. 8 Правил продажи продавец должен **до заключения договора** розничной купли-продажи предоставить покупателю информацию об основных потребительских свойствах товара и адресе (месте нахождения) продавца, о месте изготовления товара, полном фирменном наименовании (наименовании) продавца, о цене и об условиях приобретения товара, о его доставке, сроке службы, сроке годности и гарантийном сроке, о порядке оплаты товара, а также о сроке, в течение которого действует предложение о заключении договора.

---

[1] Правила пользования сайтом «ВКонтакте» (URL: http://vk.com/terms (дата обращения: 19.03.2017)).

[2] Делаем продажи через социальные сети (URL: http://www.likeni.ru/analytics/123881/ (дата обращения: 20.03.2017)).

[3] Динер Д.Ф. Ф-коммерция, покупки на Фейсбук (URL: http://www.clickz.com/author/profile/1969/janice-diner (дата обращения: 20.03.2017)).

[4] На это обращают внимание некоторые авторы, см., например: *Алексеенко Е.А.* Особенности электронной торговли в социальных сетях // Общество: социология, психология, педагогика. 2012. № 3. С. 33–38.

[5] «Dolce & Gabbana» (URL: https://www.facebook.com/DolceGabbana?fref=ts (дата обращения: 18.06.2015)).

[6] «Сердце океана» (URL: https://www.facebook.com/pages/Сердце-Океана/910745232311070?fref=ts (дата обращения: 18.01.2017)).

[7] НАЙФЛ (URL: http://vk.com/naiflgroup (дата обращения: 18.06.2016)).

При этом в соответствии с п. 9 Правил продажи на продавца налагается обязанность **в момент доставки товара** довести до сведения покупателя в письменной форме следующую информацию (для импортных товаров – на русском языке):

«а) наименование технического регламента или иное обозначение, установленное законодательством Российской Федерации о техническом регулировании и свидетельствующее об обязательном подтверждении соответствия товара;

б) сведения об основных потребительских свойствах товара (работ, услуг), а в отношении продуктов питания – сведения о составе (в том числе наименование использованных в процессе изготовления продуктов питания пищевых добавок, биологически активных добавок, информация о наличии в продуктах питания компонентов, полученных с применением генно-инженерно-модифицированных организмов), пищевой ценности, назначении, об условиях применения и хранения продуктов питания, о способах изготовления готовых блюд, весе (объеме), дате и месте изготовления и упаковки (расфасовки) продуктов питания, а также сведения о противопоказаниях для их применения при отдельных заболеваниях;

в) цена в рублях и условия приобретения товара (выполнения работ, оказания услуг);

г) сведения о гарантийном сроке, если он установлен;

д) правила и условия эффективного и безопасного использования товаров;

е) сведения о сроке службы или сроке годности товаров, а также сведения о необходимых действиях потребителя по истечении указанных сроков и возможных последствиях при невыполнении таких действий, если товары по истечении указанных сроков представляют опасность для жизни, здоровья и имущества покупателя или становятся непригодными для использования по назначению;

ж) место нахождения (адрес), фирменное наименование (наименование) изготовителя (продавца), место нахождения (адрес) организации (организаций), уполномоченной изготовителем (продавцом) на принятие претензий от покупателей и производящей ремонт и техническое обслуживание товара, для импортного товара – наименование страны происхождения товара;

з) сведения об обязательном подтверждении соответствия товаров (услуг) обязательным требованиям, обеспечивающим их безопасность для жизни, здоровья покупателя, окружающей среды и предотвраще-

ние причинения вреда имуществу покупателя в соответствии с законодательством Российской Федерации;

и) сведения о правилах продажи товаров (выполнения работ, оказания услуг);

к) сведения о конкретном лице, которое будет выполнять работу (оказывать услугу), и информация о нем, если это имеет значение исходя из характера работы (услуги);

л) информация, предусмотренная п. 21 и 32 настоящих Правил;

м) информация об энергетической эффективности товаров, в отношении которых требование о наличии такой информации определено в соответствии с законодательством Российской Федерации об энергосбережении и о повышении энергетической эффективности».

Причем необходимо обратить внимание на общую норму п. 21 Правил продажи, устанавливающую право покупателя отказаться от товара в любое время до его передачи, а после передачи товара – в течение семи дней.

Между тем, как показало проведенное исследование, содержащаяся на страницах интернет-магазинов в соцсетях информация нередко бывает ложной, покупателю не предоставляется необходимая информация, в частности, о сроках и порядке возврата товара.

В качестве примера можно привести магазин *SHIP SHOP*[1], существующий в соцсети «ВКонтакте». В нем нет требуемой Правилами продажи информации, равно как и отсутствуют сведения о регистрации продавца в качестве индивидуального предпринимателя или юридического лица. При этом на странице этого интернет-магазина указывается: «Возврата по причине «просто так» у нас нет! После того, как вы присылаете чек, начинается обработка вашего заказа и обратный процесс невозможен»[2], что вступает в прямое противоречие с п. 4 ст. 26.1. Закона РФ «О защите прав потребителей» и п. 21 Правил продажи. Аналогичный подход к электронной торговле наблюдается и в ряде других интернет-магазинов соцсети «ВКонтакте»[3].

[1] SHIP SHOP (URL: http://vk.com/shipshop (дата обращения: 23.12.2016)).

[2] Возврат (URL: http://vk.com/topic-43195721_30567480 (дата обращения: 12.01.2017)).

[3] Это наблюдается в ряде интернет-магазинов, таких как: Victoria Secret (URL: http://vk.com/victoriassecretru (дата обращения: 13.01.2017)), «ПЛАТЬЯ CRYSTAL ОДЕЖДА СУМКИ ЧАСЫ ЧЕЛЯБИНСК» (URL: http://vk.com/crystal_chel (дата обращения: 13.01.2017)), «Евгения Меркулова» (URL: http://vk.com/id203086436 (дата обращения: 13.01.2017)), «Юлия Модная» (URL: http://vk.com/id147661016 (дата обращения: 13.01.2017)), «Очки Ray Ban» (URL: http://vk.com/rayban_ray_ban (дата обращения: 13.01.2017)), «Елена Нестерова (URL: http://vk.com/id183853118 (дата обращения:

Впрочем эта тенденция характерна и для других соцсетей, в частности, в соцсети Facebook не было найдено ни одного интернет-магазина, отвечающего установленным требованиям законодательства.

В качестве примера можно привести магазин «Платьице»[1], на странице которого размещены фотографии текстильных товаров, наличие которых продавец счел достаточным для информирования покупателей о приобретаемых товарах. О способе приобретения выбранного товара продавец информирует в личном сообщении.

По итогам исследования условий приобретения товаров в соцсетях, можно констатировать, что нелегальные магазины в качестве основного условия покупки указывают стопроцентную предоплату за покупку. Договор между продавцом и покупателем, по сути, не заключается: основываясь на некоторой информации на странице такого «интернет-магазина», покупатель производит оплату приглянувшегося товара и (при необходимости) его доставку, а продавец дает «честное слово» доставить заказ.

Бесспорно, во многих случаях покупатель получает заказанное, но совсем нередки ситуации, когда «продавец», дождавшись перевода на его счет денег, пропадает. В результате проведенного нами опроса пользователей соцсети «ВКонтакте», были получены следующие данные: 68% пользователей хотя бы раз сталкивались с мошенниками при покупке товаров в интернет-магазинах этой соцсети, 20% – благополучно получили заказанные товары, а 12% – не решаются приобретать товары в соцсети из-за опасений столкнуться с мошенниками.

В таких условиях возникает закономерный вопрос: как же защитить свои права при покупке товаров в соцсетях?

К сожалению, далеко не каждый покупатель знает о возможности доказывания самого факта покупки в соцсети, что способствует увеличению числа злоумышленников. Между тем, попав в подобную ситуацию, необходимо обращаться в правоохранительные органы с заявлением о фактах незаконной предпринимательской деятельности и мошенничества, прикладывая копии платежных документов, подтверждающих произведенные транзакции, копию переписки с продавцом, а также указав ссылку на группу или аккаунт продавца в соответсвующей соцсети.

13.01.2017), «Косметика. YSL. GUERLAIN. DKNY. DIOR. ESTEE LAUDER» (URL: http://vk.com/cosmetic_brand (дата обращения: 13.01.2017)).

[1] «Платьице» (URL: https://www.facebook.com/platjice/timeline (дата обращения: 09.12.2016)).

На данный момент можно с уверенностью сказать, что развитие сектора электронной торговли способствует не только стабилизации экономики, но и появлению новых видов правонарушений и преступлений в соцсетях. В частности, проведенное нами изучение электронной торговли в соцсетях выявило огромное количество нелегальных интернет-магазинов[1].

В этих условиях, когда соцсети стали использоваться как платформа для электронной торговли, можно согласиться с мнением Н.В. Кичигина, который отметил, что «российское законодательство «не успевает» за развитием сферы информационных технологий, в частности социальных интернет-сетей, зачастую запоздало реагируя на вызовы времени»[2]. Таким образом, эта сфера применения информационных технологий ставит перед юридическим сообществом множество вопросов.

Пристатейный библиографический список:

1. *Алексеенко Е.А.* Особенности электронной торговли в социальных сетях // Общество: социология, психология, педагогика. 2012. № 3.

2. *Бойд Д.М., Эллисон Н.Б.* Социальные интернет-сети: дефиниция, история, образование // Журнал компьютерных технологий. 2008. № 13.

3. *Динер Д.Ф.* Ф-коммерция, покупки на Фейсбук (URL: http://www.clickz.com/author/profile/1969/janice-diner (дата обращения: 20.03.2017)).

4. *Егоров М.В.* Механизмы сетевой самоорганизации социального пространства: дис. ... канд. соц. наук. Ставрополь, 2016.

5. *Залоило М.В., Власова Н.В.* Социальные интернет-сети: правовые аспекты // Журнал российского права. 2014. № 5.

6. *Касенова М.Б.* Идентификация лиц в Интернете и киберпространство социальных сетей // Юрист. 2014. № 6.

7. *Кашин В.В.* Формальная социология Георга Зиммеля // Вестник ОГУ. 2008. №7.

[1] См. например, You Look Shop (URL: http://vk.com/onlineshopingr (дата обращения: 17.02.2017); COLORADO SHOP (URL: http://vk.com/colorado_shop (дата обращения: 17.02.2017)); «Женская одежда» (URL: http://vk.com/spbclothes (дата обращения: 17.06.2015)); «Камелия» (URL: http://vk.com/cameliashopru (дата обращения: 17.06.2016)).

[2] *Залоило М.В., Власова Н.В.* Социальные интернет-сети: правовые аспекты // Журнал российского права. 2014. № 5. С. 140–145.

8. *Кванина В.В.* Понятие и признаки предпринимательской деятельности // Вестник Южно-Уральского государственного университета. Серия «Право». 2004. № 11 (40). Вып. 5.

9. Можно ли продавать в социальных сетях? (URL: http://www.likeni.ru/interviews/mozhno-li-prodavat-v-sotsialnykh-setyakh/ (дата обращения: 24.03.2017)).

10. Правила пользования сайтом ВКонтакте (URL: http://vk.com/terms (дата обращения: 19.03.2017)).

11. Социальная коммерция. Год после RIW-2012 (URL: http://www.buxle.ru/2013/socialnaya-kommerciya-god-posle-riw-2012/ (дата обращения: 24.03.2017)).

12. Федеральная антимонопольная служба проверит заработки социальных сетей (URL: http://ppt.ru/news/114927 (дата обращения: 15.01.2017)).

13. ФАС проверит социальные сети (URL: http://bodytut.ru/фас-проверит-социальные-сети/ (дата обращения: 11.06.2016)).

В.Н. Глонина

ПРОБЛЕМА ПРАВОВОГО РЕГУЛИРОВАНИЯ РАЗМЕЩЕНИЯ ГИПЕРССЫЛОК В СЕТИ ИНТЕРНЕТ[1]

Аннотация. *Автор рассматривает в статье проблему правового регулирования размещения гиперссылок в сети Интернет. В частности, анализируется возможность привлечения к ответственности за гиперссылку на контент, размещенный в сети Интернет с нарушением норм авторского права. Проводится сравнительный анализ национальной и зарубежной доктрины, законодательства, а также судебной практики по данной проблеме. Автор делает вывод о необходимости выработки критериев, на основании которых будет регулироваться размещение гиперссылок, регламентироваться привлечение к ответственности за их использование в сети Интернет.*

Ключевые слова: *авторское право, сравнительное правоведение, гиперссылка, ответственность информационного посредника, доведение до всеобщего сведения.*

Гиперссылка – это указание на смысловую связь фрагмента одного документа с другим документом или его фрагментом[2].

В современном мире этот некогда специализированный термин из области информационных технологий обрел повседневный вид. Между тем использование гиперссылок для связи между электронными документами – явление настолько же широко распространенное, насколько и неопределенное с точки зрения правового регулирования. В настоящей работе гиперссылка рассматривается в контексте авторского права, поднимается вопрос о возможности привлечения к ответственности за размещение гиперссылок в сети Интернет. Анализ ведется в сравнительно-правовом контексте законодательства, судебной практики и доктрины таких государств, как Россия, США, Канада, Мексика, страны ЕС. Актуальность работы подтверждается

[1] Статья победителя конкурса IP & IT LAW – 2017.

[2] Большой толковый словарь русского язика / С.А. Кузнецов. СПб.: Норинт, 1998 (дата обращения: 28.08.2016).

как широким использованием гиперссылок, в том числе на ресурсы, содержащие охраняемые объекты интеллектуальной собственности, так и разрозненностью и фрагментарностью имеющегося правового регулирования, отсутствием масштабных исследований по данному вопросу.

Понятие гиперссылки в контексте авторского права

Несомненно, технология гиперссылок играет важнейшую роль для функционирования сети Интернет, развития информационного общества, но сама по себе технология гиперссылки не является объектом интеллектуальной собственности. В связи с этим нельзя не вспомнить дело *British Telecommunications Plc. v. Prodigy Communications Corp*, рассмотренное в США, в Окружном суде Южного округа Нью-Йорка: в этом деле суд отказал в признании наличия у истца патентных прав на технологию гиперссылки[1].

Вместе с тем для мирового сообщества остается проблематичной выработка должного правового регулирования использования гиперссылок. Особенно остро данная проблема проявляется в сфере интеллектуальной собственности: использование гиперссылок напрямую затрагивает право интеллектуальной собственности, в частности авторское право.

Так что же представляет собой гиперссылка с точки зрения норм авторского права?

В отечественном законодательстве об авторском праве гиперссылки прямо не упоминаются, да и в законодательстве зарубежных стран легальной дефиниции в ходе проведения данного исследования выявлено не было. Тем не менее, основываясь на доктринальных источниках, можно сделать вывод, что ссылка, и в том числе гиперссылка, – это способ адресации в сети Интернет. Важно отметить, что гиперссылка может представлять собой не только слово-адрес, но также текст веб-страницы, картинку или ее часть.

Так, выделяют «глубокие ссылки» (позволяющие переадресовать пользователя прямо к внутренним страницам другого сайта), фреймы (являющиеся специальным окном браузера для представления внеш-

[1] BRITISH TELECOMMUNICATIONS PLC, Plaintiff v. PRODIGY COMMUNICATIONS CORPORATION, Defendant 217 F. Supp. 2d 399 (2002), No. 00 Civ. 9451(CM). United States District Court, S.D. New York (URL: http://www.allcourtdata.com/ (дата обращения: 19.11.2016)).

него сайта), встроенные ссылки (отображающие содержание другой веб-страницы)[1].

Стоит отметить, что в немногочисленных исследованиях в рассматриваемой сфере проявляются различные подходы к пониманию гиперссылки в рамках авторского права:

1) как местоположение ресурса в сети Интернет, не затрагивающего сферу авторского права в принципе[2] (т.е. размещение гиперссылки не может нарушать авторское право, так как сама по себе гиперссылка не затрагивает охраняемые объекты авторского права, не является единственной возможностью доступа к ним);

2) как способ использования объекта интеллектуальной собственности[3];

3) как особый институт, который лишь при соблюдении четкого ряда критериев может рассматриваться как способ использования объекта интеллектуальной собственности[4].

Таким образом, очевидно, что единого подхода к пониманию гиперссылки в современном праве не выработано. Тем не менее представляется, что конкретизация правового режима гиперссылок необходима для нормального развития цифрового общества, возможности защиты авторских прав при соблюдении баланса с интересами пользователей. Ведь от того, что понимается под гиперссылкой (от выбора подхода к пониманию этого явления), зависит ответ на важнейшие вопросы в сфере авторского права: возможно ли создание гиперссылки без согласия автора; могут ли гиперссылки сами по себе нарушать интересы правообладателей; допустимо ли привлечение к ответственности за размещение гиперссылки при нарушении норм авторского права?

Размещение гиперссылки как акт доведения до всеобщего сведения

Прежде чем перейти к поиску ответов на поставленные вопросы, стоит рассмотреть подробнее позицию, согласно которой гиперссылка

[1] Connecting to Other Websites. Stanford University Library (URL: http://fairuse.stanford.edu/ (дата обращения: 28.08.2016)).

[2] *Гринюк М.* Гиперссылки. Правовые проблемы, возникающие с их использованием. Право и интернет: сб. ст., 2004 (URL: http://www.allpravo.ru (дата обращения: 30.10.2016)).

[3] *Burri Mira.* Permission to Link: Making Available via Hyperlinks in the European Union after Svensson (URL: http://www.jipitec.eu/ (дата обращения: 30.12.2016)).

[4] *Malama Georgia.* COPYRIGHT ASPECTS OF LINKING AND FRAMING. December 2013 (URL: https://repository.ihu.edu.gr/ (дата обращения: 28.12.2016)).

рассматривается как способ использования объекта интеллектуальной собственности – доведение его до всеобщего сведения. В частности, отголоски этой позиции можно найти в ст. 1270 ГК РФ, согласно которой правообладателю гарантируется исключительное право использования произведения в любой форме и любым не противоречащим закону способом, в том числе, и путем доведения произведения до всеобщего сведения.

Право на доведение произведения до всеобщего сведения исходит из ст. 8 Договора Всемирной организации интеллектуальной собственности об авторском праве (1996 г.; далее – ДАП). Однако ни в национальном законодательстве, ни на международном уровне сущность понятия «доведение произведения до всеобщего сведения» не раскрывается, что серьезно усложняет выявление случаев нарушения данного права.

В.О. Калятин пишет, что доведение до всеобщего сведения – это не столько способ использования произведения, сколько результат, достижение которого возможно различными способами[1]. В действующем ГК РФ эта форма распространения произведений определена как «доведение произведения до всеобщего сведения таким образом, что любое лицо может получить доступ к произведению из любого места и в любое время по собственному выбору».

В литературе отмечалась недостаточность и неточность содержащегося в Кодексе определения. Действительно, критерий «любого человека» используется вместо оригинального, используемого в ДАП критерия «представителя публики», выражающего доведение произведения до публики в целом, но не обязательно для всех и каждого. Справедливыми будут упреки и в отношении понятия «доступ из любого места и в любое время по своему выбору» – акцент опять делается на слове «любой», что способно создать правовую неопределенность и дать возможность обхода закона.

Но несмотря на критические замечания в отношении формулировок, нельзя отрицать значимость доведения до всеобщего сведения (в рамках настоящей работы право на доведение до всеобщего сведения будет рассматриваться в том смысле, который был заложен в это понятие ДАП). Ведь именно этот способ позволяет осуществлять

[1] Правда, нельзя не отметить, что В.О. Калятин писал об этом еще применительно к ранее действовавшему законодательству (*Калятин В.О.* Правовые проблемы использования произведения в Интернете // Информационное право. 2005. № 1 (URL: http://www.center-bereg.ru/ (дата обращения: 28.10.2016)).

коммерческое использование произведения в Интернете, например, путем предоставления платного доступа к объектам интеллектуальной собственности по запросу пользователя[1].

Но можно ли утверждать, что размещение гиперссылки есть реализация права на доведение до всеобщего сведения, а следовательно, является способом использования произведения. Выявленная неоднозначность законодательных формулировок не позволяет дать однозначный ответ.

Исходя из совокупного смысла ст. 1270, 1484, 1519 ГК РФ можно сделать вывод, что гиперссылка как способ адресации представляет собой использование результата интеллектуальной деятельности, осуществление исключительного права. Однако если речь идет об обычных текстовых гиперссылках, отсылающих пользователя к правомерно размещенному правообладателем в сети Интернет авторскому произведению (или произведению в составе иного контента сайта), то вряд ли можно согласиться с тем, что здесь имеет место использование этого произведения. Иное понимание способно парализовать работу Интернета, не будет отвечать целям развития информационного общества. Вместе с тем, возможно, в ряде случаев признание гиперссылки лишь «местоположением» ресурса, изолированным от регулирования авторского права, также не будет соответствовать идее поддержания баланса, так как защита правообладателей будет сведена на нет. Таким образом, необходимо выявить критерии, при соблюдении которых размещение гиперссылки будет признаваться доведением до всеобщего сведения.

Правовое регулирование размещения гиперссылок в сети Интернет в России

В анализируемом аспекте защита правообладателей осуществляется при помощи не столько механизмов авторского права, сколько норм информационного права, в частности Закона об информации. Статья 15.2 Закона об информации, регламентирующая ограничения доступа к информации, распространяемой с нарушением авторских и смежных прав, определяет гиперссылки как информацию, необходимую для получения указанных объектов с использованием информа-

[1] *Torremans Paul.* Research Handbook on Cross-border Enforcement of Intellectual Property. EE Elgar Publishing, 2014. P. 826–827 (дата обращения: 17.11.2016).

ционно-телекоммуникационных сетей, рассматривает наравне с самой информацией, нарушающей авторские права. Иными словами, Закон об информации признает гиперссылки использованием произведения, неправомерность которого влечет ответственность.

Аналогичный подход усматривается и в ст. 1253.1 ГК РФ, устанавливающей ответственность информационного посредника. В частности, информационным посредником признается лицо, предоставляющее возможность доступа к материалу или информации, необходимой для его получения с использованием сети Интернет – под это понятие подпадают сайты в Интернете, на которых размещаются гиперссылки на нелегальный контент.

Ответственность информационного посредника наступает при наличии вины, а освобождение от ответственности возможно только при соблюдении ряда условий: в случае передачи – не являлся ее инициатором, не определял получателя и не изменял контент, не знал и не должен был знать о том, что передача нарушает чьи-либо права; в случае размещения – не знал и не должен был знать о том, что использование контента составляет нарушение чьих-либо прав, при получении письменного заявления о нарушении прав своевременно принял меры для прекращения нарушения. Указанные критерии подвергаются критике в литературе в связи с неоднозначностью их трактовки, чрезмерно широкими возможностями правообладателей, жесткостью условий по отношению к информационным посредникам, и, что особенно важно в контексте данной работы, в связи с возложением ответственности за размещение гиперссылок на неправомерно используемые результаты интеллектуальной деятельности[1].

В.О. Калятин пишет, что «ответственность за размещение гиперссылки – весьма спорное решение, применение которого возможно лишь в исключительных случаях»[2]. Однако что это за «исключительные случаи», автор не раскрывает, тогда как это имеет определяющее значение применительно к защите авторских и смежных прав при размещении гиперссылок на информационные ресурсы, содержащие нелегальный контент.

[1] *Савельев А.И.* Критерии наличия действительного и предполагаемого знания как условия привлечения к ответственности информационного посредника (URL: http://www.justicemaker.ru/ (дата обращения: 17.11.2016)).

[2] *Калятин В.О.* Подводные камни нового антипиратского закона // Патенты и лицензии. 2013. № 10 (URL: http://patents-and-licences.webzone.ru/ (дата обращения: 17.11.2016)).

В условиях недостаточно четкого и полного правового регулирования и судебная практика не отличается единообразием.

Например, определением Мосгорсуда был ограничен доступ к информационному ресурсу, содержащему гиперссылку на информацию, подлежащую ограничению в связи с требованиями Закона об информации. Суд счел, что в данном случае такое ограничение было «единственной возможностью выполнения требований законодательства»[1].

Арбитражный апелляционный суд признал гиперссылку способом использования средства индивидуализации: он запретил использование товарного знака и сходных с ними до степени смешения обозначений, в том числе «в гиперссылках и при других способах адресации»[2].

Противоположное мнение в отношении гиперссылки высказано в другом судебном акте Мосгорсуда. Суд прямо указал: «...гиперссылка не создает какую-либо связь между сайтом, на котором она размещена, и самим объектом. Данный способ указания на размещение объекта не является способом использования произведений»[3].

Аналогичная позиция отражена и в решении другого суда, который постановил, что «наличие ссылки не является нарушением авторских прав на произведение и не является действием по его распространению»[4]. Несмотря на то, что это дело рассматривалось достаточно давно, оно весьма интересно, так как основной рассматриваемый в нем вопрос – может ли сама по себе гиперссылка на контент, размещенный в сети Интернет с нарушениями норм авторского права, составлять такое нарушение?

Прямой ответ на такой вопрос в российском законодательстве не содержится. Но в контексте последних «антипиратских» поправок, внесенных в законодательство, он будет скорее положительным. Но дискуссия пока не завершена и в условиях отсутствия в отечественном праве доктринального анализа проблемы размещения гиперссылки в контексте права на доведение до всеобщего сведения, думаем, будет продолжаться.

---

[1] Апелляционное определение Московского городского суда от 28.04.2015 по делу № 33-15614 (URL: http://www.consultant.ru/ (дата обращения: 31.10.2016)).

[2] Постановление Девятого ААС от 23.11.2015 № 09АП-44727/2015 (URL: http://www.consultant.ru/ (дата обращения: 31.10.2016)).

[3] Апелляционное определение Московского городского суда от 20.06.2015 по делу № 33-18402 (URL: http://www.consultant.ru/ (дата обращения: 31.10.2016)).

[4] Решение Бабушкинского межмуниципальном суда г. Москвы от 18.01.2000 // Право и Интнрнет: очерки теории и практики / автор/создатель Наумов В.Б. (URL: http://window.edu.ru/ (дата обращения: 28.10.2016)).

Правовое регулирование размещения гиперссылок в сети Интернет в странах ЕС

Проблема правового регулирования размещения гиперссылок в сети Интернет носит поистине глобальный, международный характер.

Так, европейская судебная практика была крайне разрозненной вплоть до 2014 г., когда Суд ЕС вынес решение по делу *Nils Svensson and others v. Retriever Sverige AB*[1]. Иск был предъявлен правообладателями-журналистами к интернет-сервису, который по запросам своих пользователей осуществлял поиск и предоставлял результаты этого поиска в виде перечня гиперссылок на другой сайт. Предметом обжалования в этом деле было предоставление результатов поиска в виде перечня гиперссылок на сайт, на котором были правомерно опубликованы статьи истцов.

Решение Суда ЕС по этому делу часто называют «спасением Интернета», поскольку Суд не признал интернет-сервис нарушителем норм авторского права. При этом в решении Суда был сделан примечательный вывод: размещение гиперссылки в данном случае не может признаваться «доведением до всеобщего сведения», а, следовательно, использованием произведения, поскольку не соответствует критерию «новой публики» (*new public*). Иными словами, в рассматриваемом деле контент (произведения) уже был размещен в сети Интернет правообладателями, т.е. «доведен до всеобщего сведения», а следовательно, размещение гиперссылки не нарушает авторских прав, поскольку «новая публика» не вовлекается – ведь при размещении самого произведения в свободном доступе в сети оно уже стало доступно всем.

Интересной в связи со сказанным представляется проведенная А.В. Семеновым аналогия с доктриной «исчерпания права»[2]. С одной стороны, об исчерпании прав, бесспорно, не может быть и речи, так как сама по себе гиперссылка не распространяет произведение,

[1] Nils Svensson and Others v. Retriever Sverige AB. Judgment of the Court (Fourth Chamber) of 13 February 2014. Case C-466/12 (URL: http://curia.europa.eu/ (дата обращения: 28.10.2016)).

[2] *Семенов А.В.* Court of Justice Case C-466/12 – критерий «новой аудитории» для квалификации доведения до всеобщего сведения (URL: https://zakon.ru/discussion/2014/02/14/court_of_justice_case_c%E2%80%9146612__kriterij_novoj_auditorii_dlya_kvalifikacii_dovedeniya_do_vseobshhego_ (дата обращения: 31.10.2016)).

и, напротив, размещение правообладателем произведения в Интернете не лишает его права на распространение и доведение этого же произведения до всеобщего сведения посредством иных информационно-телекоммуникационных сетей. Но, с другой стороны, возможно расширительное толкование «исчерпания прав» применительно к новым технологиям. И, например, А.В. Антонова прямо говорит о том, что право на доведение до всеобщего сведения подлежит исчерпанию[1].

Но при том, что, например, в США доктрина исчерпания в Интернете не признается, в ЕС в определенных случаях такое исчерпание допускается[2]. Применительно же к анализируемому делу *Nils Svensson and others v. Retriever Sverige AB* следует обратить внимание читателей на доклад *ALAI*, в котором критикуется решение Суда ЕС вследствие несоответствия конструкции права на доведение до всеобщего сведения, предложенной Судом, европейскому и международному законодательству[3]. В частности, в этом докладе критерий «новой публики» трактуется как неправомерный аналог исчерпания авторского права.

Но есть и другие вопросы в развитие выводов Суда ЕС по делу *Nils Svensson and others v Retriever Sverige AB*. Например, в ситуации, когда контент сайта доступен только зарегистрированным пользователям или предоставляется за плату, пользователь легально получает легальный доступ к нему, а затем размещает произведение (без согласия правообладателя) в сети Интернет в открытом доступе. При этом тот же пользователь (или иное лицо) размещает в сети гиперссылку, по которой можно «пройти» к этому произведению. Исходя из логики решения Суда ЕС такое размещение гиперссылки будет представлять собой «доведение до всеобщего сведения», поскольку вовлекается «новая публика». Очевидно, что в этом случае можно говорить о нарушении авторских прав, и нарушителем будет именно тот, кто разместил соответствующее произведение в Интернете в открытом доступе. Однако можно ли признать самостоятельным нарушением и факт размещения гиперссылки?

---

[1] *Антонова А.В.* К вопросу о понятии права на «доведение произведения до всеобщего сведения», 16.12.2014 (URL: http://lexandbusiness.ru/ (дата обращения: 31.10.2016)).

[2] Например, правило об исчерпании, выработанное Судом ЕС для программ для ЭВМ, в Нидерландах используется для электронных книг (URL: http://ipkitten.blogspot.ru/2015/01/exhaustion-of-rights-first-sale.html (дата обращения: 12.11.2016)).

[3] ALAI OPINION on the criterion «New Public», developed by the Court of Justice of the European Union (CJEU), put in the context of making available and communication to the public,17.09.2014 (URL: http://www.alai.org/ (дата обращения: 31.10.2016)).

Для ответа на этот вопрос будет интересно ознакомиться с решением Суда ЕС по делам *Filmspeler*[1] и *GS Media v. Sanoma*, в основе которых лежит уже затрагиваемый вопрос об ответственности в связи с размещением гиперссылки на незаконно размещенный контент[2]. Спор возник в связи с размещением информационным ресурсом *GeenStijl* гиперссылки на фотографии из журнала *PlayBoy*, загруженные в Интернет в нарушение авторских прав.

Крайне любопытной представляется позиция генерального адвоката Суда ЕС по данному делу[3]. По его словам, гиперссылки не составляют акт «доведение до сведения» в принципе; исключением может являться только гиперссылка, по которой контент впервые попадает в сеть Интернет. А критерий «новой публики» применим только в том случае, если правообладатель первоначально выразил согласие на доведение до всеобщего сведения. То есть мнение генерального адвоката расходится с позицией, высказанной Судом по упомянутым выше делам. Генеральный адвокат придерживается позиции, согласно которой гиперссылки не нарушают авторское право, так как сами по себе они не предоставляют нелегальный контент, не являются единственной возможностью доступа к нему. По его мнению, иные трактовки понятия «доведения до всеобщего сведения» в контексте рассматриваемой проблемы определенно нанесут серьезный вред функционированию сети Интернет, разрушат баланс между интересами правообладателей и пользователей, с явным ущербом для прав последних. Генеральный адвокат в своей позиции исходит из того, что для правообладателей остаются возможными иные средства защиты своих прав.

Но, как известно, позиция адвоката не является обязательной для суда, поэтому Суд в деле *GS Media v. Sanoma* высказал следующую позицию. Размещение гиперссылки на нелегальный контент не является «доведением до всеобщего сведения», если такое размещение не преследовало извлечение выгоды (*financial gain*), и лицо, размещающее такую ссылку в сети, не знало/не должно было знать, что произведе-

[1] Stichting Brein v Jack Frederik Wullems (Case C-527/15) (URL: http://curia.europa.eu/ (дата обращения: 30.10.2016)).

[2] GS Media BV v Sanoma Media Netherlands BV, Playboy Enterprises International Inc., Britt Geertruida Dekker (Case C-160/15) (URL: http://curia.europa.eu/ (дата обращения: 12.11.2016)).

[3] OPINION OF ADVOCATE GENERAL. WATHELET delivered on 7 April 2016. Case C-160/15 (URL: http://curia.europa.eu/ (дата обращения: 30.10.2016)).

ния на другом веб-сайте размещены с нарушением авторских прав. В рассматриваемом споре было установлено, что *GeenStijl* преследовал коммерческую цель, поэтому решение было вынесено в пользу правообладателя. Таким образом, Суд ЕС признал, что в некоторых случаях (которые, по словам самого Суда, должны определяться на основании разработанных критериев для каждого конкретного дела индивидуально) размещение гиперссылки является использованием произведения, влекущим нарушение авторских прав[1].

Однако далеко не все согласны с такой «расстановкой сил». Данное решение подверглось критике со стороны сообщества пользователей, поисковых систем, поскольку необоснованно расширяет права правообладателей. Критику вызвали и сами критерии, которые, по мнению многих, не отличаются должной правовой определенностью и оставляют широкий простор для дальнейшего толкования[2]. Высказываются опасения, что решение по делу *GS Media v. Sanoma* затронет и некоммерческие сайты, приведет к излишнему увеличению судебных споров по данной проблематике[3].

Следует упомянуть и решение Суда ЕС по делу *BestWater*, суть которого заключается в признании законности использования «встроенных» ссылок (*embedding*) с аргументацией, аналогичной решению по делу *Nils Svensson and others v. Retriever Sverige AB* (не составляют «доведение до всеобщего сведения», отсутствует «новая публика» и новые технические средства)[4]. Германский суд, опираясь на аргументацию Суда ЕС, при рассмотрении дела *BestWater* впоследствии пришел к собственным выводам и несколько изменил решение по этому делу[5]. Это связано с тем, что Суд ЕС при рассмотрении дела не учитывал факт отсутствия согласия правообладателя на первоначальное «доведение до всеобщего сведения», а при его отсутствии, по мнению германского

[1] См.: Приложение 1. Eleonora Rosati. Linking after GS Media... in a table. 10.09.2016 (URL: http://ipkitten.blogspot.ru/ (дата обращения: 12.11.2016)).

[2] GLYN MOODY. Links to pirated content OK if non-commercial and unwitting, top EU court rules. 8/9/2016 (URL: http://arstechnica.co.uk/ (дата обращения: 12.11.2016)).

[3] *Emma Woollacott*. Playboy Hyperlink Victory Affects Non-Profit Websites Too (URL: http://www.forbes.com (дата обращения: 12.11.2016)).

[4] BestWater International GmbH v. Michael Mebes and Stefan Potsch. Order of the Court (Ninth Chamber) of 21 October 2014 (Case C-348/13) (URL: http://curia.europa.eu/ (дата обращения: 18.11.2016)).

[5] Communication to the public in copyright law - German struggle with the CJEU concept. Jan Bernd Nordemann. April 28, 2016 (URL: http://kluwercopyrightblog.com/ (дата обращения: 30.11.2016)).

суда, именно размещение гиперссылки становится актом «доведения до всеобщего сведения», а значит, и имеется нарушение авторских прав. Эта позиция затем нашла отражение в вышеописанном деле *GS Media v. Sanoma*.

Интересно, что суды Германии подходят к решению рассматриваемых вопросов с учетом вида гиперссылки, устанавливая, какой это вид – обычная текстовая, «глубокая», встроенная. Суд ЕС сказал, что встроенные ссылки рассматриваются наравне с обычными гиперссылками, но суды Германии исходят из другой позиции: на национальном уровне дело *Nils Svensson and others v. Retriever Sverige AB* рассматривается в контексте использования «глубоких» ссылок, *BestWater* – в контексте встроенных ссылок, а обычные текстовые ссылки вообще не признаются «доведением до сведения» вне зависимости от наличия «новой публики». Схожее мнение складывается и в практике Великобритании[1]. Но большинство европейских государств не учитывают видовые различия гиперссылок.

Правовое регулирование размещения гиперссылок в сети Интернет в Канаде и США

Познавателен опыт Канады, в практике которой гиперссылки разделяются на активируемые пользователем и автоматические (встроенные)[2]. Первый вид ссылок не предполагает загрузку контента или воспроизведение, поэтому такие ссылки не является согласно праву Канады «доведением до всеобщего сведения», не могут сами по себе нарушать авторские права[3]. Однако ссылки, переход по которым осуществляется автоматически, являются «доведением до всеобщего сведения». Как следствие, их размещение может быть признано нарушением авторских прав, но только в случае заведомого знания о противоправном характере контента.

[1] AN OVERVIEW OF INTERNATIONAL JURISPRUDENCE ON EMBEDDED LINKING AND FRAMING Edited by Fieldsher, Philipp Plog and Stephan Zimprich (Hamburg), Lucy Little and Beverley Potts (London), Bruno Ducoulombier and Nathalie Hadjadj-Cazier (Paris), Hakim Haouideg and Hanne Snoeks (Brussels) (URL: http://www.fieldfisher.com/ (дата обращения: 30.11.2016)).

[2] AIPPI Study Report 2016 – Study Question (Copyright) – Linking and making available on the Internet. Canada. Responsible Reporter: Yusuke INUI (URL: http://aippi.org/ (дата обращения: 31.10.2016)).

[3] National Post v. Fournier & Warman v. Fournier 2012 FC 803 (URL: https://elegal.ca/ (дата обращения: 30.11.2016)).

Обращает на себя внимание то, что в США право на «доведение до всеобщего сведения» не выделяется в качестве самостоятельного права, а охраняется в рамках права на воспроизведение, права на публичный показ, а также права на распространение произведения[1]. При этом судебная практика демонстрирует большое разнообразие: решение суда зачастую зависит не столько от вида гиперссылки или определенных критериев ее размещения, сколько от конкретных обстоятельств дела. Основная роль в поиске баланса отводится доктрине добросовестного использования (*fair use*), при это определяющим является вывод о том, что само по себе размещение гиперссылки не нарушает авторские права.

Так, в судебной практике гиперссылка сравнивается с адресом здания, открытым для публики и позволяющим найти информацию[2]. Делается вывод о том, что гиперссылка не представляет собой нарушение прав правообладателей, так как не содержит самого контента, охраняемого авторским правом (в отличие, например, от файлов *zip*-формата)[3].

В то же время использование гиперссылки может признаваться нарушением авторских прав при размещении таковой с переадресацией на заведомо нелегальный контент. В таких случаях возможно привлечение информационного посредника к ответственности на основе доктрины косвенного нарушения, и здесь для привлечения к «контрибуционной» ответственности достаточно двух факторов: ответчик знает или должен знать о нарушении авторских прав и вносит существенный вклад в такое нарушение[4].

Примеры использования этой доктрины применительно к размещению гиперссылок существуют в судебной практике[5]. Но стоит отметить, что условие о заведомом знании о нарушении не соблюдается по большей части в случае с поисковиками, информационными

[1] 17 U.S. Code § 106 – Exclusive rights in copyrighted works (URL: https://www.law.cornell.edu/ (дата обращения: 02.12.2016)).

[2] Ticketmaster Corp. v. Tickets.com, Inc., 2003 U.S. Dist. Case No. 99-CV-07654 (URL: http://web.archive.org/ (дата обращения: 02.12.2016)).

[3] Pearson Education, Inc., et al v. Ishayev et al, No. 1:2011cv05052 – Document 99 (S.D.N.Y. 2014) // URL: http://law.justia.com/ (дата обращения: 02.12.2016)).

[4] Contributory Infringement. Cornell University Law School (URL: https://www.law.cornell.edu/ (дата обращения: 04.12.2016)).

[5] Intellectual Reserve, Inc. v. Utah Lighthouse Ministry, Inc., Jerald Tanner, Sandra Tanner, et al., U.S. District Court, Utah, Case No. 2:99-CV-808C (URL: http://www.law.uh.edu/. (дата обращения: 04.12.2016)).

интернет-ресурсами, например, в деле *Flava Works, Inc. v. Gunter*[1] косвенное нарушение сайтами-поисковиками норм авторского права при размещении гиперссылки на нелегальный контент не было установлено.

Более того, в США возможно привлечение к ответственности за создание гиперссылки на контент, полученный в обход регистрационных и иных систем сайта, направленных на охрану авторских прав. Такие действия запрещаются Законом об авторском праве в цифровую эпоху США[2]. Однако судебная практика по вопросу применения данной статьи к вопросу гиперссылок непоследовательна, зависит от обстоятельств рассматриваемого дела. Например, в деле *Universal City Studios, Inc. v. Corley*[3] соответствующее нарушение было установлено, а в деле *Comcast v. Hightech Elecs., Inc.*[4] – нет.

Международно-правовой аспект правового регулирования размещения гиперссылок в сети Интернет

Проблема размещения гиперссылок в контексте авторского права актуальна во всем мире. О значимости ее разрешения и необходимости гармонизации законодательства свидетельствует, в частности, исследование Международной ассоциации по охране промышленной собственности (AIPPI), проведенное в 2016 г.[5], на его основе был составлен общий доклад по результатам анализа практики 41 государства[6] по вопросу права «доведение до всеобщего сведения» и размещения гиперссылок.

Согласно этому докладу в 45% государств размещение гиперссылки на правомерно и свободно размещенный правообладателем контент признается «доведением до сведения» (при этом только по-

[1] FLAVA WORKS, INC. v. MARQUES RONDALE GUNTER, doing business as myVidster.com; and SALSAINDY, LLC (URL: https://www.eff.org/ (дата обращения: 02.12.2016)).

[2] 17 U.S. Code § 1201(a)(2), (b) – Circumvention of copyright protection systems (URL: https://www.law.cornell.edu/ (дата обращения: 04.12.2016)).

[3] Universal City Studios, Inc. v. Corley, 273 F.3d 429 (2d Cir. 2001) (URL: http://cyber.law.harvard.edu/ (дата обращения: 02.12.2016)).

[4] Comcast v. Hightech Elecs., Inc., 2004 WL 1718522 (N.D.Ill. July 29, 2004) (URL: http://www.linksandlaw.com/ (дата обращения: 04.12.2016)).

[5] AIPPI Study Report 2016 – Study Question (Copyright) - Linking and making available on the Internet (URL: http://aippi.org/ (дата обращения: 04.12.2016)).

[6] Россия не принимала участия в данном исследовании.

ловина из этих 45% считают «доведением до всеобщего сведения»), причем многие эксперты ссылаются на решение по делу *Nils Svensson and others v. Retriever Sverige AB;* 95% государств отметили, что гиперссылка сама по себе (на главную страницу) не может нарушать авторские права.

Единственная страна, из участвующих в исследовании, заявившая о размещении гиперссылок в целом как о прямом нарушении авторских прав, – Мексика. В Мексике сложился подход, согласно которому использование гиперссылок составляет прямое нарушение норм авторского права на основе ст. 231-I Закона об авторском праве Мексики и ст. 8 ДАП (право на «доведение до всеобщего сведения»). Мексиканские эксперты утверждают, что гиперссылка – это часть акта «доведения до всеобщего сведения», так как предоставляет пользователям доступ к контенту, даже если ведет на главную страницу. Но, говоря о признании использования гиперссылок нарушением авторских прав, эксперты все-таки имеют в виду гиперссылки на нелегально размещенные в сети произведения, в связи с чем приводится следующий пример: информационный ресурс *Ba-k* был привлечен к ответственности, в частности, за размещение гиперссылок на «пиратский» контент (номер дела – I.M.C. 2036/2014(M-340)20996).

В целом же согласно докладу AIPPI позиция, в силу которой размещение гиперссылок на неправомерный контент, является нарушением авторских прав, придерживаются 65% опрошенных. Гораздо большую разбросанность во мнениях демонстрирует вопрос о влиянии видов гиперссылок на их рассмотрение в рамках авторского права.

Выводы и предложения по совершенствованию законодательства

Таким образом, следует признать, что практика использования гиперссылок в Интернете нуждается в подчинении единым стандартам. Для этого необходимо учитывать как национальный опыт, так и зарубежный. Ведь противоречия лежат в понимании самой сути гиперссылки в отсутствие единой трактовки данного явления в рамках авторского права.

На основании проведенного исследования наиболее обоснованной представляется позиция, согласно которой гиперссылка является особым явлением, который лишь при наличии определенных критериев может рассматриваться как способ использования объекта интеллектуальной собственности. И именно на разработке таких критериев,

основанных на балансе интересов пользователей и правообладателей, необходимо сосредоточить усилия.

Здесь стоит отметить положительный опыт Суда ЕС, который, несмотря на возникающие противоречия, стремится к достижению правовой определенности по вопросу использования гиперссылок. В России ситуация осложняется отсутствием доктринальных исследований по тематике гиперссылок в контексте права на «доведение до всеобщего сведения». И здесь следует подчеркнуть, что обозначенная проблема должна решаться комплексно и не только на национальном уровне. Без межгосударственного сотрудничества, международно-правовой унификации подходов к определению сущности гиперссылок и правовых последствий их размещения в сети Интернет построение информационного правового общества будет осложнено.

Пристатейный библиографический список:

1. *Антонова А.В.* К вопросу о понятии права на «доведение произведения до всеобщего сведения». 16.12.2014 (URL: http://lexandbusiness.ru/).

2. Большой толковый словарь русского язика / С.А. Кузнецов. СПб.: Норинт, 1998.

3. *Гринюк М.* Гиперссылки. Правовые проблемы, возникающие с их использованием. Право и интернет: сб. ст., 2004 (URL: http://www.allpravo.ru).

4. *Калятин В.О.* Подводные камни нового антипиратского закона // Патенты и лицензии. 2013. № 10 (URL: http://patents-and-licences.webzone.ru/).

5. *Калятин В.О.* Правовые проблемы использования произведения в Интернете (Информационное право. 2005. № 1) (URL: http://www.center-bereg.ru/).

6. *Савельев А.И.* Критерии наличия действительного и предполагаемого знания как условия привлечения к ответственности информационного посредника (URL: http://www.justicemaker.ru/).

7. *Семенов А.В.* Court of Justice Case C-466/12 – критерий «новой аудитории» для квалификации доведения до всеобщего сведения (URL: https://zakon.ru/).

8. 8AIPPI Study Report 2016 – Study Question (Copyright) – Linking and making available on the Internet (URL: http://aippi.org/).

9. ALAI OPINION on the criterion «New Public», developed by the Court of Justice of the European Union (CJEU), put in the context of making available and communication to the public. 17.09.2014 (URL: http://www.alai.org/).

10. OVERVIEW OF INTERNATIONAL JURISPRUDENCE ON EMBEDDED LINKING AND FRAMING Edited by Fieldsher, Philipp Plog and Stephan Zimprich (Hamburg), Lucy Little and Beverley Potts (London), Bruno Ducoulombier and Nathalie Hadjadj-Cazier (Paris), Hakim Haouideg and Hanne Snoeks (Brussels) (URL: http://www.field-fisher.com/).

11. Communication to the public in copyright law - German struggle with the CJEU concept. Jan Bernd Nordemann. April 28, 2016 (URL: http://kluwercopyrightblog.com/).

12. Connecting to Other Websites. Stanford University Library (URL: http://fairuse.stanford.edu/).

13. Contributory Infringement. Cornell University Law School (URL: https://www.law.cornell.edu/).

14. *Malama Georgia* COPYRIGHT ASPECTS OF LINKING AND FRAMING. December 2013 (URL: https://repository.ihu.edu.gr/).

15. GLYN MOODY. Links to pirated content OK if non-commercial and unwitting, top EU court rules. 8/9/2016 (URL: http://arstechnica.co.uk/).

16. *Woollacott Emma*. Playboy Hyperlink Victory Affects Non-Profit Websites Too (URL: http://www.forbes.com).

17. *Burri Mira*. Permission to Link: Making Available via Hyperlinks in the European Union after Svensson (URL: http://www.jipitec.eu/).

18. OPINION OF ADVOCATE GENERAL. WATHELET delivered on 7 April 2016. Case C-160/15 (URL: http://curia.europa.eu/).

19. *Torremans Paul*. Research Handbook on Cross-border Enforcement of Intellectual Property. EE Elgar Publishing, 2014.

20. 17 U.S. Code (URL: https://www.law.cornell.edu/).

Приложение

Таблица по критериям, выработанным судом ЕС для определения наличия возможного нарушения авторского права путем размещения гиперссылки в сети Интернет. Источник: Eleonora Rosati. Linking after GS Media ... in a table. 10.09.2016 (URL: http://ipkitten.blogspot.ru/ (дата обращения: 12.11.2016)).

Linking after *GS Media*, C-160/15

Accessibility of content	Content published with rightholder's consent	Profitmaking intention	Knowledge that content linked to is unlawful	Act of communication to the public	Potential infringement
Freely accessible	Yes	n/a	n/a	No (*Svensson, GS Media*)	No
Not freely accessible	Yes	n/a	n/a	Yes (*BestWater, GS Media*)	Yes
Freely accessible	No	No	No	No (*GS Media*)	No
Freely accessible	No	No	Yes (eg because notified	Yes (*GS Media*)	Yes*
Freely accessible	No	Yes	Presumed (rebuttable presumption)	Yes (*GS Media*)	Yes*
Not freely accessible	No	n/a	n/a	Yes	Yes

*If rightholder notifies link provider (without prior knowledge of unlawfulness) that content linked to is unlawful and he refuses to remove the link, and exceptions in Article 5(3) InfoSoc Directive are inapplicable.

Ю.В. Русанова

ЛИЦЕНЗИИ CREATIVE COMMONS[1]

Аннотация. *Данное исследование посвящено проблеме лицензий Creative Commons. В работе они рассматриваются как альтернатива или дополнение традиционному авторскому праву. Автор отдельно уделяет внимание вопросу целесообразности дополнения российского законодательства, в частности Гражданского кодекса РФ, положениями о лицензиях Creative Commons.*

Ключевые слова: *лицензии Creative Commons, авторские и смежные права*.

С развитием информационных технологий и появлением сети Интернет привычные механизмы защиты авторских прав вдруг стали несостоятельными. Информация, ограниченная к распространению посредством авторских и смежных прав, расползается по сети так быстро, что остановить этот процесс практически невозможно.

Это легко проследить на примере борьбы с несанкционированным распространением музыки в Интернете, в частности в социальных сетях. Единожды появившись в свободном доступе, музыкальный трек будет появляться там снова и снова, поскольку пользователи, успевшие загрузить его на свое электронное устройство или каким-либо иным способом сделать копию после удаления музыкального произведения администратором, могут снова загружать его в сеть или отправлять адресно иным пользователям.

Разумеется, механизм, охраняющий авторские и смежные права, работает очень быстро, позволяя легко находить неправомерно размещенные произведения в Интернете и удалять их. Нет особой сложности в создании бота, который будет находить, скажем, музыкальные произведения по определенному заданному запросу и их вычищать. На мой взгляд, проблема кроется в другом. С возникновением Интернета складывается определенное мышление: люди привыкают к свободному распространению информации и противятся вероятным препятствиям

[1] Статья победителя конкурса IP & IT LAW – 2017.

к этому. Свободное распространение результатов интеллектуального труда способствует развитию инноваций, свободному творчеству, передаче идей и знаний без каких-либо барьеров. Чем большее количество человек получает наиболее свободный и быстрый доступ к результату чьего-либо творчества, тем больше вероятность, что идея будет развита, получит новое применение, даст толчок к вдохновению – и будет создано что-то еще.

Пакет защиты прав правообладателя может не удовлетворять его своей избыточностью. Многие авторы и обладатели смежных прав заинтересованы как можно в более широком распространении их произведения, что затрудняется действующим законодательством. Особенно свободное распространение может быть выгодно лицу на старте его творческой карьеры, когда необходимо как можно громче заявить о себе и распространить экземпляры своего творчества. Именно этими соображениями руководствовались создатели лицензий *Creative Commons* (далее – лицензии *CC*), стремясь создать модель регулирования, которая, с одной стороны, оставалась бы в правовых рамках и, с другой стороны, давала больше свободы выбора.

Лицензии *Creative Commons* – идеи и принципы

Идея лицензий, с помощью которых правообладатель может отказываться от части прав, предоставляемых ему авторским законодательством, была предложена некоммерческой организацией *Creative Commons*. Никоим образом не затрагивая неимущественные права авторов, такие как право автора на имя, лицензии *CC* ограничивают имущественные права правообладателей, заменяя конструкцию *All rights Reserved* на модель *Some Rights Reserved*[1].

Лицензии *CC* в разрезе договорного права представляют собой договор присоединения (*contrat d'adhésion*), так как лицензиат не может обсуждать условия договора. Ему предоставляются две опции – отказаться от договора или согласиться его заключить.

На практике часто возникает путаница лицензий *CC* с договорами дарения, поскольку предполагается, что правообладатель «дарит» часть своих прав. Такое заблуждение появилось вследствие следования ошибочной логике распространения регулирования вещных прав по аналогии с регулированием прав интеллектуальных. Как от-

[1] *Долгин А.Б.* Экономика символического обмена. М.: Инфра-М, 2006. С. 417

мечал О.С. Йоффе, «одаряемый становится собственником имущества, не принимая на себя каких-либо обязанностей перед дарителем, который в свою очередь уступает право собственности одаряемому, не приобретая каких-либо прав»[1]. Однако лицензия *CC* представляет собой лицензионный договор, который не является односторонне обязывающим, – права и обязанности возникают у обеих сторон. В частности, по лицензиям *CC* лицензиат обязуется выполнять условия, указанные в договоре, например указывать имя автора.

Аналитический доклад по лицензиям *CC* содержит указание на то, что такие лицензии преследуют определенную цель: правообладатель должен иметь возможность «идентифицировать непосредственный объект, который он желает предоставить для использования на изложенных в лицензии условиях неопределенному кругу лиц»[2].

Преимуществом лицензий *CC* является то, что они понятны среднестатистическому обывателю: не содержат сложных правовых конструкций и обозначаются значками и словосочетаниями. Например, значок с зачеркнутым долларом и подписью *Non commercial* означает, что правообладатель запрещает использовать произведение с целью извлечения прибыли.

Лицензии *CC* являются «обкатанными» стандартными договорами, что является еще одним их преимуществом. Для сторон этого договора (вернее, для правообладателя, потому что именно он в одностороннем порядке вырабатывает условия предоставления третьим лицам права на использование своего произведения) намного проще использовать стандартную лицензию, многократно опробованную на практике и широко себя зарекомендовавшую, нежели формулировать новый контракт.

Нельзя не заметить, что регулирование, подобное механизму лицензий *CC*, уже включено в российское законодательство: 12.03.2014 ГК РФ был дополнен ст. 1286.1 об открытых лицензиях на использование произведений науки, литературы или искусства. Содержание статьи приблизительно отражает идеи лицензии *CC*, например абз. 2 п. 2 ст. 1286.1 ГК РФ, говоря о возможности предоставления лицензиаром права неограниченному количеству лиц на использование произведе-

[1] *Иоффе О.С.* Обязательственное право. М., 1975. С. 394.

[2] Использование лицензий Creative Commons в Российской Федерации: аналитический доклад / под ред. Ю.Е. Хохлова. М.: Институт развития информационного общества, 2011. С. 37 (URL: http://creativecommons.ru/sites/creativecommons.ru/files/docs/ispolzovanie_ss_v_rf.pdf (дата обращения: 16.01.2017)).

ния для создания нового результата интеллектуальной деятельности, отсылает нас к одной из лицензий *CC – Share Alike*.

На мой взгляд, введение данной статьи в ГК РФ уже само по себе является большим прорывом для либерализации гражданского законодательства в сфере авторского права. В конце концов, обладатель исключительного права согласно ст. 1229 ГК РФ может пользоваться результатами интеллектуальной деятельности по своему усмотрению, поэтому тем более странно, что подобная норма появилась в ГК РФ так поздно.

Сравнивая упомянутую норму ст. 1286.1 ГК РФ с содержанием лицензий *CC*, можно заметить следующее: ст. 1286.1 является слишком общей, предоставляя правообладателю самому выбрать из всего многообразия способов распоряжения правами наиболее ему подходящий и сформулировать его в открытой лицензии. Это является одновременно преимуществом и недостатком: правообладатель имеет возможность сконструировать условия лицензии так, как ему удобно, на оптимальный для него срок, но если у него нет идей и принципиальных стратегий относительно распоряжения своими правами, создание открытой лицензии может стать затруднительным. В то же время, как уже говорилось, лицензии *CC* предлагают готовые варианты-шаблоны, которыми легко пользоваться, особенно если речь идет о распоряжении целым пакетом прав не на одно произведение, а на несколько.

В настоящий момент многие правообладатели по всему миру используют лицензии *CC*. Мировыми платформами, применяющими лицензии *CC*, являются *YouTube*, *Flickr*, *Jamendo*, *Wikipedia*, *Bandcamp* и др. В России это, в частности, некоторые страницы сайта МГИМО, сайт НИУ ВШЭ, сайт Роснано.

Согласно данным на 2011 г. (к сожалению, более свежих сведений сайт *Creative Commons* не предоставляет), более 580 млн произведений были распространены по лицензированию *CC* (можно представить, какова цифра на 2017 г.). *Creative Commons* постепенно совершенствует и адаптирует свои лицензии для разных стран – сейчас такие адаптации разработаны для 60 стран мира.

Creative Commons представляет следующие наиболее распространенные лицензии:

1) **Attribution** (с указанием авторства) – по данной лицензии пользователь практически полностью свободен в своих действиях, но обязан при распространении, переработке и ином использовании указать автора;

2) **Non Commercial** – уже упоминавшаяся лицензия разрешает любое использование, кроме коммерческого, т.е. преследующего цель извлечения прибыли;

3) **No Derivative Works** – пользователь вправе как угодно использовать произведение, но для какой-либо переработки или изменения требуется согласие правообладателя;

4) **Share Alike** – наиболее точно выражает принципы копилефта. Пользователю разрешается использовать оригинальное произведение, на его основе создавать собственное (производное) произведение, но при этом при распространении вновь созданного (производного) произведения обязательно использовать ту же лицензию, что и автор первоначального (оригинального) произведения или его правообладатель.

Все остальные виды лицензий содержат смешение данных условий. Большинство лицензий включают одну-две из перечисленных, например: *Attribution Non-Commercial No Derivatives*. Как мы можем видеть, первая лицензия – *Attribution* – фактически переводит произведение в общественное достояние: правообладатель оставляет за собой только неимущественные права – право на имя и его указание на экземплярах произведения.

Сайт *Creative Commons* позволяет создать свою уникальную лицензию – *Creative Commons Custom License*[1]. Таким образом, если правообладателю не слишком подходят стандартизированные лицензии, он сможет сконструировать свою собственную.

Все лицензии *CC* требуют указания автора произведения[2]. Такое условие объясняется прежде всего тем, что упоминание авторства является неотчуждаемым правом автора, закрепленным Бернской конвенцией (на которую опирается *CC* в своих идеях). Кроме того, свободное распространение произведений, позволяющее автору расширять охват своей аудитории, является важнейшим принципом *CC*, без которых выгода от использования лицензий *CC* сходит на нет.

При использовании произведения по лицензии *CC* рекомендуется указывать имя/псевдоним автора, источник, откуда было взято произведение (это может быть, например, гиперссылка на страницу автора в сети Интернет), используемую автором лицензию. При

[1] *Долгин А.Б.* Экономика символического обмена. С. 417

[2] Сайт Creative Commons (URL: http://creativecommons.ru/faq/ (дата обращения: 20.01.2017)).

распространении производного произведения (созданного на основе чужого оригинального произведения) необходимо оповещение о том, что производный результат интеллектуальной деятельности является модификацией или основой для другого произведения[1].

Весьма полезной моделью, на мой взгляд, является лицензия *Share Alike* – именно благодаря ей свободно распространяемых произведений становится больше. Это связано с тем, что автор производного произведения обязан использовать ту же лицензию, что была использована для первоначальной (оригинальной) работы. Вместе с тем не очень ясно, какие санкции будут применены к правообладателю производного произведения, если тот будет использовать всю полноту предоставленных ему законом авторских прав, не ограничиваясь предоставленными лицензией *CC*.

Указывая имя автора первоначального (оригинального) произведения и его источник, не используя это произведение в коммерческих целях, правообладатель производного произведения фактически выполняет все условия по соблюдению чужих исключительных прав. Кто же может принудить его ограничить свои собственные? В этом, на мой взгляд, заключается один из возможных недостатков лицензий *CC* – благородные идеи по свободному распространению результатов интеллектуального труда и самоограничению в правах могут поддержать не все пользователи, а *Creative Commons* как некоммерческая организация не обладает аппаратом принуждения. Наконец, не во всех юрисдикциях отказ от части прав (а иногда и отказ от всех прав – если лицензия фактически переводит произведение в общественное достояние) может быть признан действительным.

Вопрос имплементации лицензий *CC* в российское право

На мой взгляд, существует три возможных пути реализации идей и принципов *Creative Commons* в российском праве:

1) включение нескольких наиболее распространенных лицензий *CC* в гражданское законодательство на основе диспозитивного метода – правообладатель может выбирать любую подходящую ему модель лицензионного договора, а может на основании ст. 1286.1 ГК РФ сформулировать собственный договор;

[1] Сайт Creative Commons (URL: http://creativecommons.ru/faq/ (дата обращения: 20.01.2017)).

2) внесение изменений в законодательство и нормативные правовые акты, касающиеся организаций по управлению правами на коллективной основе: некоторые из типовых договоров, заключаемых организациями с правообладателями, должны содержать принципы *CC*;

3) «невмешательство» в использование правообладателями и лицензиатами лицензий *CC* с оставлением существующего порядка вещей. Идеи свободного обмена могут популяризироваться их сторонниками, такими как некоммерческая организация *Creative Commons*, тогда как законодательство не должно быть перегружено частными вариантами одного гражданско-правового договора.

Далее я предлагаю разобрать преимущества и недостатки всех трех подходов.

Первый подход: нуждается ли ГК РФ в дополнении лицензиями Creative Commons?

Одним из вариантов решения вопроса могло бы стать увеличение количества разновидностей оберточных лицензий в гражданском законодательстве. Загвоздка кроется в следующем: каким образом правообладатели должны выбирать тот или иной механизм?

В настоящее время мы имеем своеобразную презумпцию авторства: автор не должен ни регистрировать свое авторство, ни выполнять какие-либо еще формальности – достаточно, чтобы на оригинале или экземпляре произведения стояло его имя. Как уже говорилось, данная модель регулирования была рассчитана на неосведомленного в правовом смысле правообладателя. Каким же образом такой правообладатель будет выбирать между двумя видами лицензионных открытых договоров? Вернее, не только двумя: *Creative Commons* предлагает множество разных видов лицензий. Гражданское законодательство должно включать их все?

Представляется, что этот вариант отнюдь не предполагает полное копирование лицензий *CC* с отсылкой на них – достаточно включить в ГК РФ аналогичные механизмы, причем ничто не мешает включить лицензии *CC* в их первозданном виде – с аббревиатурами и значками. Сделать это следует в целях узнаваемости: как практически каждому известно, что © означает защиту авторских прав, так и значки лицензий *CC* будут легко считываться и узнаваться, что поспособствует предотвращению недоразумений и более эффективной защите интересов правообладателей.

А.И. Савельев к недостаткам свободных лицензий относит то, что большинство пользователей просто не знакомятся с ними по той причине, что это занимает слишком много времени[1]. Кроме того, как показывает практика, чтение каких-либо соглашений просто нехарактерно для обывательской культуры. С лицензиями *CC* вопрос обстоит проще: как правило, внизу страницы сайта указываются значки используемой лицензии, которые кратко уведомляют пользователя о режиме авторских прав. По моему мнению, это еще один плюс в пользу кратких обозначений лицензий наподобие *CC*.

Подход второй: лицензии CC в типовых договорах организаций, осуществляющих коллективное управление правом

Второе предлагаемое мной решение имеет свои существенные преимущества, что обосновывается следующими рассуждениями. Гражданское законодательство не должно бесконечно разрастаться, особенно в условиях, когда законы не отличаются высоким качеством правового регулирования. В ГК РФ уже есть статья, регулирующая свободные лицензии, – ст. 1286.1: она содержит общие правила. При этом ГК РФ не нуждается в регламентации различных модификаций одного и того же договора.

Вместе с тем лицензии *CC*, используемые всем цивилизованным миром, весьма удобны и эффективны, поэтому нельзя их игнорировать, а их конструкции могут быть восприняты отечественным правом. Поэтому организации по коллективному управлению авторскими и смежными правами могли бы способствовать распространению лицензий *CC*. Заключая договор о передаче полномочий по управлению такими правами, правообладатель мог включать в него условие о том, что организация обязана предоставлять использование его произведения на условиях определенной открытой лицензии.

Например, организация, управляющая в том числе правами конкретного певца-исполнителя, по договору с этим исполнителем предоставляет право использования его исполнений на основе лицензии *CC-BY-NC*, т.е. лицензии *CC Attribution – Non commercial*, которая

[1] *Савельев А.И.* Комментарии на предлагаемую в проект изменений в часть 4 ГК РФ концепцию регулирования отношений, возникающих в связи со свободным использованием и распространением объектов авторских прав (URL: http://www.schoolprivlaw.ru/files/kommentarii.pdf (дата обращения: 17.01.2017)).

предусматривает использование с указанием наличия смежного права, не преследующее извлечение прибыли.

Согласно абз. 2 п. 5 ст. 1243 ГК РФ организация по управлению правами на коллективной основе размещает в общедоступной информационной системе информацию о правах, переданных ей в управление, включая наименование объекта авторских или смежных прав, имя автора или иного правообладателя. Организацию по коллективному управлению правами можно также обязать размещать в общедоступной системе информацию об условиях лицензий, на основании которых возможно использование объекта авторских или смежных прав.

Соответственно ст. 1243 можно изменить и дополнить следующим образом: «Организация по управлению правами на коллективной основе размещает информацию в общедоступной системе в информационно-телекоммуникационной сети «Интернет» о правах, переданных ей в управление, включая наименование объекта авторских или смежных прав, имя автора или иного правообладателя, условия лицензионных договоров, посредством заключения которых пользователь может осуществить использование объекта авторских или смежных прав».

Дальнейшее раскрытие сути типовых лицензионных договоров, которые должны иметь в своем «арсенале» организации по коллективному управлению правами, может реализоваться в нормативных правовых актах, скажем, в постановлениях Правительства РФ или актах создаваемого мегарегулятора авторских и смежных прав. Таким образом, правообладатель, заключая договор о передаче полномочий на управление своими авторскими и (или) смежными правами с соответствующей организацией, может выбрать из предлагаемого списка типовых соглашений с пользователями тот, который для него оптимален. Это значительно упростит для правообладателя выбор того правового режима, который будет использоваться организацией для управнения его правами. Такие типовые договоры могут полностью или частично повторять лицензии *CC*.

Другим подходящим, на мой взгляд, вариантом могло бы стать не создание типовых договоров, а признание системы *CC* в целом с возможностью «перенять» ее лицензии в том виде, в каком они сформулированы организацией *Creative Commons*. Таким образом, правообладатель, заключая договор с организацией по управлению коллективными правами, мог бы просто указать, что организация должна управлять его авторскими или смежными правами и заключать лицензионные

договоры на основе лицензии *CC*, а именно, например, лицензии *CC Attribution – Noncommercial – Share Alike*.

Подход третий: сохранение status quo

Идея третьего подхода отчасти повторяет основную мысль второго: отечественное гражданское законодательство уже содержит конструкцию открытой лицензии, детализировать которую нецелесообразно. Организации по коллективному управлению правами вольны предлагать правообладателям любые договоры, с персональным подходом или же типовые, определяемые такой организацией. Идеи *Creative Commons* могут популяризироваться организацией по управлению правами, или же организация может руководствоваться иными принципами. В конце концов, при отказе от многих прав правообладателем организация по управлению коллективными правами уже не так нужна, разве что для сбора вознаграждения.

В целом данный подход можно охарактеризовать следующим образом: свобода договора в рамках существующего законодательства позволяет правообладателям и пользователям заключать любые соглашения (в рамках действующего законодательства, разумеется), в том числе договоры, аналогичные лицензионным договорам *CC*. Нет нужды для вмешательства в данный процесс.

Поиск оптимального решения

Подводя итог, полагаю, что наиболее взвешенными и целесообразными являются второй и третий подходы. Не следует изобретать велосипед: мы имеем подходящую конструкцию в ГК РФ (ст. 1286.1), разбивать которую на множество вариантов бессмысленно.

На мой взгляд, поспешно отказываться от привычного регулирования прав правообладателей было бы неправильно. Защита, представляемая частью четвертой ГК РФ, рассчитана скорее на плохо осведомленного правообладателя – она защищает «вольного художника», который не искушен в юридических тонкостях, и это представляется разумным. Полагаю, что правообладатель по закону должен иметь максимум прав, позволяющих выгодно использовать свое произведение. Обладая таким «пакетом» прав, автор должен иметь и возможность свободно распоряжаться ими, в том числе отказываться от них, если это отвечает его интересам и потребностям.

Проблема, на мой взгляд, кроется еще в том, что информация о существовании лицензий *CC* недостаточно распространена среди населения, на сегодняшний день распространение сведений об этих лицензиях – дело энтузиастов. Между тем авторы и правообладатели должны знать об альтернативном способе регулирования своих прав, поскольку лицензии *CC* действительно удобны и полезны.

Проблемы применения лицензий *CC* и судебная практика

Одной из проблем, связанных с применением лицензий *CC*, является то, что типовые тексты лицензий не содержат сведений о том, право использования на какое произведение предоставляется. При этом многие правообладатели делают отметку на своих сайтах о том, что предоставляют материалы на условиях той или иной лицензии *CC*, но нигде не указывают, на какие именно результаты интеллектуальной деятельности лицензия распространяется[1].

Согласно гражданскому законодательству Российской Федерации предмет лицензионного договора является его существенным условием, и без его указания договор будет считаться незаключенным. Вследствие этого применение лицензий *CC* становится проблематичным: в случае возникновения разногласий лицу, использовавшему произведение, будет трудно доказать, что правообладатель разрешил такое использование по открытой лицензии (например, если информация с сайта будет удалена)[2].

Обозначенная проблема представляется аргументом в пользу первого предложенного мной подхода: включая в ГК РФ различные виды лицензий *CC*, законодатель должен указать как обязательное условие заключения лицензионного договора условие о предмете договора.

Но на самом деле ничто не мешает и сейчас правообладателям размещать информацию о возможности использования их произведений на основе лицензий *CC* с уточнением, на какие произведения распространяется лицензия. Трудность заключается в том, что пользователи системы *Creative Commons* исходят из того, что одной только ссылки на лицензию *CC* достаточно для ее использования – не уточняя, права

[1] Сайт Фонда Свободы Информации и Института Развития Свободы Информации (URL: http:// www.svobodainfo.org/ (дата обращения: 16.01.2017)).

[2] *Зданович Г.В.* К вопросу о содержании свободной лицензии // Бизнес. Образование. Право. Вестник Волгоградского института бизнеса. 2014. № 2 (27). С. 282.

на какие конкретно результаты интеллектуальной деятельности они предоставляют по лицензии.

В связи с этим нельзя не отметить, что идея профессора Л. Лессига, ставшего основоположником лицензии *CC*, в свое время вызвала значительный резонанс. Многие противники свободных лицензий утверждали, что лицензия *CC* противоречит традиционному авторскому праву, способствует пиратству и противопоставляется закону.

Подобные мнения представляются в корне неверными. Использование лицензий *CC* является добровольным и никем не навязывается, а распоряжение своими правами путем заключения лицензионных договоров или отказа от части прав предусматривается законодательством большинства государств, в том числе и России. Лицензии *CC* не противоречат законодательству РФ и вполне вписываются в лицензионную систему, предлагаемую ГК РФ. Как отмечает А.И. Савельев, свободные лицензии (такие, как лицензии *CC*) и классические лицензии авторского права имеют одинаковую природу[1].

При изучении складывающейся судебной практики по рассматриваемому вопросу можно сделать вывод о том, что суды по-разному подходят к вопросу о правомерности использования лицензий *CC*. Хотя тенденция судебной практики – признавать их допустимость.

Так, в нескольких делах, рассмотренных районными судами (дело № 2-2353/16[2] и № 2-7524/2015[3]), в качестве истца выступало одно и то же лицо – В.В. Постников, который предъявлял требования о защите своих авторских прав разным ответчикам. В первом случае сделанная им и обработанная в графическом редакторе фотография была размещена в качестве стенда в магазине «Спортмастер», во втором – другое фото истца оказалось размещенным в торговом центре «Алатырь».

[1] *Савельев А.И.* Лицензирование программного обеспечения в России: законодательство и практика. М.: Инфотропик Медиа, 2013. С. 213.

[2] Решение Кировского районного суда г. Екатеринбурга от 18.04.2016 № 2-2353/16 // Архив решений арбитражных судов и судов общей юрисдикции (http://sudrf.kodeks.ru: http://sudact.ru/regular/doc/oMs5TU0FMUVQ/?regular-txt=Creative+Commons&regular-case_doc=&regular-doc_type=&regular-date_from=&regular-date_to=&regular-workflow_stage=&regular-area=&regular-court=&regular-judge=&_=1484840355896&snippet_pos=2014#snippet (дата обращения: 19.01.2017)).

[3] Решение Черемушкинского районного суда г. Москвы от 14.12.2015 по делу № 2-7524/2015 //Архив решений арбитражных судов и судов общей юрисдикции (http://sudrf.kodeks.ru: http://sudact.ru/regular/doc/WfSfR5kTAu6C/?regular-txt=Creative+Commons&regular-case_doc=&regular-doc_type=&regular-date_from=&regular-date_to=&regular-workflow_stage=&regular-area=&regular-court=&regular-judge=&_= 1484840355896&snippet_pos=1570#snippet (дата обращения: 19.01.2017)).

В обоих случаях истец выложил сделанные им фотографии на сайте *wikipedia.org*, откуда они были взяты ответчиками. Размещение фотографий на стендах истец посчитал незаконным воспроизведением своих фотографий, поскольку оно было совершено без его согласия. Ответчики в обоих случаях возражали, ссылаясь на тот факт, что информация, размещенная на сайте «Википедия», подпадает под условия, указанные в лицензии *CC Attribution-Share Alike 3.0 Unported* – эта лицензия не запрещает использование фотографии иными лицами.

Суды признали их доводы несостоятельными, поскольку ответчики не указали истца в качестве автора произведения, его имени не было на стендах. В итоге оба дела были разрешены в пользу истца: судами было признано, что ответчики не имели права воспроизводить фотографии истца в коммерческих целях без разрешения автора и выплаты ему вознаграждения. Таким образом, суды признали правомерность использования лицензий *CC*; на основании использованной истцом лицензии *CC* был сделан вывод о неправомерном воспроизведении ответчиками фотографий.

В решении по другому делу суд указал, что «использование открытых лицензий, аналогичных лицензиям *Creative Commons*, регулируется ст. 1286.1 ГК РФ»[1]. В связи с этим интересно заметить, что до введения этой статьи, еще в 2011 г. суды ссылались на то, что условия лицензий *CC* применяться не могут, поскольку «это противоречит действующему законодательству РФ»[2]. Такую позицию можно было понять, поскольку в то время конструкция свободных лицензий в законодательстве отсутствовала, вследствие чего применение лицензий *CC* становилось действительно спорным.

В завершение этой части статьи следует заметить, что организация *Creative Commons* не оказывает юридической помощи при возникнове-

---

[1] Решение Центрального районного суда г. Тулы от 24.02.2015 № 2-341/15 2-341/2015 // Архив решений арбитражных судов и судов общей юрисдикции http://sudrf.kodeks.ru: http://sudact.ru/regular/doc/BGpbbN7j6gYe/?regular-txt=Creative+Commons&regular-case_doc=&regular-doc_type=&regular-date_from=&regular-date_to=&regular-workflow_stage=&regular-area=&regular-court=&regular-judge=&_=1484840355896&snippet_pos=6096#snippet (дата обращения: 19.01.2017).

[2] Определение Иркутского областного суда от 22.08.2011 № 33-8451/2011 // Архив решений арбитражных судов и судов общей юрисдикции http://sudrf.kodeks.ru: http://sudact.ru/regular/doc/YHHERV1dBn14/?regular-txt=Creative+Commons&regular-case_doc=&regular-doc_type=&regular-date_from=&regular-date_to=&regular-workflow_stage=&regular-area=&regular-court=&regular-judge=&_=1484840355896&snippet_pos=1806#snippet (дата обращения: 19.01.2017).

нии затруднительных ситуаций, связанных с лицензиями *CC*. Организация устраняется от разрешения спорных моментов, таких, например, как выяснение, является ли то или иное использование произведения коммерческим или нет[1], и это отчасти затрудняет использование лицензий *CC*. *Creative Commons* скорее помогает в толковании своих лицензий, чем оказывает правовую поддержку.

Заключение

На мой взгляд, предоставление исключительных прав на основе лицензий *CC* наиболее полно отвечает требованиям будущего, краеугольным камнем которых выступает Интернет. Какие бы новые механизмы удаления или блокировки неправомерно размещенной информации ни создавались, сеть Интернет остается открытым и доступным пространством.

Новаторство *Creative Commons* заключается не в лицензировании как таковом – лицензионные договоры присутствуют в законодательстве большинства стран, а в революционной идее свободного обмена произведениями на основе типовых лицензий с легко узнаваемыми обозначениями.

Интернет заставил многих задуматься о нежизнеспособности авторского права; все чаще можно услышать мнения о том, что право на доступ в Интернет, право на информацию и ее свободное получение является неотъемлемым правом человека, которое должно появиться в конституциях цивилизованных стран. Если следовать этой логике, вся информация, за исключением включающей государственную тайну или тайну частной жизни человека, должна свободно распространяться, стимулируя прогресс и творчество.

На мой взгляд, мир, в котором все свободно делятся результатами интеллектуальной деятельности, не пытаясь брать за это плату, несколько утопичен (во всяком случае, в обозримом будущем). Тем не менее лицензии *CC* способствуют поиску золотой середины между развивающимся информационным обществом, где информация имеет первоочередную ценность, и стремлением века Интернета сделать информацию общедоступным благом.

[1] Сайт Creative Commons (URL: http://creativecommons.ru/faq/ (дата обращения: 20.01.2017)).

Подводя итоги, хочу сказать, что имплементация лицензионных договоров *CC* в ГК РФ нецелесообразна, поскольку Кодекс содержит нормы о договоре открытого лицензирования, применительно к которому лицензии *CC* становятся лишь вариациями. Все эти вариации не требуется включать в Кодекс – в противном случае его нормы станут слишком громоздкими и, увы, нечеткими.

По моему мнению, лицензии *CC* имеют свои преимущества и заслуживают распространения и признания по всему миру (что и происходит). Они должны спокойно восприниматься и квалифицироваться отечественными правоприменителями, поскольку вписываются в существующий российский правопорядок. Необходима лишь популяризация лицензий *CC*.

Пристатейный библиографический список:

1. *Долгин А.Б.* Экономика символического обмена. М.: Инфра-М, 2006. – 632 с.

2. *Зданович Г.В.* К вопросу о содержании свободной лицензии // Бизнес. Образование. Право. Вестник Волгоградского института бизнеса. 2014. № 2 (27).

3. *Иоффе О.С.* Обязательственное право. М., 1975. – 673 с.

4. *Савельев А.И.* Комментарии на предлагаемую в проект изменений в часть 4 ГК РФ концепцию регулирования отношений, возникающих в связи со свободным использованием и распространением объектов авторских прав. URL: http://www.schoolprivlaw.ru/files/kommentarii.pdf (дата обращения: 17.01.2017).

5. *Савельев А.И.* Лицензирование программного обеспечения в России: законодательство и практика. М.: Инфотропик Медиа, 2013. – 416 с.

6. Использование лицензий Creative Commons в Российской Федерации: аналитический доклад / под ред. Ю.Е. Хохлова. М.: Ин-т развития информационного общ-ва, 2011. – 94 с. (URL: http://creativecommons.ru/sites/creativecommons.ru/files/docs/ispolzovanie_ss_v_rf.pdf (дата обращения: 16.01.2017)).

7. Сайт Фонда Свободы Информации и Института Развития Свободы Информации (URL: http:// www.svobodainfo.org/ (дата обращения: 16.01.2017)).

8. Сайт Creative Commons (URL: http://creativecommons.ru/faq/ (дата обращения: 20.01.2017)).

А.Ю. Самсонова

ОТВЕТСТВЕННОСТЬ ПОИСКОВЫХ СИСТЕМ ПО ИСКАМ О НАРУШЕНИИ ПРАВ НА ТОВАРНЫЙ ЗНАК В СВЯЗИ С ИСПОЛЬЗОВАНИЕМ КЛЮЧЕВЫХ СЛОВ: РОССИЙСКАЯ И ЗАРУБЕЖНАЯ ПРАКТИКА

Аннотация. *В настоящее время широко распространена контекстная реклама в поисковых системах на основе ключевых слов, «запускающих» показ объявлений. В статье исследован вопрос о том, должна ли поисковая система привлекаться к ответственности за нарушение исключительных прав на товарный знак, если рекламодатель в качестве ключевого слова использует товарный знак, принадлежащий третьему лицу.*

Ключевые слова: *нарушение прав на товарные знаки, реклама с использованием ключевых слов.*

В последнее десятилетие реклама в сети Интернет стала одним из наиболее эффективных способов продвижения товаров и услуг. Помимо того, что объявления демонстрируются широкой аудитории пользователей, современные технологии позволяют персонализировать рекламу для каждого пользователя, предлагая именно то, что интересует его в данный момент. Ярким примером является контекстная реклама в поисковых системах, которые отображают объявления о товарах и услугах, соответствующих сделанному пользователем поисковому запросу.

Показ рекламных объявлений пользователям поисковых систем устроен следующим образом[1]. Рекламодатели выбирают так называемые ключевые слова – слова, при вводе которых в поисковую строку наряду с результатами «естественного» поиска будет показано объявление рекламодателя. Иными словами, ключевое слово – это своего рода метка, запускающая показ рекламного объявления, которое, как

[1] *Tan A.* Google Adwords: Trademark Infringer or Trade Liberalizer // Michigan Telecommunications and Technology Law Review. 2010. Vol. 16. Issue 2 (URL: http://repository.law.umich.edu/cgi/viewcontent.cgi?article=1049&context=mttlr (дата обращения 21.05.2017)). P. 475–476.

представляется рекламодателю, окажется интересным для данного пользователя.

С распространением контекстной рекламы в поисковых системах и продажи рекламодателям ключевых слов, которые могут совпадать с зарегистрированными словесными товарными знаками, возникла новая категория споров о защите прав на товарные знаки. Истцами в таких спорах выступают правообладатели исключительных прав на словесные товарные знаки, а ответчиками – их конкуренты, использующие для привлечения на свои сайты в сети Интернет ключевые слова, совпадающие с такими товарными знаками, и сами поисковые системы.

Обстоятельства подобных дел во многом схожи: в качестве нарушений правообладатели рассматривают демонстрацию пользователям поисковых систем контекстной рекламы компаний-конкурентов в ответ на поисковые запросы, содержащие словесные товарные знаки правообладателей. В таком случае одновременно с результатами поиска, сортированными поисковой системой по степени релевантности, в числе первых результатов пользователю будет представлено объявление со ссылкой, ведущей на сайт компании-конкурента, а не обладателя прав на товарный знак, которого, вероятнее всего, искал пользователь. Злоупотребление в использовании ключевых слов со стороны недобросовестных рекламодателей может быть расценено как нарушение прав владельца товарного знака.

Ответчиками по искам правообладателей чаще всего выступают рекламодатели, т.е. лица, избравшие в качестве ключевых слов слова, совпадающие со словесными товарными знаками истца. Однако иногда иски подаются и против самих поисковых систем, поскольку именно они организовывают показ объявлений и продажу ключевых слов. В мировой практике большое количество споров возникло после изменения крупнейшей поисковой системой *Google* политики продажи ключевых слов в рамках сервиса *AdWords*[1] и *Keyword Suggestion Tool*[2].

Услуга *Google AdWords* позволяет рекламодателям организовывать показ объявлений пользователям, использующим в поисковых запросах выбранные рекламодателями ключевые слова. При этом *Google* устанавливает определенные ограничения на использование ключе-

[1] Дословно: «Ключевые слова для рекламы» (англ.).

[2] Дословно: «Подсказчик ключевых слов» (англ.).

вых слов[1], в том числе с учетом географического фактора. Политика *AdWords*, т.е. правила, которые определяют порядок выбора ключевых слов, неоднократно претерпевала изменения.

Так, до 2004 г. использование товарных знаков, принадлежащих третьим лицам, в тексте объявлений и в качестве ключевых слов было запрещено. В 2004 г. эти правила были изменены: в США и Канаде рекламодатели получили возможность приобретать посредством аукциона ключевые слова, совпадающие со словесными товарными знаками третьих лиц[2]. Согласия правообладателя не требовалось, однако по его требованию мог быть установлен запрет на использование соответствующих слов в тексте объявления. В 2009 г. было разрешено ограниченное использование словесных товарных знаков в тексте объявления, если рекламодатель являлся продавцом оригинального товара, продавцом или производителем комплектующих или сопутствующих товаров или же предоставлял информацию или отзывы о продукте правообладателя. Правообладатели выступили против разрешения использовать ключевые слова, совпадающие с их словесными товарными знаками. В результате этого после 2004 г. *Google* столкнулся во многих юрисдикциях с волной исков о защите от нарушений прав на товарный знак.

Наибольшее количество судебных процессов против *Google* и его политики *AdWords* прошло в США. Основанием для исков послужил § 32(1) Закона о товарных знаках, известного также как Закон Лэнхема[3]. В соответствии со сложившимся в судебной практике толкованием положений Закона Лэнхема истец должен доказать присутствие следующих элементов:

1) товарный знак пользуется защитой в соответствии с Законом Лэнхема;

2) ответчик использовал товарный знак в коммерческой деятельности (*use in commerce*);

3) использование было осуществлено в связи с продажей или рекламой товаров или услуг;

---

[1] Google AdWords Policies // URL: https://support.google.com/adwordspolicy/answer/6008942?hl=en (дата обращения: 21.05.2017).

[2] *Scardamaglia A.* Keywords, Trademarks, and Search Engine Liability // *König R, Rasch M.* (eds), Society of the Query Reader: Re-ections on Web Search. Amsterdam: Institute of Network Cultures, 2014. P. 167.

[3] Lanham (Trademark) Act 1946, 15 U.S.C. // URL: https://www.law.cornell.edu/uscode/text/15/chapter-22 (дата обращения: 21.05.2017).

4) использование осуществлялось без согласия истца;

5) использование товарного знака ответчиком способно ввести в заблуждение относительно связи ответчика с истцом, а также создать впечатление того, что товары, услуги или коммерческая деятельность ответчика спонсируются или одобряются истцом[1].

Существенные противоречия в судебной практике США по делам о ключевых словах связаны с квалификацией использования ключевых слов, идентичных словесному товарному знаку, в качестве использования в коммерческой деятельности (*use in commerce*). До 2009 г. практика в рамках судебных округов существенно отличалась. В противоположность подходу, сложившемуся в большинстве судов США, районные суды Второго апелляционного округа (*Second Circuit*) были склонны признавать использование ключевых слов не связанным с коммерческой деятельностью. Причиной такого подхода являлось то, что использование ключевых слов расценивалось как строго внутреннее и обусловленное функциональной необходимостью.

Примерами дел, в которых использование ключевых слов было признано в качестве «*use in commerce*», являются, в частности, *American Blind and Wallpaper Factory Inc. v. Google*[2] (рассмотрено Федеральным районным судом по Северному округу Калифорнии, входящим в Девятый апелляционный округ) и *GEICO v. Google*[3] (рассмотрено Федеральным районным судом по Восточному округу Виргинии, входящим в Четвертый апелляционный округ).

Так, в решении по делу *GEICO v. Google*[4] суд признал использование совпадающих со словесными товарными знаками ключевых слов в качестве коммерческого использования (*use in commerce*). Отметив, что использование товарного знака в самом объявлении может ввести пользователей в заблуждение, суд признал, что истец не обосновал

[1] Lanham (Trademark) Act, §114, 1125(a); *Armstrong Paint&Varnish Works v. Nu-Enamel Corp.*, 305 US (1938) (URL: https://www.law.cornell.edu/supremecourt/text/305/315 (дата обращения: 21.05.2017)); *Government Employees Insurance Company v. Google, Inc. et al.*, U.S. District Court for the Eastern District of Virginia, 08.08.2005 (URL: http://blog.ericgoldman.org/archives/geicogoogleaug2005.pdf (дата обращения: 21.05.2017)). P. 7.

[2] *American Blind and Wallpaper Factory, Inc. v. Google, Inc.*, U.S. District Court for the Northern District of California, 18.04.2007 (URL: https://ia600302.us.archive.org/32/items/gov.uscourts.cand.15960/gov.uscourts.cand.15960.308.0.pdf (дата обращения: 21.05.2017)).

[3] *Government Employees Insurance Company v. Google, Inc. et al.*, U.S. District Court for the Eastern District of Virginia, 08.08.2005 (URL: http://blog.ericgoldman.org/archives/geicogoogleaug2005.pdf (дата обращения: 21.05.2017)).

[4] Там же.

вероятность введения пользователей в заблуждение в случаях, когда в тексте объявления товарный знак не используется. Однако суд не ответил на вопрос, может ли поисковая система нести ответственность за выбор ключевых слов, осуществленный пользователями[1].

Суды Второго апелляционного округа основывали мнение о том, что ключевые слова не являются *use in commerce*, на прецеденте *1-800 Contacts, Inc. v. WhenU.com, Inc.*[2]. Однако указанное судебное решение в действительности было связано с несколько иным использованием ключевых слов. Ответчик, *WhenU.com*, устанавливал на компьютеры пользователей программное обеспечение *SaveNow*, которое сохраняло информацию о поисковых запросах и предлагало всплывающие рекламные объявления. При этом ответчик не раскрывал никому используемые ключевые слова и не представлял возможность выбирать ключевые слова для показа объявлений, поэтому такое использование действительно можно было расценивать как строго внутреннее.

Суд Второго округа впервые признал использование ключевых слов в качестве *use in commerce* в решении по делу *Rescuecom v. Google*[3].

Дело *Rescuecom Corp. v. Google* прошло рассмотрение в двух инстанциях. Нарушением исключительных прав на товарный знак, по мнению истца, являлись сервисы *Google AdWords* и *Keyword Suggestion Tool*, которые позволяли его конкурентам приобретать показы своих рекламных объявлений в ответ на поисковые запросы, содержащие товарный знак истца. В своих возражениях ответчик ссылался на уже упомянутое дело *1-800 Contacts, Inc. v. WhenU.com, Inc.*, в котором было установлено, что ключевые слова не могут быть рассмотрены в качестве *use in commerce*.

Суд первой инстанции согласился с доводами ответчика и отклонил иск, признав *AdWords* и *Keyword Suggestion Tool* внутренним использованием и указав, что в тексте объявлений товарный знак истца не использовался.

Суд апелляционной инстанции это решение отменил, отправив дело на новое рассмотрение. Проанализировав ссылку истца на ре-

[1] URL: http://blog.ericgoldman.org/archives/geicogoogleaug2005.pdf (дата обращения: 21.05.2017)

[2] *1-800 Contacts, Inc. v. WhenU.com, Inc. & Vision Direct, Inc.,* Docket Nos. 04-0026-CV(L), 04-0446-CV(CON), U.S. Court of Appeals, 2nd Circuit, 27.06.2005 (URL: http://caselaw.findlaw.com/us-2nd-circuit/1439019.html (дата обращения: 21.05.2017)).

[3] *Rescuecom Corp. v. Google Inc.*, U.S. Court of Appeals, Second Circuit, 03.04.2009 (URL: http://caselaw.findlaw.com/us-2nd-circuit/1267844.html (дата обращения: 21.05.2017)).

шение *1-800 Contacts, Inc. v. WhenU.com, Inc.*, суд апелляции установил фундаментальные различия в обстоятельствах дела. Во-первых, в указанном деле ключевые слова, используемые программным обеспечением для показа рекламных объявлений, не раскрывались и тем более не продавались рекламодателям в отличие от сервисов *Google*, через которые клиенты могли приобрести права на использование ключевых слов, совпадающих со словесными товарными знаками. Следовательно, сервис *AdWords* представлял собой use in commerce. Во-вторых, имел значение и тот факт, что в деле *1-800 Contacts* ответчик *WhenU.com* использовал в качестве ключевых слов доменные имена, а не товарные знаки. Интересным представляется также аргумент истца о сходстве механизма *AdWords* с мерчендайзинговыми приемами, в частности с размещением массовых товаров рядом с брендовыми. Суд апелляции указал, что в данной ситуации важна не цель, а возможность введения потребителя в заблуждение. В рассматриваемых обстоятельствах пользователи по ошибке могли перейти по ссылке на сайт рекламодателя – третьего лица, думая, что приобретают искомый товар.

Таким образом, решение *Rescuecom v. Google* ликвидировало разногласия, существовавшие в судебной практике США относительно того, является ли использование ключевых слов коммерческим (*use in commerce*). Однако суд нижестоящей инстанции так и не пересмотрел дело в соответствии с указаниями апелляции: в 2010 г. истец отказался от иска[1]. И истец, и ответчик рассматривали решение как свою победу. *Rescuecom* назвал дело «битвой между Давидом и Гуглиафом», объявив о «победе» на своем сайте[2]. Слово *Rescuecom* было исключено из списка предлагаемых ключевых слов. В то же время дело закончилось мировым соглашением, и вопрос о том, нарушает ли поисковая система права на товарные знаки, в частности, есть ли вероятность введения в заблуждение, не был решен, что было выгодно *Google*[3].

Решение по делу *Rescuecom Corp. v. Google* было вынесено в 2009 г. Наиболее поздним крупным делом против *Google AdWords* считается

[1] Rescuecom Abandons Its Litigation Against Google. 05.03.2010 (URL: http://blog.ericgoldman.org/archives/2010/03/rescuecom_aband.htm (дата обращения: 21.05.2017)).

[2] A Case of David versus Googleaith. 05.03.2010 (URL: http://www.rescuecom.com/news-press-releases/a-case-of-david-versus-googleiath.aspx (дата обращения: 21.05.2017)).

[3] *Kemnitzer K.* Beyond Rescuecom v. Google: The Future of Keyword Advertising // Berkeley Technology Law Journal. January 2010. Vol. 25. Issue 2. P. 427 (URL: http://scholarship.law.berkeley.edu/cgi/viewcontent.cgi?article=1831&context=btlj (дата обращения 21.05.2017)).

дело *Rosetta Stone*[1], которое, по утверждению правоведов, ознаменовало собой устранение препятствий политике *Google AdWords* в США.

Разбирательство в суде первой инстанции закончилось победой *Google*[2]. В первую очередь суд признал, что использование в качестве ключевых слов товарных знаков, принадлежащих третьим лицам, не создавало риска введения в заблуждение. В самом тексте рекламных объявлений товарный знак отсутствовал, что исключало возможность создания ложного впечатления относительно лица, предоставлявшего услуги. Кроме того, суд обратил внимание на то, что, поскольку услуги по обучению иностранным языкам являются дорогостоящими, потребители склонны проявлять бо́льшую внимательность при их выборе; следовательно, вероятность ошибки исключена. Примечательно, что суд применил в деле о нарушении прав на товарный знак доктрину функциональности. Как было указано в решении, использование ключевых слов функционально необходимо для деятельности поисковой системы, что, по мнению суда, свидетельствовало в пользу отсутствия нарушения со стороны *Google*.

Однако победа в суде первой инстанции не была окончательной: в апелляции решение было отменено в части[3]. Суд квалифицировал политику *AdWords* как нарушение исключительных прав на товарный знак ввиду так называемого *initial interest confusion* – «сбоя первоначального интереса». Как указал суд, всплывающие рекламные объявления третьих лиц со ссылками на их веб-сайты отвлекают пользователя от его первоначального намерения – поиска контактов правообладателя.

В 2012 г. дело завершилось мировым соглашением между *Google* и *Rosetta Stone*, условия которого неизвестны[4]. Как отмечает американский юрист Эрик Голдман, дело *Rosetta Stone* можно расценивать как победу *Google* в США, так как компания *Rosetta Stone* являлась последним крупным истцом в делах, связанных с *AdWords*, и прецедент,

[1] *Rosetta Stone Ltd. v. Google Inc.*, 4th Cir., 2012 (URL: https://casetext.com/case/rosetta-stone-ltd-v-google-inc-3 (дата обращения: 21.05.2017)).

[2] *Rosetta Stone Ltd. v. Google Inc.*, U.S. District Court for the Eastern District of Virginia, 03.08.2010 (URL: https://ru.scribd.com/document/35324447/Rosetta-Stone-v-Google-Summary-Judgment (дата обращения: 21.05.2017)).

[3] *Rosetta Stone Ltd. v. Google Inc.*, 4th Cir., 2012 (URL: https://casetext.com/case/rosetta-stone-ltd-v-google-inc-3 (дата обращения: 21.05.2017)).

[4] Rosetta Stone and Google Settle Trademark Law Suit // Reuters. 31.10.2012 (URL: http://www.reuters.com/article/us-usa-court-rosettastone-google-idUSBRE89U1GE20121031 (дата обращения: 21.05.2017)).

который мог бы положить конец политике рекламных объявлений *Google*, в итоге не был создан[1].

Интересно обратить внимание на то, что в США предпринимались попытки урегулировать вопросы ключевых слов и контекстной рекламы на законодательном уровне. Таким примером является штат Юта, где все три законодательные инициативы не увенчались успехом[2].

В 2004 г. на уровне штата был принят Закон «О контроле за «всплывающей» рекламой» (*Spyware Control Act*), который полностью запретил использование *spyware* – программ, которые позволяют демонстрировать всплывающие объявления на основе ключевых слов[3]. Впоследствии данный Закон был признан неконституционным, и в 2005 г. в него были внесены поправки, которые фактически аннулировали положения, ограничивающие использование ключевых слов. В 2007 г. был принят новый Закон «О защите товарных знаков», который вводил новый вид интеллектуальной собственности – знак электронной регистрации (*electronic registration mark*). После регистрации товарного знака в качестве знака электронной регистрации поисковым системам запрещалось продавать права на использование совпадающих с ним ключевых слов. Но в 2008 г. этот акт также был отменен[4]. В 2009 г. новая законодательная инициатива касалась введения системы *opt-out*: правообладатель, считавший, что его права нарушены, должен был подать запрос ответчику о прекращении нарушения[5]. В случае добровольного прекращения ответчиком использования товарного знака его ответственность исклю-

[1] *Goldman E.* Fourth Circuit's Rosetta Stone v. Google Opinion Pushes Back Resolution of Keyword Advertising Legality Another 5-10 Years (URL: http://blog.ericgoldman.org/archives/2012/04/fourth_circuits.htm (дата обращения: 21.05.2017)).

[2] *Goldman E.* Utah Trying to Regulate Keyword Advertising (URL: http://blog.ericgoldman.org/archives/2009/03/utah_trying_to.htm (дата обращения: 21.05.2017)); *Barret M.* State Regulation for Keyword Advertising: A Lesson from the Utah Legislature // Journal of Intellectual Property Law. Vol. 15. – Issue 2. – P. 284 (URL: http://digitalcommons.law.uga.edu/cgi/viewcontent.cgi?article=1298&context=jipl (дата обращения: 21.05.2017)).

[3] *Goldman E.* Utah Amends Spyware Control Act. (URL: http://blog.ericgoldman.org/archives/2005/03/utah_amends_spy.htm (дата обращения: 21.05.2017)); *Goldman E.* A Cosean Analysis of Marketing // Wisconsin Law Review. 2006 (URL: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=912524 (дата обращения 21.05.2017)).

[4] *Barret M.* State Regulation for Keyword Advertising: A Lesson from the Utah Legislature // Journal of Intellectual Property Law. Vol. 15. Issue 2. P. 284 (URL: http://digitalcommons.law.uga.edu/cgi/viewcontent.cgi?article=1298&context=jipl (дата обращения: 21.05.2017)).

[5] *Spendlove G.* High Noon on the Internet: The Death of Utah's HB450 (URL: http://archive.utahbusiness.com/dev/articles/view/high_noon_on_the_internet (дата обращения: 21.05.2017)).

чалась. Примечательно, что законопроект исключал из сферы действия поисковые системы – «продавцов», а не «покупателей» ключевых слов. Но и этот законопроект так и не был принят[1].

В противоположность США, где было подано большое число исков в отношении *Google*, в Австралии известно лишь одно крупное судебное дело против поисковой системы. В качестве истца в нем выступил не обладатель исключительных прав на товарный знак, а орган государственной власти в сфере защиты конкуренции и прав потребителей – Австралийская комиссия по вопросам конкуренции и защиты потребителей (*Australian Competition & Consumer Commission, ACCA*).

Дело *Australian Competition & Consumer Commission v. Google*[2] прошло рассмотрение в двух судебных инстанциях. Иск был основан на разделе 52 Акта о торговой практике (*Trade Practices Act*), запрещающим при осуществлении коммерческой деятельности совершать действия, которые могут ввести в заблуждение[3]. Комиссия утверждала, что политика *AdWords* может ввести пользователей в заблуждение и представляет собой недостоверную рекламу, так как пользователи могут не отличить платные объявления третьих лиц от обычных результатов поиска. Такая вероятность была обусловлена в том числе тем, что ключевые слова содержались в заголовке объявлений. Например, в ответ на запрос *Harvey World Travel* поисковая система отображала объявление с заголовком *Harvey Travel. Unbeatable deals on flights, Hotel & Pkg's Search, Book & Pack Now!*, содержащее гиперссылку на сайт *www.startravel.com.au*, принадлежащий не компании *Harvey World Travel*, которую искал автор запроса, а ее конкуренту – *Star Travel*.

В первой инстанции судья Федерального суда Австралии отклонил иск, признав, что *AdWords* нельзя квалифицировать как ложную рекламу. Суд отметил, что поисковая система использует ключевые слова исключительно как функционально необходимый инструмент. Пленум Федерального суда Австралии, напротив, установил, что политика поисковой системы нарушала раздел 52 Акта о торговой практике.

[1] *Goldman E.* Brand Spillovers // Harvard Journal of Law and Technology. Vol. 22. No. 2. Spring 2009. P. 402. // URL: http://jolt.law.harvard.edu/articles/pdf/v22/22HarvJLTech381.pdf (дата обращения: 21.05.2017)).

[2] Google Inc v Australian Competition and Consumer Commission [2013] HCA 1 (6 February 2013) (URL: http://eresources.hcourt.gov.au/downloadPdf/2013/HCA/1 (дата обращения: 21.05.2017)).

[3] Trade Practices Act 1974 (URL: https://www.legislation.gov.au/Details/C2010C00426 (дата обращения: 02.06.2017)).

Наконец, Верховный суд Австралии в своем решении 2013 г. освободил *Google* от ответственности. Суд признал *Google* посредником (*mere condui*»), предоставляющим рекламные услуги таким же образом, как это делают газеты, радио и иные СМИ. Помимо этого, пользователи, по мнению суда, имели возможность понять, что «всплывающие объявления» не являются результатами естественного поиска. Суд пришел к выводу о том, что *Google* не несет ответственности за осуществляемый рекламодателями выбор ключевых слов.

В Израиле наиболее известны два судебных дела, в которых *Google* выступал в качестве соответчика наряду с компанией-конкурентом. Суды первой инстанции по этим двум делам вынесли прямо противоположные решения.

В 2006 г. районный суд Тель-Авива рассматривал дело *Matim Li Large Sizes Fashion Chain Ltd. and Matim Li Stores 1997 Ltd. v. Crazy Line Ltd, Eran Levin and Google Israel Ltd*.[1] Соответчик, сеть магазинов одежды *Crazy Line*, использовал для контекстной рекламы в Интернете ключевые слова *Matim Li* (в пер. с иврита – «мне идет») и *ML*, сходные с товарным знаком истца. По мнению истцов, политика *Google AdWords*, дающая возможность использовать чужие товарные знаки в качестве ключевых слов, нарушали их исключительные права. Суд отклонил требования истцов к *Google* и компании-конкуренту, установив, что подобная деятельность не является использованием товарного знака[2]. Суд также указал, что указанные слова не использовались в тексте объявлений, которые было легко идентифицировать как контекстную рекламу, а не как результаты поиска[3]. Интересно заметить, что суд провел аналогию с размещением товаров в магазинах (*product placement*), которая в свое время была отклонена в США в упомянутом выше решении *Rescuecom v. Google*.

Второе дело, *Dr. Dov Klein v. Proportion PMC Ltd and Google Israel Ltd*.[4], было рассмотрено всего годом позже, но суд первой инстанции пришел к противоположным выводам. Клиника пластической хирургии

[1] *Matim Li Large Sizes Fashion Chain Ltd. and Matim Li Stores 1997 Ltd v. Crazy Line Ltd, Eran Levin and Google Israel Ltd*, C.A. 8774/06, Tel Aviv District Court, 31 July 2006.

[2] An advertiser and Google win the first sponsored links trademark case in Israel. Adin-Liss Law Offices (URL: http://www.wptn.com/wptn-in/Mailing/Apr_2007_3/details/trademarks/israel.html (дата обращения: 21.05.2017)).

[3] *Smith G. J. H. et al.* Internet Law and Regulation. 4th ed. London: Sweet&Maxwell, 2007. P. 250.

[4] *Dr. Dov Klein v. Proportion PMC Ltd. and Google Israel Ltd.*, C.F. 48511/07.

Proportion использовала в качестве ключевого слова имя известного пластического хирурга, доктора Кляйна, однако в тексте объявления фраза *Dr. Klein* не употреблялась, как и в деле *Matim Li*. Суд первой инстанции возложил на *Google* ответственность за неосновательное обогащение, которое выразилось в получении поисковой системой вознаграждения за продажу рекламодателям прав на использование ключевых слов, нарушающих права истца. Но окончательное решение было принято в контексте не товарных знаков, а защиты персональных данных: суд установил нарушение раздела 2(6) Акта о защите частной жизни (*Privacy Act*), запрещавшего использование имени лица с целью извлечения прибыли. Однако районный суд Тель-Авива в апелляции это решение отменил, отметив, что само по себе использование имени в качестве ключевого слова не является нарушением[1]. Таким образом, определенную роль сыграло, что в качестве ключевого слова использовалось имя лица, а не товарный знак.

В европейских странах долгое время не существовало единства в подходах, в том числе в пределах одной юрисдикции, к решению вопроса об ответственности поисковой системы за выбор ключевых слов, сделанных рекламодателями.

Лидирующую позицию по числу поданных против поисковой системы *Google* исков занимает Франция[2]. По данным обзора, составленного Международной ассоциацией товарных знаков (*International Trademark Association – INTA*), по состоянию на 2013 г. во Франции было вынесено около 14 судебных решений[3]. В большинстве решений была признана ответственность *Google* либо за нарушение товарного знака (например, *Pierre Alexis v. Google & Tiger*[4]), либо по иным основаниям (см., напр, *Auto IES v. Google France*[5], в котором была признана

[1] *Proportsia PMC Ltd et al v. Dr Dov Klein*, Civil Appeal Tel Aviv, 29.07.2013. См. *Reichman J.D.* (ed.) Getting the Deal Through: Right of Publicity 2015. P. 71 (URL: http://luthi.co.il/wp-content/uploads/2016/07/ROP2014-Israel.pdf (дата обращения: 21.05.2017)).

[2] URL: http://www.linksandlaw.com/adwords-google-keyword-lawsuit-France.htm (дата обращения: 21.05.2017)).

[3] Internet Committee Keyword Jurisprudence Chart (URL: http://www.inta.org/Advocacy/Documents/INTA%20Intro%20Paper%20on%20Keyword%20Jurisprudence%20and%20Search%20Engine%20Policies.pdf (дата обращения: 21.05.2017)).

[4] *Pierre Alexis v. Google & Tiger,* Cour d'appel de Versailles, 23.03.2006 (URL :https://www.legifrance.gouv.fr/affichJuriJudi.do?idTexte=JURITEXT000020555777 (дата обращения: 01.06.2017)).

[5] *Auto IES v. Google France*, Tribunal de grande instance de Paris, 03.04.2006 (URL: https://www.legalis.net/jurisprudences/tribunal-de-grande-instance-de-paris-3eme-chambre-2eme-section-jugement-du-27-avril-2006 (дата обращения: 21.05.2017)).

деликтная ответственность *Google* в соответствии со ст. 1382 ФГК). Одним из немногих примеров освобождения *Google* от ответственности является дело *Atrya*[1], в котором исковые требования в отношении поисковой системы были отклонены судом и ответственность была возложена на компанию-конкурента, который осуществил выбор соответствующих ключевых слов.

В Испании в решении по делу *Tienda del espía v. Google*, вынесенном в 2013 г., Торговый суд Мадрида, отклоняя иск компании *Tienda del espía*, обратил внимание на то, что *Google* выступает в качестве посредника и никак не участвует в выборе ключевых слов и подаче рекламных объявлений. Выбор ключевых слов осуществляется самими рекламодателями. Следовательно, только на них может быть возложена ответственность за нарушение исключительных прав на товарные знаки[2].

В Германии два наиболее цитируемых судебных решения придерживаются такого же подхода. Так, в деле *Nemetschek v. Google*[3] суд отметил, что на поисковую систему не возложена обязанность контролировать процесс выбора ключевых слов рекламодателями. Решение *Metaspinner Media v. Google* подтвердило этот вывод, также установив, что, поскольку товарный знак используется не в самом тексте объявления, а в ключевых словах, которые являются метатегами и, следовательно, не демонстрируются пользователям, нарушения прав на товарный знак в таком использовании нет[4].

Особое значение для унификации судебной практики государств – членов Европейского союза имеет решение Суда Европейского союза

---

[1] *Atrya v. Google & K par K & Techni Feneres*, Tribunal de grand instance de Strasbourg, 20.07.2007 (URL : https://www.legalis.net/jurisprudences/tribunal-de-grande-instance-de-strasbourg-1ere-chambre-civile-jugement-du-20-juillet-2007 (дата обращения: 01.06.2017)).

[2] Google gana la batalla judicial a 'La tienda del espía' (URL: http://www.lainformacion.com/espana/google-gana-la-batalla-judicial-a-la-tienda-del-espia_YBZi7bQMTmX8FJvkw7BVZ3/ (дата обращения: 21.05.2017)).

[3] *Nemetschek AG v.Google*, Решение Земельного суда Мюнхена по делу № 33 O 21461/03 от 03.12.2003 (URL: http://linksandlaw.de/urteil76-adwords-haftung-markenverletzung.htm (дата обращения: 21.05.2017)).

[4] *Metaspinner GmBH v. Google Deutschland*, Решение Земельного суд Гамбурга по делу № 312 O 324/04 от 21.09.2004 (URL: http://linksandlaw.de/urteil77-adwords-haftung-suchmaschine-google.htm (дата обращения: 21.05.2017)). См. также: German Court Dismisses Metaspinner's Trademark Suit v. Google https://www.law360.com/articles/2220/german-court-dismisses-metaspinner-s-trademark-suit-vs-google (дата обращения: 21.05.2017).

(*European Court of Justice – ECJ*), вынесенное по обращению Кассационного суда Франции[1]. Кассационный суд Франции обратился с запросом в связи с рассмотрением трех упомянутых выше судебных дел *Louis Vuitton Malletier v. Google France & Google*, *Viaticum & Luteciel v. Google France* и *Centre national de recherche en relations humaines & Tiger v. Google France*. Ключевым в решении является тезис о том, что *Google* представляет собой лишь *Internet referencing service* – инструмент (сервис), представляющий ссылки на искомые интернет-ресурсы по запросу пользователей, что исключает ответственность поисковой системы за нарушение товарных знаков. По мнению Суда, сам факт того, что поисковая система создает необходимые технические условия и получает оплату за размещение рекламных объявлений, не означает, что она осуществляет использование товарного знака[2].

Основные выводы Суда Европейского союза сводятся к следующим положениям. Во-первых, Суд обратил внимание на то, что ст. 5(1)(a) Первой Директивы Совета № 89/104/ЕЕС от 21.12.1988 о сближении законодательств государств-членов о товарных знаках[3] и ст. 9(1)(a) Регламента Совета № 40/94 от 20.12.1993 о товарном знаке Сообщества[4] позволяет правообладателю запретить использовать без его согласия товарный знак в качестве ключевого слова в целях рекламы идентичных товаров или услуг, если такая реклама не дает возможности сделать вывод о том, что товар или услуга предоставляются третьим лицом. Во-вторых, сам факт хранения в базе ключевых слов слова, идентичного зарегистрированному товарному знаку, и организация показа рекламы на основе содержания такого ключевого слова в метатегах объявления, не могут рассматриваться как использование товарного знака. В-третьих, ст. 14 Директивы 2000/31/ЕС Европейского парламента

[1] *Google France SARL v. Louis Vuitton Malletier SA*, C-236/08 – Judgment of the Court (Grand Chamber) of 23 March 2010 (URL: http://curia.europa.eu/juris/liste.jsf?num=C-236/08 (дата обращения: 21.05.2017)).

[2] *Google France SARL v. Louis Vuitton Malletier SA*, C-236/08 – Judgment of the Court (Grand Chamber) of 23 March 2010 § 57 (URL: http://curia.europa.eu/juris/liste.jsf?num=C-236/08 (дата обращения: 21.05.2017)).

[3] First Council Directive 89/104/EEC of 21 December 1988 to approximate the laws of the Member States relating to trade marks (URL: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31989L0104:en:HTML (дата обращения: 03.06.2017)).

[4] Council Regulation (EC) No 40/94 of 20 December 1993 on the Community trade mark (URL: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31994R0040:en:HTML (дата обращения: 03.06.2017)).

и ЕС от 08.06.2000 (Директива об электронной торговле)[1] применима к провайдеру интернет-услуг, если провайдер не играет активной роли в использовании ключевых слов и исключает ответственность за хранение данных. Ответственность наступает только в том случае, если после получения сведений о незаконности действий рекламодателей, провайдер не предпринял мер по их пресечению.

Таким образом, решение Суда Европейского союза заложило основы для унификации судебной практики в рамках ЕС и обозначило поворот в сторону отказа от возложения на поисковые системы ответственности за нарушение исключительных прав на товарные знаки в случаях, когда рекламодатели используют в качестве ключевых слов для своих объявлений товарные знаки конкурентов. Эта тенденция позволила *Google* в дальнейшем сгладить региональные различия своей политики *AdWords*[2]. В настоящее время на сайте *Google* прямо указано, что даже в случае получения жалобы компания не будет рассматривать вопросы нарушения прав на товарный знак или вводить ограничения на подобное использование, если товарный знак используется в качестве ключевого слова, а не в тексте объявления[3].

В России исковые требования предъявлялись в основном в отношении поисковой системы «Яндекс» в связи с действием сервиса «Яндекс. Директ» – российского аналога *Google Adwords*.

Одним из самых свежих решений является вынесенное 22.03.2017 решение Арбитражного суда г. Москвы по делу № А40-217174/16-5-1882[4]. Истец, ООО «ОНЛАЙНТУР», обратился с требованием запретить ответчику, ООО «Яндекс», размещение в сети Интернет рекламных объявлений по поисковым запросам *onlinetour*, «онлайнтур», тождественных или сходных до степени смешения со словесным элементом товарного знака истца. Исковые требования были отклоне-

[1] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (URL: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32000L0031:en:HTML(дата обращения: 03.06.2017)).

[2] *Tonkin S.* Google Inc. v. Australian Competition and Consumer Commission // Adelaide Law Review. Vol. 34. 2013. P. 208 (URL: http://www.austlii.edu.au/au/journals/AdelLawRw/2013/11.pdf (дата обращения: 21.05.2017)).

[3] Google's approach to trademarks (URL: https://support.google.com/adwordspolicy/answer/6118?hl=en (дата обращения: 21.05.2017)).

[4] По сведениям системы kad.arbitr.ru, данное решение в настоящее время обжалуется в Девятом арбитражном апелляционном суде (URL: https://kad.arbitr.ru/Card/a587f9c7-7fa1-414c-b4ff-1b66f076a5ab (дата обращения: 01.06.2017)).

ны судом со следующим обоснованием. Во-первых, ключевые слова не могут рассматриваться в качестве способа использования товарного знака, так как у них отсутствует индивидуализирующая способность. Ключевые слова определяются рекламодателями, и одно и то же ключевое слово может запускать показ объявлений разных рекламодателей. Следовательно, ключевые слова не вызывают смешения товаров истца и рекламодателя. Во-вторых, использование ключевых слов не может рассматриваться в качестве «иного способа адресации в сети Интернет» в смысле ст. 1484 ГК РФ. Существующие способы адресации в сети Интернет обладают общим сущностным признаком: определяют единственного адресата. Однако у ключевых слов указанный признак отсутствует, поскольку они не дают возможности с точностью определить лицо или товар.

Указанное решение продолжает сложившуюся в российских судах практику. Такая же аргументация содержится в мотивировочной части решений по делу № А40-172653/12[1], в котором компания *International Environmental Group GmbH* предъявила иск к соответчикам: ООО «Яндекс» и ООО «Сириус», компании-конкуренту[2]; а также по делу № А40-164436/12 (ООО «КМ-Элит» против ООО «Яндекс», ООО «Гугл» и ЗАО «Домашние продукты»)[3].

Следует отметить, что в приведенных решениях суд не проводил разграничений между ответственностью компании-конкурента, которая использует ключевые слова, совпадающие со словесным товарным знаком истца, и ответственностью поисковой системы. Исковые требования в отношении обоих соответчиков были отклонены в полном объеме. В связи с этим показательно дело № А40-76957/14, которое завершилось отказом истца от исковых требований к ООО «Яндекс» и заключением мирового соглашения с соответчиком, компанией-конкурентом[4].

---

[1] Решение Арбитражного суда г. Москвы от 22.03.2017 г. по делу № А40-217174/16-5-1882.

[2] Суд апелляционной инстанции подтвердил вынесенное решение: Постановление Девятого ААС от 07.10.2014 № 09АП-21300/2014-ГК.

[3] Решение Арбитражного суда г. Москвы от 08.04.2013 г. по делу № А40-164436/12. Выводы суда подтверждены судами апелляционной и кассационной инстанций: см. постановление Девятого ААС от 24.07.2013 г. № 09АП-19422/2013-ГК, Постановление Суда по интеллектуальным правам от 26.11.2013 г. № С01-198/2013.

[4] Определение Арбитражного суда г. Москвы от 13.11.2014 г. о прекращении производства по делу № А40-76957/14.

Тенденция отклонения исковых требований к поисковой системе при удовлетворении иска к компании-конкуренту обозначилась в решении, вынесенном всего месяцем позже, чем упомянутое выше, по делу № А40-70362/14[1]. ООО «Дистрибьюторский центр «Санг-Йонг»» обратилось с иском к ООО «Аверт Медиа» и ООО «Яндекс». Обстоятельства данного дела отличались тем, что объявление конкурента истца не только демонстрировалось при вводе поискового запроса с использованием словесного товарного знака истца, но и содержало в своем тексте обозначение *Actyon*, сходное до степени смешения с этим товарным знаком. Арбитражный суд г. Москвы со ссылкой на п. 6 ст. 38 и подп. 7 п. 3 ст. 5 ФЗ от 13.03.2006 № 38-ФЗ «О рекламе» отметил, что ответственность должен нести рекламодатель, а не поисковая система.

Такой же логике последовал суд первой инстанции в деле «Мани Мен»[2]. Суд, на наш взгляд, очень точно охарактеризовал суть претензий к использованию ключевых слов, совпадающих с товарным знаком третьего лица: «оспариваемое объявление обращает внимание интернет-пользователей, которые в данный момент хотят получить заем в компании «Мани Мен», и предлагает пользователю получить заем в компании «еКапуста», приводя пользователю конкурентные преимущества [этого] сервиса». Признав, что отсутствует риск смешения, суд отклонил исковые требования к компании-конкуренту. Что касается ответственности поисковых систем, которые осуществляют показ контекстной рекламы, суд обратил внимание на то, что возложение на них ответственности было бы наделением поисковых систем функциями органа по защите исключительных прав на товарный знак. Суд апелляционной инстанции отменил решение только в части удовлетворения требований к компании – конкуренту истца, согласившись с выводами относительно исключения ответственности поисковых систем по подобным искам[3].

Исходя из этого можно отметить, что современная российская судебная практика по рассматриваемому вопросу следует мировым

[1] Решение Арбитражного суда г. Москвы от 22.12.2014 г. по делу № А40-70362/14.

[2] Решение Арбитражного суда г. Москвы от 27.05.2016 г. по делу № А40-184746/15.

[3] Постановление Девятого ААС от 18.08.2016 г. № 09АП-34533/2016. Суд по интеллектуальным правам оставил в силе решение суда апелляционной инстанции постановлением от 27.10.2016 г. № С01-957/2016. В передаче кассационной жалобы в Судебную коллегию по экономическим спорам ВС РФ отказано: см. Определение ВС РФ № 305-ЭС16-21484 от 27.02.2017.

тенденциям, не признавая ответственность поисковых систем за нарушение исключительных прав на товарный знак в связи с показом контекстной рекламы на основе указанных рекламодателями ключевых слов.

Показ рекламы поисковыми системами, основанный на ключевых словах, как и любое новое решение в области информационных технологий, с момента своего широкого распространения вызвал противоречивое отношение правоприменителей по всему миру. С модификацией правил выбора ключевых слов поисковыми системами у недобросовестных рекламодателей появилась возможность использовать слова, совпадающие с товарными знаками конкурентов, для «перетягивания» на свой сайт пользователей, которые изначально интересовались товарами или услугами конкурента. Отсутствие прямого законодательного регулирования привело к спорам о квалификации действий поисковых систем в качестве нарушения прав на товарные знаки.

С течением времени во многих зарубежных юрисдикциях сложился подход, отрицающий ответственность поисковых систем за нарушение товарных знаков. Так, в рамках Европейского союза ключевым шагом в данном направлении можно считать решение Суда ЕС, высказавшегося против ответственности поисковых систем. В США, где было рассмотрено большое количество исков против *Google*, вопрос о правомерности действий поисковой системы в судебной практике до сих пор окончательно не решен, так как многие процессы заканчивались мировыми соглашениями. Представляет интерес предпринятая в штате Юта попытка урегулировать данный вопрос на законодательном уровне. Учитывая сходство обстоятельств дела во многих судебных процессах, такое регулирование представляется целесообразным, однако необходим поиск юридических конструкций, которые бы позволили эффективно урегулировать данную сферу, что так и не удалось законодателю Юты.

В России отрицание ответственности поисковых систем за использование ключевых слов долгое время, до вынесения решения по делу «Мани Мен», шло рука об руку с освобождением от ответственности рекламодателей, осуществлявших выбор ключевых слов. Но и после того, как была признана ответственность рекламодателей-конкурентов, подход в вопросе ответственности поисковых систем сохранился.

Вместе с тем в мировой судебной практике наблюдается уменьшение числа исков об использовании ключевых слов. Это свидетельствует

о том, что в мире процессы против сервиса *Google AdWords* и иных подобных услуг поисковых систем в большинстве своем постепенно уходят в прошлое[1].

Пристатейный библиографический список:

1. *Barret M.* State Regulation for Keyword Advertising: A Lesson from the Utah Legislature // Journal of Intellectual Property Law. Vol. 15. Issue 2 (URL: http://digitalcommons.law.uga.edu/cgi/viewcontent.cgi?article=1298&context=jipl (дата обращения: 21.05.2017)).

2. *Goldman E.* A Coasean Analysis of Marketing // Wisconsin Law Review. 2006. URL: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=912524 (дата обращения: 21.05.2017)).

3. *Goldman E.* Brand Spillovers // Harvard Journal of Law and Technology. Vol. 22. No. 2. Spring 2009 (URL: http://jolt.law.harvard.edu/articles/pdf/v22/22HarvJLTech381.pdf (дата обращения: 21.05.2017)).

4. *Goldman E.* Fourth Circuit's Rosetta Stone v. Google Opinion Pushes Back Resolution of Keyword Advertising Legality Another 5-10 Years (URL: http://blog.ericgoldman.org/archives/2012/04/fourth_circuits.htm (дата обращения: 21.05.2017)).

5. Goldman E. More Evidence Why Keyword Advertising Litigation Is Waning (URL: http://blog.ericgoldman.org/archives/2016/12/more-evidence-why-keyword-advertising-litigation-is-waning.htm (дата обращения: 21.05.2017)).

6. *Goldman E.* Utah Amends Spyware Control Act (URL: http://blog.ericgoldman.org/archives/2005/03/utah_amends_spy.htm (дата обращения: 21.05.2017)).

7. *Goldman E.* Utah Trying to Regulate Keyword Advertising (URL: http://blog.ericgoldman.org/archives/2009/03/utah_trying_to.htm (дата обращения: 21.05.2017)).

8. *Kemnitzer K.* Beyond Rescuecom v. Google: The Future of Keyword Advertising // Berkeley Technology Law Journal. January 2010. Vol. 25. Issue 2 (URL: http://scholarship.law.berkeley.edu/cgi/viewcontent.cgi?article=1831&context=btlj (дата обращения: 21.05.2017)).

[1] *Goldman E.* More Evidence Why Keyword Advertising Litigation Is Waning (URL: http://blog.ericgoldman.org/archives/2016/12/more-evidence-why-keyword-advertising-litigation-is-waning.htm (дата обращения: 21.05.2017)).

9. *Scardamaglia A.* Keywords, Trademarks, and Search Engine Liability // König R, Rasch M. (eds), Society of the Query Reader: Reflections on Web Search. Amsterdam: Institute of Network Cultures, 2014.

10. *Spendlove G.* High Noon on the Internet: The Death of Utah's HB450 (URL: http://archive.utahbusiness.com/dev/articles/view/high_noon_on_the_internet (дата обращения: 21.05.2017)).

11. *Tan A.* Google Adwords: Trademark Infringer or Trade Liberalizer //Michigan Telecommunications and Technology Law Review. 2010. Vol. 16. Issue 2 (URL: http://repository.law.umich.edu/cgi/viewcontent.cgi?article=1049&context=mttlr (дата обращения: 21.05.2017)).

12. *Tonkin S.* Google Inc. v. Australian Competition and Consumer Commission // Adelaide Law Review. Vol. 34. 2013 (URL: http://www.austlii.edu.au/au/journals/AdelLawRw/2013/11.pdf (дата обращения: 21.05.2017)).

А.А. Семенова

МЕМЫ: ВОПРОСЫ ПРАВОМЕРНОГО И НЕПРАВОМЕРНОГО ИСПОЛЬЗОВАНИЯ

Аннотация. *Статья посвящена проблеме определения правового режима мемов, их использованию в Интернете и в предпринимательской деятельности. В работе отражена история создания некоторых из них.*

Ключевые слова: *мемы, авторское право, товарный знак, незаконное использование.*

Современная культура развивается стремительными темпами: не успеешь оглянуться, и кто-то предлагает вновь созданное «нечто» – новое направление, новое течение, новое веяние. Но будет ли оно реально новым? И здесь вспоминается постулат постмодернизма, согласно которому остается экспериментировать с формой, но не с содержанием, ибо все возможные велосипеды уже изобретены. Сегодня творчество – это интеллектуальная деятельность, основанная на уже существующих произведениях, их элементах и частях, изменяющая эти произведения по велению своей фантазии, придающая существующему новые значение, звучание и смысл.

Вероятно, достаточно неожиданным после такого вступления будет переход к рассмотрению одного из сумасшедших «поветрий», захвативших Интернет, – мемам, которые знакомы, наверное, каждому пользователю Интернета. Это вдруг становящаяся безумно популярной картинка или фраза, которой начинают пользоваться все, придумывая ее разнообразные интерпретации.

Многие наверняка встречали фотографию, где запечатлена весьма недовольная кошачья мордочка – это и есть знаменитый *Grumpy Cat* (англ. – Сердитый кот), который признан самым прибыльным мемом всех времен. Первые его фото были размещены в сети Интернет в сентябре 2012 г. и сразу стали очень популярны. Хозяева использовали известность своего домашнего любимца в коммерческих целях: зарегистрировали изображение Сердитого кота в качестве

товарного знака[1] и заключили различные сделки по предоставлению прав на использование этого товарного знака (например, договор с *Friskies*, договор с компанией *Grenade Beverage LLC* на выпуск кофейных напитков с изображением кошки *Grumppuccino* и т.п.). Но коммерческая успешность Сердитого кота стала поводом для различных нарушений, например без разрешения правообладателей его изображение помещались на различные товары, появились сайты *GrumpyCat.com*. и *DrinkGrumpyCat.com*.[2] Это привело к тому, что хозяева Сердитого кота (правообладатели) были вынуждены предъявлять иски с требованием денежной компенсации за нарушение прав на товарный знак, с требованием передачи им упомянутых сайтов и т.д.

Кстати, регистрация мема в качестве товарного знака – достаточно часто встречающаяся практика. Так, зарегистрированы в качестве товарного знака *KeepCalm* (правообладатель – Челябинская обувная компания «Юничел»), «+100500» (телешоу «Карамба Медиа»), «Печалька» (компания «Вимм-Билль-Данн») и «Тро-ло-ло» (кафе «Улей-К»)[3].

Появлению мемов способствовало развитие форумов, социальных сетей и т.д., т.е. таких информационных ресурсов, на которых множество людей могут одновременно обмениваться информацией. Забавная поза, удачный ракурс, меткая фраза, подхваченные в Интернете, – и вот основа для будущего «шедевра» найдена, а автору остается добавить только необходимые штрихи!

Характеризуя мем с правовой точки зрения, большинство авторов соглашаются с тем, что он является результатом творческой деятельности, а следовательно, авторским произведением. По всей видимости, мем следует рассматривать как производное произведение, т.е. произведение, возникающее вследствие переработки другого (оригинального) произведения.

---

[1] Информацию о товарном знаке, принадлежащем *GRUMPY CAT LIMITED,* можно найти на сайте Ведомства по патентам и товарным знакам США *www.uspto.gov*. Изобразительные и словесные товарные знаки (85836805, 85836812, 85837936, 85838010 и 85983483) зарегистрированы для таких групп товаров, как чехлы для телефоном и ноутбуков, ковриков для мышек, декоративных магнитов и мягких игрушек.

[2] См.: http://intelaspekt.ru/rubric/346/

[3] *Кондратьева И.* +100500 к копирайту: кто владеет правами на мемы (https://pravo.ru/story/view/134865/).

Иногда предлагается рассматривать мем как пародию[1]. И, действительно, в некоторых случаях мем и является пародией[2], но такие случаи крайне редки. Обычно же мем используется в других целях, и, например, мемы на основе фотографии Сердитого кота не высмеивают самого домашнего питомца, а служат средством передачи чувств авторов различных по своему характеру мемов.

Можно усмотреть за мемом и некоторые черты произведений, создаваемых в стиле мэш-ап – произведений, которые базируются на известном оригинальном тексте или музыкальном произведении, перешедшем в общественное достояние, с добавлением авторских включений, меняющих сущность заимствованного (оригинального) произведения[3]. Как и произведения в стиле мэш-ап, мемы обычно основываются на оригинальном произведении с добавлением каких-то включений, преобразовывающих оригинал. Однако признавать мемы произведениями в стиле мэш-ап нет достаточных оснований.

Таким образом, правовой режим мемов на сегодняшний день неясен. Но он нуждается в уточнении, поскольку мемы все чаще используются не только в личных целях, но и для бизнеса.

---

[1] *Martinez Nicole*. Posting an Internet Meme? You May Receive a Getty Letter (http://artlawjournal.com/internet-meme-getty-letter/).

[2] Обстоятельный и детальный анализ понятия «пародия» содержится в статье В.А. Колосова, который предлагает следующие критерии, на основании которых можно отнести произведение к пародии:

1. Творческая цель; автор подчеркивает, что объектом высмеивания должен быть сам оригинал – использование же чьего-то результата творческой деятельности для юмористических и сатирических выпадов против окружающих явлений может задевать права автора;

2. Добросовестность автора – не оскорбить, не злоупотребить правом, не нанести вред чести и достоинству автора оригинала;

3. Пародия не должна наносить ущерб нормальному использованию оригинального произведения и ущемлять законные права и интересы автора оригинала;

4. Объем заимствования – строго в рамках оригинала, проводя параллели и ассоциации с ним;

5. Связь с оригиналом, отражение оригинального произведения в себе (см.: Колосов В.А. Пародия в системе авторского права // Закон. 2013. № 9). В решении по делу No А40-125210/09-110-860 суды отмечали, что «пародия неизменно связана с комическим эффектом и должна быть сразу же узнаваема, соответственно, пародия не может быть совершенно отделена от оригинального произведения, так как в этом случае пропадает сам смысл создания пародии».

[3] *Семенова Е.* Правомерность «креативных» нарушений авторских прав: стиль мэш-ап в современной литературе // ИС. Авторские и смежные права. 2016. Октябрь.

Определение правового режима мема позволит правообладателям и заинтересованным лицам при решении различного рода вопросов опираться на соответствующие правовые нормы. Ведь свобода творчества – даже столь своеобразного, как создание мема, должна подчиняться установленным законом правилам. Отсутствие четкости в вопросе правового режима порождает проблемы на практике, что можно проиллюстрировать следующими примерами.

Так, фотография кота в колпачке под заголовком *I'm Fat, Let's Party*[1] (англ. – Я толстый, давайте веселиться) появилась на сайте *justcuteanimals.com* в 2013 г. Автор фотографии не указал каких-то особых условий использования фотографии, что предполагает обращение к правилам самого сайта[2].

Правила сайта, в свою очередь, содержат специальный раздел «Интеллектуальная собственность»[3], где указано, что при посещении сайта необходимо помнить о том, что его содержимое защищено законом. И далее следовало следующее правило: «Вы обязуетесь не изменять, копировать, распространять, передавать, демонстрировать, публиковать, создавать производные работы, продавать или перепродавать любые данные или информацию, полученную на сайте или с помощью него»[4]. При явном несогласии с этим положением владелец сайта рекомендует немедленно покинуть сайт.

Таким образом, правилами сайта установлен запрет на распространение или изменение фото, размещенных на этом сайте. Это, по всей видимости, исключает возможность использовать фотографию в качестве мема. Однако, несмотря на изложенные правила, это фото кота в колпачке впоследствии появилось на сайте *funniestmemes.com* с новой подписью *I must consult the cards* (англ. – Я должен свериться с картами), а затем с космической скоростью распространилось в российском сегменте Интернета в различных интерпретациях (мем «Вжух»).

---

[1] См.: http://justcuteanimals.com/post/1650

[2] См.: http://justcuteanimals.com/terms-of-service

[3] Следует заметить, что владелец сайта – компания *xPand Media Ltd*, принимая фото к размещению на сайте, тем самым заключает с автором фотографии лицензионный договор и обязуется использовать его работу на определенных условиях.

[4] *IntellectualProperty.*

You acknowledge and agree that all content and information on the Site is protected by proprietary rights and laws.

You agree not to modify, copy, distribute, transmit, display, perform, reproduce, publish, license, transfer, create derivate work from, sell or re-sell any content or information obtained from or through the Site.

Изложенное заставляет вспомнить появление в 2009 г. другого мема – черно-белого пингвина на синем фоне, снимок которого был сделан фотографом *National Geographic*. Газета *The Washington Post* опубликовала эту фотографию, сопроводив словами *Posta meme – lawsuit* (англ. – Разместил мем – к судебному иску). И пингвин стал мемом для высмеивания различных неловких ситуаций. При этом он стал приносить немалую прибыль: согласно наблюдениям *The Washington Post,* этого пингвина можно встретить практически везде – от галстуков до стаканов[1]. Здесь важно заметить, что за использование фотографии *The Washington Post* выплатила правообладателю соответствующее вознаграждение. Обычные пользователи Интернета при составлении своего варианта картинки с «пингвином-социофобом»[2] этого, разумеется, не делают.

Можно ли назвать правомерным создание мемов в описанных выше случаях?!

Для решения вопроса относительно правомерности использования авторских произведений для создания мемов целесообразно обратиться к доктрине *fair use* (доктрине добросовестного использования). Она определяет условия для свободного использования произведения с учетом нескольких факторов (17 U.S. Code § 106 и 17 U.S. Code § 106A). К таким факторам отнесены:

1. Цель и характер использования: будет ли оно носить коммерческий характер, или предполагается обращаться к произведению исключительно для личных целей.

2. Сущность произведения, охраняемого авторским правом.

3. При использовании части произведения – ее величина и существенность по отношению ко всему произведению, защищенному авторским правом.

4. Влияние использования на потенциальный рынок или стоимость произведения, защищенного авторским правом[3].

---

[1] *Dewey Caitlin*. How copyright is killing your favorite memes. TheWashingtonPost, 8.09.2015 https://www.washingtonpost.com/news/the-intersect/wp/2015/09/08/how-copyright-is-killing-your-favorite-memes/?utm_term=.e188f85d5d30

[2] Указывается, что компания *Getty* (правообладатель) запросила *Get Digital* оплатить лицензию в размере 785,40 евро за использование картинки в течение года, по прошествии которого необходимо будет продолжить выплаты или прекратить ее использование (см.: https://www.getdigital.de/blog/getty-images-wants-license-fees-for-the-awkward-penguin-meme/).

[3] United States Code: Supplement III. Washington, 2013. P. 1053.

Scott J. Slavick пишет, что у компаний часто возникает проблема доказывания добросовестности использования авторских произведений, в связи с чем рекомендует идти по пути заключения лицензионного договора с автором[1]. Такой союз, по его мнению, будет прибылен и автору, который сможет получать определенные проценты от коммерческой деятельности, в которой использовано его «творение». Но, как специально подчеркивает *Scott J. Slavick*, перед заключением такого договора необходимо удостовериться в том, что лицо, с которым заключается лицензионное соглашение, действительно обладает правами на произведение, – в противном случае есть вероятность стать звеном в цепочке правонарушений.

Если мемом становится, например, чья-то фотография, которая изменяется другим лицом путем добавления к ней различных надписей, рисунков и т.д., то закономерным будет вопрос о соблюдении в такой ситуации прав как автора самой фотографии, так и лица, изображенного на этой фотографии. И проблема, с которой можно столкнуться при создании мема на основе фотографии конкретного лица, – оскорбление чести и достоинства личности, изображенной на фото.

Использование чужого изображения даже для целей создания смешной (с точки зрения автора мема) картинки по общему правилу допускается только с согласия лица, изображенного на фотографии. Такое правило содержится, в частности, в п. 1 ст. 152.1 ГК РФ, устанавливающей, что обнародование и дальнейшее использование изображения гражданина (в том числе его фотографии, а также видеозаписи или произведения изобразительного искусства, в которых он изображен) допускаются только с согласия этого гражданина, за исключением некоторых предусмотренных законом случаев. Если такое изображение, полученное или используемое с нарушением п. 1 ст. 152.1 ГК РФ, распространено в сети Интернет, гражданин вправе требовать удаления этого изображения, а также пресечения или запрещения дальнейшего его распространения (п. 3 ст. 152.1 ГК РФ). Правда, на сегодняшний день для защиты прав изображенных лиц обычно используют не указанную статью ГК РФ, а нормы Закона о персональных данных[2].

[1] *Slavick Scott J.* I Can Haz Copyright Infringement? Internet Memes and Intellectual Property Risks – Corporate Council, 14.11.2012.

[2] Примером может стать первое дело о меме: по требованию Роскомнадзора из интернет-энциклопедии Lurkmore был удален мем, созданный на основании фотографии певца Валерия Сюткина с добавлением нецензурной надписи (решение Мещанского районного суда Москвы по делу № 2-1869/2015).

Примечательна в связи с этим инициатива испанских парламентариев: они предложили внести изменения и дополнения в Органический закон о гражданской защите права на честь, неприкосновенность личной и семейной тайны и собственного изображения (*Ley Orgánica 1/1982, de 5 de mayo, de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen*[1]). Существующие положения Органического закона не запрещают фотографирование и публикацию изображения публичного лица, карикатур на него (разумеется, не выходя за рамки разумного), регулируя при этом другие вопросы (об изображении умерших, о запрете использования изображения в коммерческих целях без согласия лица) весьма поверхностно и обще. Изменения предполагают, в частности, включение в Закон положений, которые позволят лицу, считающему себя оскорбленным картинкой в Интернете, обратиться в суд с требованием об устранении правонарушения.

Завершая настоящую статью, хотелось бы заметить, что в январе 2017 г. появилось любопытное сообщение: пользователи сайта *Reddit* (известный зарубежный социальный новостной ресурс, где пользователи делятся ссылками на интересную информацию) создали для мемов... фондовую биржу, алгоритм которой позволяет рассчитать стоимость понравившейся картинки относительно ее популярности в сети[2]. Правда, эта стоимость определяется в фиктивной валюте. Но на сегодняшний день права на мемы (даже при существующей нечеткости их правового режима) вполне способны стать весьма ценным экономическим активом, что позволяет говорить об их реальной ценности, а следовательно, необходимости определения их правового режима.

Пристатейный библиографический список:

1. Ley Orgánica 1/1982, de 5 de mayo, de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen. «BOE» núm. 115, de 14 demayode 1982.

2. *Колосов В.А.* Пародия в системе авторского права // Закон. 2013. № 9.

[1] Ley Orgánica 1/1982, de 5 de mayo, de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen. «BOE» núm. 115, de 14 de mayo de 1982. P. 12546–12548.

[2] См. подробнее: https://lenta.ru/news/2017/01/11/memestock/

3. *Кондратьева И.* +100500 к копирайту: кто владеет правами на мемы (https://pravo.ru/story/view/134865/).

4. *Семенова Е.* Правомерность «креативных» нарушений авторских прав: стиль мэш-ап в современной литературе // ИС. Авторские и смежные права. 2016. Октябрь.

5. *Dewey Caitlin* . How copyright is killing your favorite memes

6. *Martinez Nicole* . Posting an Internet Meme? You May Receive a Getty Letter

7. *Slavick Scott J.* I Can Haz Copyright Infringement? Internet Memes and Intellectual Property Risks.

Е.В. Гаврилов

ЗАЩИТА ДЕЛОВОЙ РЕПУТАЦИИ ОТ ДИФФАМАЦИИ НА ИНТЕРНЕТ-ФОРУМАХ

Аннотация. *В статье исследуется проблема защиты деловой репутации (ст. 152 ГК РФ) от диффамации на интернет-форумах. Приводится противоречивая судебно-арбитражная практика, мнения ученых, правовая позиция Судебной коллегии по экономическим спорам ВС РФ. Автором делается вывод, что информация, размещенная на интернет-форумах, не всегда является оценочным суждением, мнением, убеждением; защита деловой репутации от диффамации на интернет-форумах вполне допустима.*

Ключевые слова: *деловая репутация, Интернет, судебно-арбитражная практика*.

Совет Европы рекомендует государствам-участникам поощрять «использование ИКТ (включая онлайн-форумы, веб-блоги, политические чаты, системы немедленной передачи текстовых сообщений и иные формы коммуникации) гражданами, неправительственными организациями и политическими партиями, с тем чтобы участвовать в демократических обсуждениях, электронной активности и электронных кампаниях, раскрывать свои заботы, идеи и инициативы, поощрять диалог и обсуждения с представителями и правительством, а также для контроля в отношении должностных лиц и политиков по вопросам, представляющим общественный интерес»[1].

Как справедливо отмечает О.Ш. Аюпов, «множество людей уже сейчас ведут Живой Журнал, блоги, в том числе видеоблоги (*youtube.com*, *rutube.ru*), активно пользуются сервисами социальных сетей (например, *vkontakte.ru*, *odnoklassniki.ru*, *facebook.com*, *twetter.com*), что по-

[1] Рекомендация CM/Rec (2007) 16 Комитета министров государствам-членам о мерах по повышению ценности Интернета как общественной службы (цит. по: *Рихтер А.Г.* Комментарий на форуме интернет-СМИ: право и практика в России // Медиаскоп. 2012. № 4. С. 4).

зволяет им доводить свою информацию до тысяч людей, а иногда и до миллионов... Встречаются случаи, когда то или иное сообщение, в том числе видеообращение, какого-то конкретного лица вызывает целую волну обсуждения в сети «Интернет», которая часто передается и традиционным СМИ...»[1]. При этом В. Карпенков подчеркивает: «...в современных условиях опорочить деловую репутацию в сети Интернет достаточно просто. Недобросовестные субъекты могут использовать для этого различные инструменты: многочисленные форумы на интернет-сайтах, доски бесплатных объявлений, ленты СМИ на интернет-сайтах, электронные рассылки, аналитические и сравнительные обзоры и т.п.»[2]. По мнению Н.Н. Парыгиной, «создаются угрозы деловой репутации граждан и организаций в целом, но особый смысл элементы «информационной войны» в Интернете обретают для субъектов предпринимательства»[3].

В связи с вступлением в 2013 г. в силу ФЗ от 02.07.2013 № 142-ФЗ «О внесении изменений в подраздел 3 раздела I части первой Гражданского кодекса Российской Федерации»[4] в российском гражданском законодательстве произошли существенные изменения. В частности, была обновлена редакция ст. 152 ГК РФ, посвященной защите чести, достоинства и деловой репутации.

Среди новелл этой статьи – законодательное закрепление защиты чести, достоинства и деловой репутации от информации в сети Интернет. Согласно п. 5 ст. 152 ГК РФ, если сведения, порочащие честь, достоинство или деловую репутацию гражданина, оказались после их распространения доступными в сети Интернет, гражданин вправе требовать удаления соответствующей информации, а также опровержения указанных сведений способом, обеспечивающим доведение опровержения до пользователей Интернета. Кроме того, гражданин вправе требовать возмещения убытков и компенсации морального вреда, причиненных распространением таких сведений (п. 9 ст. 152 ГК РФ).

---

[1] *Аюпов О.Ш.* Защита деловой репутации юридического лица от диффамации в гражданском праве России: дис. ... канд. юрид. наук. Томск, 2013. С. 177–178.

[2] *Карпенков В.* Защита деловой репутации в сети Интернет // Библиотечка журнала «Юрист». Право и бизнес. 2015. № 3. С. 21.

[3] *Парыгина Н.Н.* Защита права на деловую репутацию юридических лиц и индивидуальных предпринимателей по гражданскому законодательству Российской Федерации: дис. ... канд. юрид. наук. Омск, 2017. С. 137.

[4] Вступил в силу с 01.10.2013.

Названные правила, за исключением положения о компенсации морального вреда, могут быть применены судом также к случаям распространения любых не соответствующих действительности сведений о гражданине, если такой гражданин докажет несоответствие указанных сведений действительности (п. 10 ст. 152 ГК РФ). Эти правила, за исключением положений о компенсации морального вреда, применяются и к защите деловой репутации юридического лица (п. 11 ст. 152 ГК РФ). Таким образом, гражданско-правовая законодательная форма защиты граждан и юридических лиц от диффамации[1] в сети Интернет создана[2].

Пленум ВС РФ ориентирует на то, что распространение сведений, порочащих честь и достоинство граждан или деловую репутацию граждан и юридических лиц, возможно посредством сети Интернет, а также с использованием иных средств телекоммуникационной связи (абз. 2 п. 7 постановления Пленума ВС РФ от 24.02.2005 № 3 «О судебной практике по делам о защите чести и достоинства граждан, а также деловой репутации граждан и юридических лиц»; далее – Постановление Пленума ВС РФ № 3). При этом следует учитывать, что информация распространяется на сайтах, а также на страницах сайтов в сети Интернет (см., примеры, указанные в п. 1, 3, 9, 16 Обзора практики рассмотрения судами дел по спорам о защите чести, достоинства и деловой репутации, утвержденного Президиумом ВС РФ 16.03.2016; далее – Обзор Президиума ВС РФ).

В судебной практике неоднократно вставал вопрос: возможна ли защита деловой репутации по правилам ст. 152 ГК РФ от диффамации на интернет-форумах или размещение такой информации на интернет-форумах в любом случае подразумевает изложение оценочного суждения, мнения, убеждения (далее – оценочное суждение), при которых указанная защита исключается, так как такую информацию априори невозможно проверить на предмет ее соответствия действи-

[1] В соответствии с абз. 5 п. 1 постановления Пленума ВС РФ от 24.02.2005 № 3 «О судебной практике по делам о защите чести и достоинства граждан, а также деловой репутации граждан и юридических лиц» понятие *диффамации* тождественно понятию распространения не соответствующих действительности порочащих сведений, содержащемуся в ст. 152 ГК РФ (здесь и далее практика судов приводится по СПС «КонсультантПлюс»).

[2] Об этом подробнее см., например: *Гаврилов Е.В.* Удаление информации в сети Интернет как способ защиты чести, достоинства и деловой репутации // Законодательство и экономика. 2014. № 2. С. 49–53.

тельности (абз. 3 п. 9 Постановления Пленума ВС РФ № 3[1], п. 6 Обзора Президиума ВС РФ[2])?

Проведенное исследование показало, что в судебно-арбитражной практике по этому вопросу отсутствует единообразие.

Некоторые арбитражные суды расценивали информацию на интернет-форумах как оценочные суждения, защита от которых по правилам ст. 152 ГК РФ невозможна[3]. Этот вывод можно проиллюстрировать на примере трех дел.

Первое дело: Университет обратился в арбитражный суд с иском к ООО и гражданке Г. о признании не соответствующими действительности и порочащими деловую репутацию истца сведений об Университете и его руководителе, содержащихся в статье «Отчислена за собственное мнение?» и комментариях к ней, распространенных на форуме сайта *fontanka.ru* (интернет-газета). Кроме того, истец просил суд обязать ответчиков опубликовать на главной странице этого сайта текст опровержения сведений об Университете, изложенных в указанной статье и комментариях к ней, а также взыскать солидарно с ответчиков 2 млн 400 тыс. руб. компенсации вреда, причиненного деловой репутации истца.

В удовлетворении исковых требований было отказано.

---

[1] Согласно абз. 3 п. 9 Постановления Пленума ВС РФ № 3 при рассмотрении дел о защите чести, достоинства и деловой репутации судам следует различать имеющие место утверждения о фактах, соответствие действительности которых можно проверить, и оценочные суждения, мнения, убеждения, которые не являются предметом судебной защиты в порядке ст. 152 ГК РФ, поскольку, являясь выражением субъективного мнения и взглядов ответчика, не могут быть проверены на предмет соответствия их действительности.

[2] В соответствии с п. 6 Обзора Президиума ВС РФ при рассмотрении дел о защите чести, достоинства и деловой репутации необходимо учитывать, что содержащиеся в оспариваемых высказываниях ответчиков оценочные суждения, мнения, убеждения не являются предметом судебной защиты в порядке ст. 152 ГК РФ, если только они не носят оскорбительный характер.

[3] См., например, постановления: ФАС Уральского округа от 13.08.2009 № Ф09-5765/09-С6 по делу № А76-24275/2008; ФАС Северо-Западного округа от 07.09.2009 по делу № А56-14384/2008, от 15.06.2009 по делу № А56-22460/2008; ФАС Западно-Сибирского округа от 24.03.2010 по делу № А45-15768/2009; ФАС Московского округа от 14.12.2010 № КГ-А40/16066-10 по делу № А40-44562/10-12-267, от 11.09.2013 по делу № А40-42622/12-27-384; ФАС Северо-Западного округа от 17.02.2014 № Ф07-11041/2013 по делу № А56-14971/2013; АС Уральского округа от 19.02.2016 № Ф09-12215/15 по делу № А60-10981/2015; Одиннадцатого ААС от 22.09.2016 по делу № А55-26741/2015; Семнадцатого ААС от 11.10.2016 № 17АП-12604/2016-ГК по делу № А60-11108/2016. См. также: Арбитражный суд Свердловской области в 2009 году / под ред. проф. И.В. Решетниковой / сост. В.С. Трухин. Екатеринбург, 2009. С. 38–39.

Отказывая в иске, суды подчеркнули, что Интернет является общепризнанным средством массовой коммуникации, использующимся с целью общения и получения информации. При этом подчеркивалось, что форум на указанном сайте смоделирован таким образом, что комментарии читателей (пользователей) поступают на него в режиме онлайн и не могут быть предварительно проверены на соответствие действительности содержащейся в них информации. Суд признал, что *комментарии к статье, размещенной на сайте, являются личными мнениями читателей, излагаемыми в ходе широкого обсуждения – дискуссии по вопросам, затронутым в статье,* и, соответственно, на учредителя интернет-газеты не может быть возложена ответственность по заявленным истцом требованиям и в части опубликованных комментариев к статье «Отчислена за собственное мнение?». Оспариваемые истцом фрагменты комментариев к статье, размещенных на форуме интернет-газеты, не относятся к фактам, соответствие действительности которых можно проверить, поскольку являются оценочным суждением их авторов[1].

Второе дело: ООО и гражданин З. обратились в арбитражный суд с иском к ООО – владельцу сайта *rabota.ngs.ru* о признании не соответствующими действительности и порочащими деловую репутацию истцов распространенные на форуме сайта сведения относительно нарушения истцом ТК РФ, низкого профессионального уровня сотрудников истцов, торговли неликвидным товаром по неконкурентным ценам. Кроме того, истцы требовали опровергнуть не соответствующие действительности и порочащие деловую репутацию сведения, взыскать с ответчика 100 тыс. руб. в возмещение репутационного вреда, причиненного умалением деловой репутации, взыскать с ответчика 100 тыс. руб. в возмещение морального вреда, причиненного гражданину З.

Заявленные требования были удовлетворены судом первой инстанции частично[2]. Суд признал не соответствующими действительности и порочащими деловую репутацию сведения, относительно нарушения истцами ТК РФ, низкого профессионального уровня сотрудников, работающих в данной организации, торговли нелик-

[1] Решение АС города Санкт-Петербурга и Ленинградской области от 19.02.2009 по делу № А56-14384/2008, оставленное без изменения постановлениями Тринадцатого ААС от 22.05.2009 и ФАС Северо-Западного округа от 07.09.2009 по тому же делу. Определением ВАС РФ от 23.12.2009 № ВАС-17363/09 отказано в передаче дела № А56-14384/2008 в Президиум ВАС РФ для пересмотра в порядке надзора вышеуказанных судебных актов.

[2] Решение АС Новосибирской области от 25.09.2009 по делу № А45-15768/2009.

видным товаром по неконкурентным ценам. Суд также обязал ответчика опровергнуть указанные сведения. В остальной части исковых требований отказано.

Постановлением апелляционной инстанции решение было отменено, в удовлетворении заявленных требований отказано полностью[1].

Кассационная инстанция согласилась с выводами суда апелляционной инстанции о том, что оспариваемые сведения изложены в форме обмена мнениями и размещены в сети Интернет на форуме. В судебном акте в связи с этим отмечалось следующее.

Форум (англ. www-conference, синонимы: конференция, веб-конференция) – это инструмент для общения на сайте, это форма общения в виде сообщений конкретных лиц, которые высказывают собственные мнения и оценки относительно темы, заданной этими же лицами. Исследуемые фрагменты сведений содержат оценку личных качеств истцов, являются объективным мнением авторов, которая не может быть проверена на предмет ее соответствия действительности. Частное мнение автора может быть оспорено заинтересованным лицом в порядке полемики, т.е. ответа, реплики или комментария.

Суд признал, что оспариваемые сведения, размещенные на форуме на сайте ответчика в период с 12.11.2008 по 21.05.2009, не являются утверждением о событиях и фактах, которые имели место в реальной действительности, а отражают субъективное мнение анонимных авторов и не относятся к сведениям, не соответствующим действительности и порочащим деловую репутацию истцов. Специально подчеркивалось, что все сообщения, размещенные на сайте ответчика, фактически являются анонимными и не содержат сведений, позволяющих идентифицировать их авторов[2].

Третье дело: Общество обратилось в арбитражный суд с иском к индивидуальному предпринимателю (далее – ИП) с требованием о защите деловой репутации, обязании последнего удалить сведения, порочащие честь, достоинство и деловую репутацию истца с сайта *ati.su* (система «Автотрансинфо»). Кроме того, истец требовал от ответчика написать опровержение на форуме «Круглый стол» на сайте *ati.su* в 10-дневный срок и просил суд взыскать с ответчика компенсацию в размере 150 тыс. руб.

[1] Постановлением Седьмого ААС от 22.12.2009 по делу № А45-15768/2009.

[2] Постановление ФАС Западно-Сибирского округа от 24.03.2010 по делу № А45-15768/2009.

В удовлетворении исковых требований было отказано[1].

Арбитражные суды, проанализировав словесно-смысловую конструкцию оспариваемых фраз и выражений, оценив предлагаемые истцом фрагменты в контексте всех публикаций на форуме, пришли к выводу о том, что материал представляет собой комментарий в виде выраженного собственного мнения ответчика об истце, о фактических событиях в отношении данной компании, которые имели место быть. Судами также принято во внимание, что *информация размещена в Интернете на ресурсе, предназначенном для размещения комментариев/отзывов относительно той или иной компании*. Оцененный материал представляет собой диалог на форуме в виде выраженного мнения ИП о ситуации, сложившейся в связи с уклонением Общества (истца) от оплаты задолженности за перевозку. Эта *информация носит дискуссионный характер и явно выражена в форме диалога*, в том числе и с Обществом. Целевое и функциональное назначение форума «Круглый стол» (сайт для профессиональных перевозчиков и экспедиторов) состоит в обмене мнениями и не предполагает размещение исключительно положительной оценки деятельности компании ее контрагентами. *Как содержание, так и общий контекст информации, ее размещение на соответствующей целевой интернет-странице* (*форуме*), *по мнению суда, указывают на субъективно-оценочный характер оспариваемых высказываний, являющихся реализацией права на свободу слова*.

При таких обстоятельствах суды пришли к выводу о том, что высказывания автора-ответчика представляют собой оценочные суждения, субъективное мнение автора и в порядке ст. 152 ГК РФ не могут быть проверены на предмет их соответствия действительности. Обсуждавшиеся на форуме сведения о наличии задолженности истца, образовавшейся в связи с невыполнением договорных обязательств перед ответчиком, соответствуют действительности. При этом размещение информации о наличии задолженности (тем более сделанное на специальном интернет-форуме, созданном для обмена мнениями), как указали суды, не может рассматриваться как неправомерное ущемление деловой репутации в соответствии со ст. 152 ГК РФ. С учетом этого в удовлетворении исковых требований было отказано[2].

[1] Решение АС Свердловской области от 09.09.2015 по делу № А60-10981/2015 было оставлено без изменения постановлениями Семнадцатого ААС от 26.11.2015 и АС Уральского округа от 19.02.2016 № Ф09-12215/15 по делу тому же делу.

[2] Постановление АС Уральского округа от 19.02.2016 № Ф09-12215/15 по делу № А60-10981/2015.

Другие арбитражные суды, напротив, не исключали возможность распространения на форумах в сети Интернет не только оценочных суждений, но и сведений, имеющих «фактологическую основу», утверждений о фактах, при наличии которых защита, предусмотренная ст. 152 ГК РФ, вполне реальна[1]. Этот подход можно также проиллюстрировать тремя примерами.

Первое дело: Общество обратилось в арбитражный суд с иском к гражданке А. и другому Обществу о признании не соответствующими действительности и порочащими деловую репутацию сведений, распространенных гражданкой А. на сайте *e1.ru* в разделе «Автострахование»; возложить на Общество-ответчика обязанность разместить на сайте *e1.ru* в разделе «Автострахование» опровержение оспариваемых сведений; взыскать с гражданки А. 50 тыс. руб. компенсации нематериальных убытков, причиненных умалением деловой репутации истца.

В удовлетворении иска судом первой инстанции было отказано[2].

Отказывая в удовлетворении исковых требований, суд исходил из того, что оспариваемые истцом сведения не подпадают под действие ст. 152 ГК РФ, поскольку представляют собой *личное мнение автора и его оценку относительно конкретной темы, обсуждаемой на форуме в форме публичных дебатов*. Оспариваемые сведения изложены в форме обмена мнениями и размещены на интернет-форуме.

При этом суды указали, что *форум – это инструмент для общения на сайте, т.е. это форма общения в виде сообщений конкретных лиц, которые высказывают собственные мнения и оценки относительно темы, заданной этими же лицами*. По мнению судов, оспариваемые фразы являются оценочными суждениями автора-ответчика и с точки зрения композиционной структуры текста, а также жанровых и стилистических особенностей подачи материала (о чем свидетельствуют использование вводных слов, наличие вопросительных предложений

[1] См., например, постановления: ФАС Уральского округа от 12.10.2009 № Ф09-7703/09-С6 по делу № А60-33583/2008-С7, от 14.07.2010 № Ф09-7703/09-С6 по делу № А60-33583/2008-СР; ФАС Московского округа от 22.05.2012 по делу № А41-19354/11; АС Северо-Западного округа от 09.09.2014 по делу № А56-53759/2013; АС Московского округа от 25.09.2014 № Ф05-8127/2013 по делу № А40-145328/12-19-1235, от 27.11.2014 № Ф05-16421/2013 по делу № А40-151241/12-12-698; АС Волго-Вятского округа от 22.06.2015 № Ф01-1801/2015, Ф01-1802/2015 по делу № А82-1121/2013.

[2] Решение АС Свердловской области от 07.04.2009 по делу № А60-33583/2008-С7, оставленное без изменения постановлением Семнадцатого ААС от 09.07.2009 по тому же делу.

без ответа и таких словесных конструкций, как «расскажу про случай, когда...», «двойные стандарты» и т.д.).

Кассационная инстанция не согласилась с указанным обоснованием. Суд сделал вывод: из содержания п. 7 Постановления Пленума ВС РФ № 3 следует, что возможность опровержения сведений в порядке, предусмотренном положениями ст. 152 ГК РФ, поставлена в *зависимость от содержания этих сведений, а не от формы или способа их изложения. Таким образом, в сообщениях лиц, которые размещаются на форуме, также могут содержаться утверждения порочащего характера, которые могут быть проверены на предмет их соответствия действительности*. Кроме того, по мнению суда, в данном случае особенностью общения на форуме явилось то, что сначала была размещена информация (сведения о факте) и затем на эту информацию последовали отзывы участников форума.

Таким образом, по мнению арбитражного суда округа, нельзя согласиться с выводом о том, что, поскольку оспариваемая информация была изложена на интернет-форуме, который, по мнению ответчиков, создан для обмена мнениями по какому-либо вопросу, она изначально является **субъективным мнением (оценочным суждением)** и не может быть опровергнута в порядке, предусмотренном ст. 152 ГК РФ. Кассация обратила внимание на то, что текст сообщений, имеющихся на сайте e1.ru в разделе «Автострахование», в котором содержатся в том числе и оспариваемые сведения, начинается с утверждения «СК «Северная казна» нарушает закон!!!»; далее в тексте также идут ссылки на то, что истец нарушает закон, не выполняет своих обязательств. Кроме того, в сообщении указывается и то, каким образом истцом нарушаются требования закона. Утверждения о нарушении юридическим лицом действующего законодательства имеют порочащий характер.

При таких обстоятельствах принятые по делу судебные акты были отменены, а дело направлено на новое рассмотрение в суд первой инстанции[1].

По итогам нового рассмотрения исковые требования были удовлетворены частично: признаны не соответствующими действительности и порочащими деловую репутацию истца отдельные сведения, распространенные ответчиком А. на сайте *el.ru*, на Общество – владельца

[1] Постановление ФАС Уральского округа от 12.10.2009 № Ф09-7703/09-С6 по делу № А60-33583/2008-С7.

сайта возложена обязанность разместить на этом сайте в разделе «Автострахование» опровержение диффамационных сведений. С ответчика А. в пользу истца взыскано 5 тыс. руб. компенсации нематериальных убытков, причиненных умалением деловой репутации[1].

Второе дело: ООО обратилось в арбитражный суд к гражданину Х. о признании не соответствующими действительности, порочащими деловую репутацию истца сведений, содержащихся на сайте *diac.ru*.

В удовлетворении иска было отказано[2]. Кассационная инстанция решение и постановление апелляционной инстанции отменила, дело направила на новое рассмотрение[3].

При новом рассмотрении исковые требования были удовлетворены. Это решение было поддержано кассационной инстанцией.

В постановлении кассации указывалось, что размещение информации на интернет-сайте относится к публикациям в СМИ. Поскольку оспариваемая информация содержит утверждения о фактах и изложена в утвердительной форме, не содержит оценочных суждений, при ее прочтении складывается определенное негативное мнение об истце, информация не является выражением субъективного взгляда и может быть проверена на предмет соответствия действительности, представляет собой акт недобросовестной конкуренции. Оспариваемые утверждения порочат деловую репутацию истца, поскольку создают у потенциальных партнеров, клиентов или заказчиков ложное представление о том, что истец осуществляет предпринимательскую деятельность с грубыми нарушениями действующего законодательства. Суд округа обратил внимание, что *распространение сведений на интернет-форуме анонимными авторами не может являться основанием для отказа в иске*. Анализ всех комментариев посетителей сайта позволяет сделать вывод о том, что оспариваемые сведения распространены именно в отношении истца, который является профессиональным участником рынка в области технического обслуживания контрольно-кассовых машин, притом что сайт *diac.ru* используется только участниками указанного рынка обслуживания[4].

---

[1] Постановление ФАС Уральского округа от 14.07.2010 № Ф09-7703/09-С6 по делу № А60-33583/2008-СР.

[2] Решение АС города Москвы от 22.02.2013 по делу № А40-145328/12-19-1235, оставленное без изменения постановлением Девятого ААС от 19.04.2013 по тому же делу.

[3] Постановление АС Московского округа от 24.07.2013.

[4] Постановление АС Московского округа от 25.09.2014 № Ф05-8127/2013 по делу № А40-145328/12-19-1235.

Третье дело: ООО обратилось в арбитражный суд к Издательскому дому и гражданину Н. с иском о признании не соответствующими действительности и порочащими деловую репутацию истца отдельных сведений, размещенных на сайте *gmstar.ru*. Истец просил обязать гражданина Н. удалить в электронном СМИ (на сайте *gmstar.ru*) страницу, посвященную ООО, а также взыскать с ответчиков солидарно компенсацию нематериального (репутационного) вреда в размере 5 млн руб., расходы по нотариальному удостоверению доказательств в размере 10 тыс. руб.

В иске было отказано[1]. По мнению судов первой и апелляционной инстанций, оспариваемые фрагменты сообщения с интернет-форума, как отдельно, так и в совокупности с содержательно-смысловой направленностью статьи, в целом не содержат порочащих сведений в форме утверждений о совершении истцом каких-либо противоправных деяний. Иными словами, эти сообщения не являются утверждением о событиях и фактах, которые имели место в реальной действительности, а представляют собой субъективное мнение посетителей форума относительно оценки купленной продукции. Таким образом, оспариваемые истцом высказывания, размещенные на сайте www.gmstar.ru, являются *оценочными суждениями посетителей форума, представляют собой эмоциональное описание личного мнения людей*.

С таким выводом не согласился суд кассационной инстанции. Он указал, что для того, чтобы выяснить, является ли распространенная информация сведениями или же в ней содержится субъективное мнение того или иного лица, необходимо исследовать вопрос о возможности проверки такой информации на ее соответствие объективной действительности. Суд подчеркнул, что мнения отражают внутреннюю, субъективную оценку описываемой информации конкретного лица и не могут быть подвергнуты подобной проверке; правдивость оценочных суждений не поддается доказыванию исходя из природы их происхождения.

Суд обратил внимание на то, что *объективную сторону клеветы может составлять ограниченный круг оценочных суждений – только те, которые имеют под собой фактическую основу*. Такого рода оценки следует рассматривать как разновидность сведений, отличную от описательных суждений (утверждений о фактах). Как таковые они не со-

[1] Решение АС г. Москвы от 03.06.2013 по делу № А40-151241/12-12-698, оставленным без изменения постановлением Девятого ААС от 16.09.2013 по тому же делу.

держат прямого указания на действительные события или действия, но дают основания аудитории домыслить соответствующие факты исходя из того спектра, который задает оценочное суждение.

Если мнение или оценка порождены состоянием внутреннего мира человека, его частными убеждениями, установками и предпочтениями, то такие оценочные суждения не могут признаваться соответствующими либо не соответствующими объективной действительности и быть опровергнуты. Однако *если выраженное мнение привязано к каким-либо фактам или информации, т.е. появляется фактическое основание оценки или информационная составляющая мнения, то это мнение* (*или оценка*) *может быть проверено в ходе судебного разбирательства и опровергнуто.*

Суд кассационной инстанции указал, что нижестоящие суды не дали конкретную оценку ни оспариваемым истцом высказываниям, ни отдельным словам (таким, как «зомбирование», «обман», «развод на деньги»), не проводилось разграничение высказываний на те, которые являются личными оценочными суждениями посетителей форума, и те, которые содержат (обоснованные или нет) обвинения истца в недобросовестной предпринимательской деятельности и т.д. С учетом этого вынесенные судебные акты были отменены, а дело направлено на новое рассмотрение в суд первой инстанции[1].

При новом рассмотрении дела в иске снова было отказано[2]. Суды указали, что оспариваемые сведения представляют собой выражение субъективного мнения по ряду событий и направлены на так называемую *политико-публицистическую дискуссию, начатую в СМИ*. В связи с этим, с точки зрения судов, эти мнения не могут быть проверены на соответствие действительности и быть предметом доказывания. Также суды не нашли оснований рассматривать оспариваемые фрагменты сообщений с интернет-форума как содержащие порочащие сведения о совершении истцом каких-либо противоправных деяний, суды признали эти фрагменты оценочным, субъективным суждением потребителя. Суд первой инстанции отметил, что *спорные сообщения рассматриваются без корректировки*[3]*, с сохранением лексики и грамма-*

[1] Постановление ФАС Московского округа от 25.12.2013 № Ф05-16421/2013 по делу № А40-151241/12-12-698.

[2] Решение АС г. Москвы от 11.04.2014 по делу № А40-151241/12-12-698, оставленному без изменения постановлением Девятого ААС от 07.08.2014 по тому же делу.

[3] Дополнительно следует отметить, что согласно абз. 3 п. 7 Постановления Пленума ВС РФ № 3 судам следует иметь в виду: в случае, если не соответствующие действительности порочащие сведения были размещены в сети Интернет на информацион-

тики авторов, из чего можно сделать вывод, что отдельные слова могут быть авторской формой выражения, продиктованные эмоциональным восприятием ситуации, их реакцией на происходящие, и никоим желанием нанести вред репутации истца. Апелляционный суд также отметил, что способ опубликования данной информации (на интернет-форуме) по своему предназначению предполагает высказывание субъективной оценки различными лицами.

Арбитражный суд Московского округа вышеназванные судебные акты отменил как противоречащие правовой позиции КС РФ, сформулированной в Определении от 01.03.2010 № 323-О-О. Согласно этой позиции *реальная защита прав и законных интересов лица, чьи честь, достоинство и доброе имя потерпели ущерб в результате распространения не соответствующей действительности негативной информации, в любом случае должна быть обеспечена*.

Основываясь на положениях Постановления КС РФ от 09.07.2013 № 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», суд кассационной инстанции признал неверными выводы судов обеих инстанций о том, что способ опубликования информации на интернет-форуме по своему пред-

ном ресурсе, зарегистрированном в установленном законом порядке в качестве СМИ, при рассмотрении иска о защите чести, достоинства и деловой репутации необходимо руководствоваться нормами, относящимися к СМИ. В силу абз. 6 п. 23 постановления Пленума Верховного Суда РФ от 15.06.2010 № 16 «О практике применения судами Закона Российской Федерации «О средствах массовой информации»», если на сайте в сети Интернет, зарегистрированном в качестве СМИ, комментарии читателей размещаются *без предварительного редактирования* (например, на форуме читателей материалов такого сайта), то в отношении содержания этих комментариев следует применять правила, установленные в п. 5 ч. 1 ст. 57 Закона РФ от 27.12.1991 № 2124-I «О средствах массовой информации» (далее – Закон о СМИ) для авторских произведений, идущих в эфир без предварительной записи, т.е. редакция, главный редактор, журналист не несут ответственность за диффамацию. В случае поступления обращения уполномоченного государственного органа, установившего, что размещенные комментарии являются злоупотреблением свободой массовой информации, редакция указанного СМИ вправе удалить их с сайта либо отредактировать, руководствуясь положениями ст. 42 Закона о СМИ. Если комментарии, представляющие собой злоупотребление свободой массовой информации, и после этого остаются доступными для пользователей данного сайта в сети Интернет, то правила п. 5 ч. 1 ст. 57 Закона о СМИ не применяются. С учетом этого при рассмотрении вопроса о допустимости привлечения редакции к ответственности судам следует выяснять, выдвигались ли уполномоченным государственным органом требования об удалении сведений с форума, а также было ли произведено удаление либо редактирование сведений, в связи с распространением которых перед судом поставлен вопрос о привлечении редакции к ответственности.

назначению предполагает лишь высказывание субъективной оценки различными лицами, а анонимность авторов (пользователей сайта Интернет) не дает возможности для проверки действительности и достоверности их высказываний. По мнению кассационной инстанции, подобный подход фактически лишает обратившееся в суд лицо судебной защиты; при рассмотрении подобных исков юридических лиц суд должен проверить достоверность оспариваемых истцом высказываний пользователей и установить, являются ли они порочащими деловую репутацию юридического лица.

Вместе с тем, поскольку сведения, которые истец оценивал как порочащие его деловую репутацию, на момент вынесения решения по существу дела уже были удалены с сайта, у суда отсутствовали основания для судебной защиты истца ввиду устранения нарушений его прав. В связи с этим обстоятельством в удовлетворении иска было отказано[1].

В юридической литературе также отсутствует однозначное понимание исследуемого вопроса. Одни юристы выступают против отнесения содержащихся на интернет-форумах сообщений к сведениям, влекущим судебную защиту по правилам ст. 152 ГК РФ, другие – напротив, считают, что в некоторых случаях подобные сообщения представляют собой полноценное основание для постановки вопроса о защите деловой репутации.

Так, например, З.В. Каменева указывает, что «распространение информации на форуме представляет собой изложение субъективного мнения, так как его изначальное предназначение – высказывание личного мнения по поставленному вопросу»[2]. И. Смоленский категорично заявляет, что «не может считаться сведениями о фактах содержание дискуссионных интернет-форумов»[3].

Иной точки зрения придерживается О.Ш. Аюпов. Он не ставит под сомнение допустимость защиты деловой репутации от диффамации на интернет-форумах и, акцентируя внимание на проблеме надлежащего ответчика по делам о диффамацию в сети Интернет, приходит к следующему заключению: «...если диффамация содержалась в комментарии пользователя, который размещается без предварительно-

[1] Постановление АС Московского округа от 27.11.2014 № Ф05-16421/2013 по делу № А40-151241/12-12-698.

[2] *Каменева З.В.* Опыт правового регулирования диффамации в мире // Адвокат. 2014. № 6. С. 46–47.

[3] *Смоленский И.* Ложное утверждение – наказуемо, ошибочное мнение – допустимо // эж-ЮРИСТ. 2011. № 13. С. 4.

го редактирования на сайте в сети Интернет, зарегистрированном в качестве СМИ, то ответственность несет не владелец сайта, а такой пользователь. Однако если владелец сайта был уведомлен государственным органом или иным заинтересованным лицом о том, что на его сайте размещена информация, которая нарушает права других лиц, то он будет нести ответственность вместе с лицом, разместившим такие сведения. Вместе с тем не все сайты в сети «Интернет» зарегистрированы как СМИ. Но и в таких случаях, на наш взгляд, должно применяться указанное правило, поскольку отсутствует вина владельца сайта... Вместе с тем владелец сайта не освобождается от иных правовых последствий за диффамацию, в том числе в виде опровержения и (или) удаления информации, поскольку они наступают независимо от вины»[1]. Н.Н. Парыгина по исследуемому вопросу приходит к справедливому выводу о том, что «анализу все же должны подвергаться сами сообщения, суть распространяемых сведений. В противном случае получилось бы, что для безнаказанного незаконного «вброса» порочащей дезинформации следует только выбрать правильное место обнародования, судебная же защита от диффамации стала бы в этом случае призрачной»[2]. Е.И. Сизова отмечает, что «трактовка форума и сообщений на форуме и в комментариях к статьям в качестве мнений и суждений не дает возможности истцу получить возмещение не только с владельца форума, но и с автора распространенной информации и, кроме того, не позволяет восстановить нарушенное право в форме опубликования опровержения на сайте»[3].

В завершение хотелось бы разобрать позицию Судебной коллегии по экономическим спорам ВС РФ, за которой на сегодняшний день следует признать определяющую роль для правоприменительной практики по исследуемому вопросу.

Дело было возбуждено на основании иска Предприятия к гражданке В., в рамках которого было заявлено требование о признании сведе-

[1] *Аюпов О.Ш.* Указ. соч. С. 105–106, 109. К проблеме надлежащего ответчика за диффамацию в сети Интернет обращались и другие авторы, например В.В. Карпенков (*Карпенков В.В.* Защита деловой репутации юридических лиц по законодательству Республики Беларусь: автореф. дис. ... канд. юрид. наук. Минск, 2012. С. 4, 5, 14, 15), В. Петров и Д. Бородин (*Петров В., Бородин Д.* Имя компании порочат в интернете. Как добиться опровержения и взыскать возмещение вреда // Юрист компании. 2016. № 8. С. 72–75).

[2] *Парыгина Н.Н.* Указ. соч. С. 84.

[3] *Сизова Е.И.* Некоторые аспекты дел о защите деловой репутации, затронутой недостоверными порочащими сведениями, распространенными в сети Интернет // Арбитражные споры. 2010. № 4. С. 147–148.

ний, распространенных ответчиком, порочащими деловую репутацию истца, об обязании ответчика опровергнуть эти сведения путем размещения соответствующей информации в сети Интернет, о взыскании 1 руб. убытков и 50 тыс. руб. компенсации нематериального вреда.

Мотивом для обращения в суд явилось распространение ответчиком в социальной сети «Вконтакте» на странице группы, посвященной археологии (*vk.com/archaeologynews*), информации, которая, по мнению Предприятия, была недостоверной и порочила его деловую репутацию. Предприятие сочло, что вследствие распространения этой информации для него наступили неблагоприятные последствия. В частности, умаление деловой репутации Предприятия привело к отказу потенциальных контрагентов, имеющих возможность осуществлять деятельность, связанную с археологическими раскопками, от участия в конкурсе на заключение договора на проведение спасательных археологических работ, – в итоге конкурс был признан несостоявшимся; действия ответчика привели к срыву сроков реализации федеральной программы на территории Республики Башкортостан; истец вынужден был заключать договоры с третьими лицами на осуществление услуг эксплуатационно-технического обслуживания оборудования, а также на осуществление услуг по техническому обеспечению включения в региональный эфир телеканала ТВЦ и НТВ региональной рекламы в городе Уфе, неся убытки в размере 217 787 руб.

Решением суда, поддержанным вышестоящими судебными инстанциями[1], в удовлетворении иска было отказано со ссылкой на то, что оспариваемые сведения являются не утверждениями о фактах, а оценочными суждениями, размещенными на интернет-форуме, что исключает возможность защиты деловой репутации в порядке ст. 152 ГК РФ.

Судебная коллегия по экономическим спорам ВС РФ с таким выводом не согласилась.

Ссылаясь на ст. 150, 152 ГК РФ, п. 7 Постановления Пленума ВС РФ № 3, п. 5 Обзора Президиума ВС РФ, практику Европейского суда по правам человека, Судебная коллегия констатировала, что оспариваемые сведения представляют собой информацию о незаконном и недобросовестном поведении предприятия, сформулированы в фор-

[1] Решение АС Республики Башкортостан от 30.11.2015 по делу № А07-12906/2015, оставленное без изменения постановлением Восемнадцатого ААС от 12.02.2016 и постановлением АС Уральского округа от 31.05.2016 по тому же делу.

ме утверждений. Изложение этих сведений не указывает на то, что описываемые факты предполагаются автором или автор таким образом оценивает поведение истца. Избранный автором стиль изложения информации указывает на наличие описываемых фактов в реальной действительности (факта занижения стоимости работ, факта установления демпинговой цены, факта некомпетентности составителей конкурсной документации, фактов коррупционного и иного незаконного поведения, мошенничества). При таких обстоятельствах, по мнению Судебной коллегии ВС РФ, *выводы судов о субъективном характере оспариваемых сведений не являются верными*, а перечисленные факты допускают их проверку на соответствие действительности, что подтверждает и позиция самого ответчика, доказывавшего соответствие действительности своих утверждений.

По мнению Судебной коллегии, информация, размещаемая на форумах в социальных сетях, может быть и не оценочным суждением. Поэтому судам необходимо установить, можно ли оспариваемые сведения проверить на предмет соответствия их действительности или нет. Если такая проверка возможна, то имеют место утверждения о фактах, а не оценочные суждения, а в этом случае защита деловой репутации в порядке ст. 152 ГК РФ вполне допустима. Исходя из изложенного Судебная коллегия оспариваемые судебные акты отменила, дело направила на новое рассмотрение в суд первой инстанции[1].

При новом рассмотрении Арбитражный суд Республики Башкортостан уточненные исковые требования удовлетворил частично[2].

Дополнительно обращаем внимание, что выводы, сделанные Судебной коллегией по экономическим спорам ВС РФ, нашли свое отражение в Обзоре судебной практики ВС РФ № 1 (2017), утвержденном Президиумом ВС РФ 16.02.2017 (в редакции Обзора судебной практики ВС РФ № 2 (2017), утвержденного Президиумом ВС РФ 26.04.2017).

По нашему мнению, с такой позицией сложно не согласиться. Не важно, где распространены сведения (в печати, по радио, телевидению или в Интернете) – если суд установит, что они являются порочащими деловую репутацию и (или) не соответствующими действительности, представляют собой утверждения о фактах, то заинтересованное лицо вправе требовать защиты своей деловой репутации

[1] Определение Судебной коллегии по экономическим спорам ВС РФ от 16.12.2016 № 309-ЭС16-10730.

[2] Решение АС Республики Башкортостан от 24.08.2017 по делу № А07-12906/15.

в соответствии со ст. 152 ГК РФ. При противоположном подходе есть угроза того, что деловая репутация, которой посредством Интернета нанесен урон, останется без должной защиты, а нарушители – без наказания[1].

Пристатейный библиографический список:

1. *Аюпов О.Ш.* Защита деловой репутации юридического лица от диффамации в гражданском праве России: дис. ... канд. юрид. наук. Томск, 2013. – 224 с.

2. *Гаврилов Е.* Компенсация нематериального (репутационного) вреда юридическим лицам: история и современное состояние // Приложение к ежемесячному юридическому журналу «Хозяйство и право». 2017. № 2.

3. *Гаврилов Е.В.* Удаление информации в сети Интернет как способ защиты чести, достоинства и деловой репутации // Законодательство и экономика. 2014. № 2.

4. *Каменева З.В.* Опыт правового регулирования диффамации в мире // Адвокат. 2014. № 6.

5. *Карпенков В.* Защита деловой репутации в сети Интернет // Библиотечка журнала «Юрист». Право и бизнес. 2015. № 3.

6. *Карпенков В.В.* Защита деловой репутации юридических лиц по законодательству Республики Беларусь: автореф. дис. ... канд. юрид. наук. Минск, 2012. – 21 с.

7. *Парыгина Н.Н.* Защита права на деловую репутацию юридических лиц и индивидуальных предпринимателей по гражданскому законодательству Российской Федерации: дис. ... канд. юрид. наук. Омск, 2017. – 270 с.

8. *Петров В., Бородин Д.* Имя компании порочат в интернете. Как добиться опровержения и взыскать возмещение вреда // Юрист компании. 2016. № 8.

9. *Рихтер А.Г.* Комментарий на форуме интернет-СМИ: право и практика в России // Медиаскоп. 2012. № 4.

[1] В частности, при наличии соответствующих основания и условий юридическое лицо имеет право на денежную компенсацию за необоснованное умаление деловой репутации (см. об этом подробнее, например: *Гаврилов Е.* Компенсация нематериального (репутационного) вреда юридическим лицам: история и современное состояние // Приложение к журналу «Хозяйство и право». 2017. № 2).

10. *Сизова Е.И.* Некоторые аспекты дел о защите деловой репутации, затронутой недостоверными порочащими сведениями, распространенными в сети Интернет // Арбитражные споры. 2010. № 4.

11. *Смоленский И.* Ложное утверждение – наказуемо, ошибочное мнение – допустимо // эж-ЮРИСТ. 2011. № 13.

С.А. Курочкин

ОНЛАЙН АРБИТРАЖ: ПРАВОВЫЕ АСПЕКТЫ

Аннотация. *Распространение современных способов передачи и хранения данных не обошло стороной и сферу арбитража. Применение при разрешении споров электронных средств коммуникации привело к появлению онлайн арбитража – простого и действенного способа разрешения правовых конфликтов, возникающих в сфере гражданского оборота. В предлагаемой читателям статье представлены итоги исследования онлайн арбитража как прагматичного правового механизма разрешения споров арбитрами и последующего принятия третейским судом обязательного для сторон решения с применением современных средств коммуникации и накопления данных. Особое внимание уделено анализу правовых аспектов онлайн арбитража, выявлению сферы его эффективного применения, а также вопросам организации арбитражного разбирательства в режиме онлайн.*

Ключевые слова*: онлайн арбитраж, арбитражное соглашение, место арбитража, разрешение споров, делокализация, процедура, арбитражное решение.*

Международным сообществом самое серьезное внимание уделяется вопросам урегулирования споров в режиме онлайн, прежде всего применительно к трансграничным электронным коммерческим сделкам. Комиссия ООН по праву международной торговли в 2010 г. сформировала Рабочую группу по урегулированию споров в режиме онлайн, которая в настоящее время работает над проектом итогового документа ЮНСИТРАЛ, отражающего элементы и принципы процедуры разрешения споров онлайн[1]. Среди способов урегулирования споров в онлайн режиме наибольшее распространение в настоящее время получил онлайн арбитраж (*online arbitration*). Как форма разрешения споров этот вид арбитража становится все более популярным, прежде всего в связи с развитием электронной торговли.

[1] Урегулирование споров в режиме онлайн применительно к трансграничным электронным коммерческим сделкам. Проект итогового документа, отражающего элементы и принципы процедуры УСО. Рабочая группа III. Тридцать третья сессия. Нью-Йорк, 29 февраля – 4 марта 2016 года (www.uncitral.org).

За рубежом многими организациями, работающими в сфере альтернативного разрешения правовых конфликтов, предприняты шаги по развитию проектов онлайн арбитража. Одним из первых среди них стал «Виртуальный Магистрат» (*Virtual Magistrate*), созданный при поддержке Американской Арбитражной Ассоциации. Вынесение «Виртуальным Магистратом» 08.05.1996 решения по спору после взаимодействия с его сторонами исключительно при помощи электронных коммуникаций считается первым случаем применения онлайн арбитража. В России с 2015 г. действует арбитраж онлайн при Российской Арбитражной Ассоциации (далее – РАА).

Что же такое онлайн арбитраж?

*Онлайн арбитраж – это процесс разрешения спора арбитрами и последующего принятия третейским судом обязательного для сторон решения с применением современных способов передачи и хранения данных***.** Онлайн арбитраж является не примирительной процедурой, а полноценным способом независимого, беспристрастного и эффективного разрешения споров, возникающих из договорных и внедоговорных отношений, посредством использования электронных средств передачи и хранения информации.

Несмотря на все технические особенности, онлайн арбитраж остается процессом разрешения спора реальным человеком, а не машиной. Данное замечание обусловлено тем, что арбитражные процедуры, в которых решение формулируется в автоматическом режиме компьютерной программой, а не реальным человеком – арбитром, не могут признаваться арбитражем для целей исполнения итогового решения[1].

По оценкам специалистов, онлайн арбитраж обещает стать наиболее перспективным способом разрешения споров в киберпространстве по двум причинам. Во-первых, из-за недостаточной эффективности согласительных, неюрисдикционных механизмов урегулирования возникающих споров. Во-вторых, вследствие часто возникающей невозможности реально разрешить такой спор в суде из-за коллизии между территориальным характером юрисдикции судов и глобальным характером киберпространства[2].

Потребность в эффективном разрешении споров, возникающих между участниками отношений в киберпространстве, и вызывает

[1] *Rubino-Sammartano M.* International Arbitration Law and Practice. NY, 2014. P. 1728.

[2] *Kaufmann-Kohler G., Schultz T.* Online Dispute Resolution: Challenges for Contemporary Justice. Hague, 2004. P. 27.

к жизни онлайн арбитраж. Некоторые даже говорят о принципиально новом правовом явлении, таком как *Cybitration*.

Правовая природа онлайн арбитража

Онлайн-арбитраж является разновидностью классического арбитража, дополненной применением современных способов передачи и хранения данных для оптимизации процедуры рассмотрения спора арбитрами и принятия ими решения. Именно поэтому правовая природа онлайн арбитража производна от природы арбитража классического. При этом он не является тождественным традиционному арбитражному разбирательству, в ходе которого арбитры и стороны используют защищенные электронные системы коммуникации, такие, например, как *NetCase ICC*[1].

Существенным аспектом при анализе онлайн арбитража как правового явления становится его делокализация (денационализация). Онлайн арбитраж существует в киберпространстве. Специалисты справедливо отмечают, что в киберпространстве нет суверена и никакое государство не распространяет свой суверенитет на него. Поэтому обязывающее сторон разрешение споров в киберпространстве должно основываться на таких юрисдикционных парадигмах, как арбитраж. Арбитраж может стать наиболее эффективным методом разрешения споров в киберпространстве[2].

Делокализация позволяет строить теорию онлайн арбитража на фундаменте так называемой автономной доктрины, предложенной в 60-х гг. XX в. французским ученым Рюбеллин-Девиши. Именно онлайн арбитраж являет собой пример той самой «оригинальной системы, свободной от договорных и процессуальных элементов, позволяющей обеспечить необходимую быстроту рассмотрения дел и гарантии, на которые претендуют стороны».

Сторонники автономной теории, как известно, полагали, что юридическая природа арбитража может быть определена только с учетом его целей и реальной пользы, т.е. тех гарантий, которые необходимы сторонам, чтобы не обращаться в государственный суд. Цели онлайн

[1] Подробнее об этой системе: *Филипп М.* NetCase ICC // Legal Insight. 2014. № 8. С. 8 и далее.

[2] *Gibbons L.* Rusticum Judicium? Private “Courts” Enforcing Private Law and Public Rights: Regulating Virtual Arbitration in Cyberspace // Ohio-Northern Law Review. 1998. N 23. P. 793.

арбитража и его реальная польза – вот те условия, которые подвигают стороны к отказу от обращения как к традиционным судебным процедурам, так и к сложным альтернативным способам разрешения правовых конфликтов. Быстрое и экономичное разрешение спора без оглядки на формальные процедурные правила – цель применения онлайн арбитража.

Онлайн арбитраж – это яркий пример полной делокализации арбитража. Подобного рода разбирательство спора не предполагает физического проведения заседаний, заслушивания сторон, сам арбитраж может проходить вне какого-либо конкретного места. Не только на практике, но даже и в теории становится проблемным связать онлайн арбитраж с каким бы то ни было правопорядком, что требует выработки новых подходов к этой форме разрешения споров, и прежде всего к определению юридического места арбитража. Как известно, оно имеет принципиальное значение для выбора применимого права, оспаривания итогового арбитражного решения, его признания и приведения в исполнение, а также многих других аспектов арбитражного разбирательства.

Делокализация, однако, не всегда обеспечивает эффективность. При этом делокализация не ущемляет автономии воли сторон арбитража, а потому многими учеными сторонам рекомендуется самостоятельно согласовать место онлайн арбитража, либо включив соответствующее условие в арбитражное соглашение, либо сделав отсылку к применимым правилам арбитража. В отсутствие соглашения сторон юридическим местом онлайн арбитража предлагается считать место, где находится сервер, либо место, в котором находится арбитр в момент отправки и получения электронных сообщений.

Некоторые авторы говорят о том, что местом арбитража является место нахождения арбитражного института, применение правил которого согласовано сторонами, либо место, где зарегистрирован веб-сайт, в силу его важной роли как технического и содержательного посредника при разрешении спора[1].

Другие ученые вообще не усматривают причин менять общий подход к определению места арбитража только из-за того, что стороны решили провести разбирательство своего дела в режиме онлайн[2].

[1] *Jingzhou Tao* Arbitration Law and Practice in China. Hague, 2004. P. 188.

[2] *Solovay N., Reed C.* The Internet and Dispute Resolution: Untangling the Web. NY, 2003. P. 2–36.

Еще одна группа специалистов предлагает в отсутствие соглашения сторон о месте онлайн арбитража наделить арбитра правом определить это место и отразить соответствующее условие в арбитражном решении. Этот подход, на наш взгляд, в полной мере отвечает требованиям российского законодательства об арбитраже и может быть принят за основу.

Виды онлайн арбитража

Многие специалисты выделяют обязательный и необязательный онлайн арбитраж.

Так, И.М. Чупахин, опираясь на мнение проф. Шульца, подразделяет формы онлайн арбитража на два вида. Во-первых, обязательный арбитраж, решения которого приводятся в исполнение по правилам Нью-Йоркской конвенции 1958 г., и, во-вторых, необязательный, решения которого по общему правилу не подлежат принудительному исполнению, но в последующем, если стороны согласятся, его можно облечь в форму решения на согласованных условиях или в форму соглашения об урегулировании спора. Использование терминов «обязательный» и «необязательный», по оценке И.М. Чупахина, связано только с объемом участия органов государственной власти при исполнении арбитражного решения, таким образом, при обязательном арбитраже решение для сторон является окончательным и может быть приведено в исполнение в соответствии с положениями Нью-Йоркской конвенции 1958 г., при необязательном соответственно – без участия государственных органов[1].

Отметим, что такое толкование серьезно сужает сферу онлайн арбитража, поскольку Нью-Йоркская конвенция 1958 г. применяется только к иностранным арбитражным решениям. В целом изложенная позиция представляется дискуссионной, а различие между обязательной и необязательной формами онлайн арбитража кроется глубже.

Обязательный онлайн арбитраж – это юрисдикционная процедура, способ разрешения правового спора. Необязательный, или, как еще говорят, рекомендательный, онлайн арбитраж – это форма не разрешения, а урегулирование правового конфликта, разновидность примирительной процедуры.

[1] *Чупахин И.М.* Решение третейского суда: теоретические и прикладные проблемы. М., 2015. С. 18.

При внешнем и терминологическом сходстве содержание таких арбитражей существенно различается.

Обязательный онлайн арбитраж в полной мере должен отвечать требованиям *lex arbitri*, гарантировать соблюдение надлежащей юрисдикционной процедуры, несмотря на свое во многом виртуальное воплощение.

Необязательный онлайн арбитраж является менее формальным. Например, применяемые стандарты независимости и беспристрастности третьих лиц («арбитров»), равно как и процедурные требования, могут быть смягчены сторонами. Такой способ урегулирования конфликта не в полной мере может являться арбитражем в его классическом понимании. Необязательный онлайн арбитраж не исключает параллельного или последующего рассмотрения спора по существу судом *de novo*, соглашение о передаче дела в такой онлайн арбитраж не обладает дерогационным эффектом.

Таким образом, онлайн арбитраж (обязательный онлайн арбитраж) – это процедура разрешения спора арбитрами и последующего принятия третейским судом обязательного для сторон решения с применением современных способов передачи и хранения данных. «Необязательный онлайн арбитраж» – это процедура урегулирования спора нейтральными третьими лицами с использованием современных средств передачи и хранения данных, завершающаяся принятием итогового документа, имеющего для сторон рекомендательную силу.

Международный или внутренний онлайн арбитраж

Полная денационализация (делокализация) онлайн арбитража нередко становится основой для выводов о его исключительно международном характере. Многие ученые склонны рассматривать онлайн арбитраж как вненациональное явление, поскольку киберпространство физически распространяется на все государства.

Технические особенности, однако, не меняют характера возникающих отношений. Принято считать, что онлайн арбитраж между сторонами, действующими в одной стране, должен рассматриваться как внутренний арбитраж, в то время как если стороны действуют в различных юрисдикциях, арбитраж может считаться международным[1]. Совершенно очевидно, что признание онлайн арбитража как

[1] *Rubino-Sammartano M.* Op. cit. P. 1737.

арбитража внутренних споров или как международного коммерческого арбитража влечет применение разных правовых норм.

Серьезные практические последствия имеют и выводы о том, становится ли решение онлайн арбитража иностранным для целей применения Нью-Йоркской конвенции 1958 г.

На наш взгляд, выработанные в науке подходы к определению того, какое арбитражное решение не является «внутренним», могут и должны применяться при оценке решений онлайн арбитража. Напомним, что иностранными признаются арбитражные решения, вынесенные арбитрами на территории государства иного, нежели то государство, где испрашивается признание и приведение в исполнение таких решений, а также арбитражные решения, которые не считаются «внутренними» решениями в том государстве, где испрашивается их признание и приведение в исполнение. К числу последних в международной практике принято относить решения, вынесенные на территории государства, где испрашивается признание, но вынесение которых по соглашению сторон регулировалось правом другого государства[1], арбитражные решения, содержащие иностранный элемент, а также арбитражные решения, которые нельзя квалифицировать как вынесенные в каком-либо конкретном государстве. Решения онлайн арбитража, которые нельзя расценивать как вынесенные в каком-либо конкретном государстве, не будут считаться «внутренними» в том государстве, где испрашивается их признание и приведение в исполнение.

Принципы онлайн арбитража

По оценке Рабочей группы ЮНСИТРАЛ, принципы, которые лежат в основе любой процедуры урегулирования споров в режиме онлайн, включают справедливость, прозрачность, надлежащие правовые процедуры и подотчетность.

Прозрачность онлайн арбитража обеспечивается требованиями к его администратору. В международной практике крайне желательной признается публичность информации о любых отношениях между администратором онлайн арбитража и его сторонами (например, конкретным продавцом) с тем, чтобы пользователи услуг онлайн арбитража были информированы о потенциальном конфликте инте-

[1] *Berg van den A.J.* When Is an Arbitral Award Nondomestic Under the New York Convention of 1958? // Pace Law Review. 1985. N 6. P. 64.

ресов. В России на администратора онлайн арбитража в полной мере распространяются требования закона о недопустимости конфликта интересов в деятельности постоянно действующего арбитражного учреждения.

В рассматриваемой сфере конфликт интересов – это ситуация, в которой личная заинтересованность (прямая или косвенная) администратора влияет или может повлиять на надлежащее, объективное и беспристрастное исполнение им своих обязанностей по администрированию онлайн арбитража. Конфликт интересов презюмируется при администрировании онлайн арбитража, в котором в качестве стороны выступает некоммерческая организация, при которой действует администратор онлайн арбитража, либо ее учредитель (участник), либо лицо, фактически определяющее действия некоммерческой организации, при которой создано постоянно действующее арбитражное учреждение – администратор онлайн арбитража.

Самое серьезное внимание уделяется вопросам обеспечения независимости и беспристрастности лиц, которые вовлечены в урегулирование споров в режиме онлайн. Международными организациями администратору урегулирования споров в режиме онлайн настоятельно рекомендуется принять политику по вопросам выявления и урегулирования конфликта интересов. В связи с этим администратор онлайн арбитража может разработать для арбитров собственный свод этических норм как ориентир в том, что касается коллизий интересов и других правил поведения, либо использовать для этих целей документы, утвержденные иными уважаемыми организациями.

Так, например, в октябре 2014 г. Международной ассоциацией юристов было одобрено обновленное Руководство по конфликту интересов в международном арбитраже, в состав которого были включены общие стандарты, касающиеся беспристрастности, независимости и раскрытия фактов, а также указания к их практическому применению[1].

Еще одним принципом любой процедуры урегулирования споров в режиме онлайн является профессиональная компетентность. В силу специфики таких процедур администраторам настоятельно рекомендуется осуществлять комплексную политику, регулирующую не только отбор, но также и дополнительную подготовку нейтральных лиц. Цель подобной подготовки – обеспечивать наряду с механизмами

[1] IBA Guidelines on Conflicts of Interest in International Arbitration // IBA Publication. L., 2014.

внутреннего контроля качества соответствие решений нейтральных лиц стандартам, установленным администраторам процедуры урегулирования споров в режиме онлайн для себя.

Преимущества онлайн арбитража

Принято считать, что любая процедура урегулирования споров в режиме онлайн (в том числе и онлайн арбитраж) должна быть простой, оперативной и эффективной, с тем чтобы ее можно было применять «в условиях современной действительности». Урегулирование споров в режиме онлайн не должно порождать для сторон затрат, задержек и бремени, несоизмеримых с экономической выгодой от сделки. Именно поэтому одним из основных преимуществ онлайн арбитража является экономичность.

Арбитражное разбирательство онлайн (как и классический арбитраж) является конфиденциальным. Именно поэтому администраторам онлайн арбитража рекомендуется принимать надлежащие меры по обеспечению конфиденциальности.

Некоторые платформы онлайн арбитража в целях защиты персональных данных используют шифрование сообщений и документов, пересылаемых в рамках разбирательства. Такого рода защита не должна изменять содержание документов, используемых в качестве доказательств.

Будущие пользователи онлайн арбитража нередко интересуются опытом разрешения споров на той или иной платформе, поэтому в международной практике считается допустимой публикация администратором обезличенных сведений или статистических данных, касающихся разрешенных ранее дел. Соответствующая информация размещается на веб-сайте администратора в удобной и доступной для пользователя форме.

Правовые ограничения применения онлайн арбитража

В доктрине принято говорить о трех видах правовых препятствий, ограничивающих применение онлайн арбитража[1]. Эти ограничения связаны с арбитражным соглашением, процедурными аспектами, арбитражным решением и, наконец, арбитрабильностью споров, возни-

[1] См. подробнее: *Rubino-Sammartano M.* Op. cit. P. 1728–1734.

кающих из отношений электронной торговли. В ряде стран, например, в США, арбитрабильность таких споров исключена или ограничена. Массу вопросов у специалистов вызывает безопасность использования документов и авторизации сторон спора.

Первая группа правовых препятствий, ограничивающих распространение онлайн арбитража, касается арбитражного соглашения.

Классическое требование обязательной письменной формы арбитражного соглашения не всегда соблюдается в онлайн арбитраже. Как известно, Нью-Йоркская конвенция 1958 г. под письменным арбитражным соглашением понимает арбитражную оговорку в договоре или арбитражное соглашение, подписанное сторонами, или содержащееся в обмене письмами или телеграммами.

На первый взгляд арбитражное соглашение, заключенное путем обмена электронными сообщениями, не подпадает под действие ст. II Нью-Йоркской конвенции. Это обстоятельство стало бы серьезным препятствием на пути распространения онлайн арбитража. Однако международная практика развивается по другому пути и опирается на критерий письменной фиксации арбитражного соглашения. Как отмечается, все средства сообщения, которые соответствуют этому критерию, включая факсы и электронную почту, следует считать соответствующими п. 2 ст. II.

Что касается электронной почты, консервативный подход состоит в том, что требования Конвенции о письменной форме будут считаться соблюденными, если подписи заверены электронным способом или имевший место обмен сообщениями может быть засвидетельствован другими заслуживающими доверия способами[1]. В этих условиях особую значимость приобретает платформа онлайн арбитража, позволяющая фиксировать волю сторон на заключение соглашения о передаче дела в онлайн арбитраж.

В разных странах суды по-разному относятся к арбитражным соглашениям, заключаемым сторонами путем обмена электронными сообщениями.

Так, особую известность приобрело дело, рассмотренное норвежским апелляционным судом в августе 1999 г. Суд отказал в признании арбитражного решения на том основании, что обмен электронными письмами в подтверждение заключения арбитражного соглашения

[1] Руководство МСКА по толкованию Нью-Йоркской конвенции 1958 г.: пособие для судей. М., 2012. С. 43.

не отвечает требованиям Нью-Йоркской конвенции 1958 г., поскольку такие письма не были подписаны.

В США, напротив, Окружной суд в рассмотренном в 2000 г. деле *Realnet Works Inc. v. Privacy Litigation* признал, что арбитражное соглашение, заключенное в сети Интернет, отвечает требованиям письменной формы, закрепленным в Федеральном Арбитражном Акте. В некоторых странах обмен электронными сообщениями как форма заключения арбитражного соглашения приравнивается к обмену телеграммами.

Российский законодатель пошел еще дальше, сформировав либеральные условия для заключения арбитражных соглашений в электронной форме. Так, арбитражное соглашение считается заключенным в письменной форме в виде электронного сообщения, если содержащаяся в нем информация является доступной для последующего использования и если арбитражное соглашение заключено в соответствии с требованиями закона, предусмотренными для договора, заключаемого путем обмена документами посредством электронной связи (ч. 4 ст. 7 Закона РФ от 07.07.1993 № 5338-I «О международном коммерческом арбитраже» (в ред. от 29.12.2015))[1]. Требование о письменной форме арбитражного соглашения считается соблюденным, если арбитражное соглашение заключено путем обмена письмами, телеграммами, телексами, телефаксами и иными документами, включая электронные документы, передаваемые по каналам связи, позволяющим достоверно установить, что документ исходит от другой стороны (ч. 3 ст. 7 ФЗ от 29.12.2015 № 382-ФЗ «Об арбитраже (третейском разбирательстве) в Российской Федерации»)[2].

Вторая группа правовых препятствий, ограничивающих применение онлайн арбитража, связана с процедурными аспектами.

Основным среди них является место арбитража и сложности с его определением в онлайн арбитраже. Закономерным итогом нередко становятся проблемы с выбором права, применимого к процедуре и к существу спора.

Третья группа правовых препятствий для развития онлайн арбитража связана с итоговым решением.

В этом аспекте упоминается необходимость соблюдения письменной формы арбитражного решения, требований к изложению мотивов его вынесения, а также тот факт, не нарушает ли решение онлайн арбитража

[1] Российская газета. 1993. № 156. 14.08.

[2] Российская газета. 2015. № 297. 31.12.

публичный порядок в силу своей виртуальной нематериальной природы и может ли оно быть принудительно исполнено. Добавив к этому сложности с использованием электронных документов в качестве доказательств, становится очевидной оценка специалистов, что «наиболее часто используемой формой онлайн арбитража является так называемый необязательный арбитраж, то есть арбитраж, результатом которого становится решение, не являющееся эквивалентом судебному решению»[1], решение рекомендательное, но не обязательное для сторон. Причины тому – большая гибкость процедуры онлайн арбитража и отсутствие необходимости следовать строгим процессуальным требованиям.

Организация онлайн арбитража

Для любых механизмов урегулирования споров в режиме онлайн, в том числе и для онлайн арбитража, необходим посредник с технологической базой. В отличие от традиционных способов альтернативного разрешения правовых конфликтов урегулирование споров в режиме онлайн не может осуществляться *ad hoc*, на разовой основе без администратора, с участием только сторон в споре и нейтрального арбитра. Для использования технологии в целях содействия процессу разрешения спора процедура онлайн арбитража требует наличия системы для подготовки, отправления, получения, хранения, обмена или иной обработки сообщений. Такую систему принято называть «платформой онлайн арбитража». Очевидно, что необходимо управлять платформой онлайн арбитража и координировать ее работу. Субъект, который осуществляет такое управление и координацию, обычно именуется «администратором онлайн арбитража». Администратор онлайн арбитража может быть отдельным от платформы онлайн арбитража субъектом или являться ее частью. В России администратор онлайн арбитража должен отвечать требованиям к постоянно действующим арбитражным учреждениям, установленным гл. 9 ФЗ «Об арбитраже (третейском разбирательстве) в Российской Федерации».

Примером платформы онлайн арбитража может стать Система РАА – защищенная информационная система электронной подачи, обработки, хранения и передачи документов для разрешения споров по Регламенту онлайн арбитража РАА[2].

[1] *Kaufmann-Kohler G., Schultz T.* Online Dispute Resolution. P. 33.

[2] Регламент арбитража онлайн РАА доступен на сайте: www.arbitrations.ru

Для получения доступа к этой системе каждая сторона арбитражного разбирательства онлайн соглашается на взаимодействие с Арбитражной ассоциацией как с администратором онлайн арбитража, арбитром и другими сторонами спора с использованием глобальной компьютерной сети Интернет. Стороны спора осуществляют действия в Системе PAA исключительно через своих представителей, которые получают доступ к указанной системе посредством самостоятельной регистрации. В ходе такой регистрации создается ключ простой электронной подписи (логин и пароль), используемый впоследствии для идентификации в Системе PAA. Каждое лицо, совершающее действия в системе от имени стороны с использованием логина и пароля, персонифицируется в качестве лица, подписавшего электронный документ с помощью ключа простой электронной подписи (логина и пароля), и выступает в качестве представителя указанной стороны онлайн арбитража. Все действия, совершенные таким лицом в платформе онлайн арбитража, признаются действиями соответствующей стороны (разд. 1.2 Регламента арбитража онлайн PAA).

Передача документов через платформу онлайн арбитража производится участниками разбирательства или их представителями только после идентификации с помощью ключа электронной подписи. Идентификация участника онлайн арбитража в платформе является достаточным для всех целей доказательством передачи документов, сообщений, уведомлений этим участником арбитражного разбирательства онлайн.

Отметим, что коммуникация сторон онлайн арбитража, арбитров и администратора может осуществляться как с помощью электронной почты, так и путем заполнения специальных форм на сайте, либо в форме ответов онлайн, сделанных в реальном времени. Задача платформы онлайн арбитража – фиксировать такого рода коммуникации и обеспечивать доведение информации до лиц, участвующих в разбирательстве дела в режиме онлайн.

Процедура онлайн арбитража

К процедуре обязательного онлайн арбитража, место которого согласовано сторонами, применяются нормы законодательства по месту его проведения. Ключевым обстоятельством при конструировании процедуры онлайн арбитража становится необходимость соотнесения требований справедливой процедуры и высокой скорости разрешения

спора – одного из основных преимуществ такого арбитража. В международной практике принято исходить из того, что арбитры, проводящие арбитражное разбирательство онлайн, должны предоставить сторонам достаточно времени на изложение своей позиции и представление доказательств. Такая задача решается через использование удобных, ориентированных на пользователей способов представления доказательств.

Формирование состава онлайн арбитража осуществляется в порядке, определенном законом и соглашением сторон.

Как правило, арбитражное разбирательство онлайн проводится единоличным арбитром, назначаемым администратором. При назначении арбитров, отвечающих требованиям независимости и беспристрастности, учитывается их профессиональная компетентность. Для этого организации, оказывающие услуги онлайн арбитража, практикуют отбор и подготовку соответствующих нейтральных лиц.

Одновременно с уведомлением о назначении арбитра администратор направляет сторонам онлайн арбитража заполненное арбитром заявление о беспристрастности и независимости. Отвод арбитру может быть заявлен на любой стадии арбитражного разбирательства онлайн не позднее вынесения решения по причинам, вызывающим оправданные сомнения в независимости и беспристрастности арбитра.

Сторона, инициирующая арбитражное разбирательство онлайн, направляет исковое заявление с приложениями другой стороне путем размещения данных документов в электронном виде в платформе онлайн арбитража. Некоторые организации после получения просьбы об арбитраже предлагают сторонам услуги онлайн медиации или переговоров. После размещения искового заявления в платформе онлайн арбитража администратор направляет информацию об этом по электронным адресам, указанным в арбитражном соглашении.

Если исковое заявление подано в соответствии с установленными требованиями, администратор выносит постановление о возбуждении арбитражного разбирательства онлайн с указанием данных о назначенном администратором арбитре и уведомляет стороны об этом по адресам электронной почты, указанным в арбитражном соглашении. Это считается надлежащим и достаточным уведомлением сторон арбитражного разбирательства онлайн. Нередко администратор онлайн арбитража дополнительно направляет сторонам онлайн арбитража постановление о возбуждении арбитражного разбирательства заказным письмом с уведомлением о вручении.

Ответчик представляет отзыв на исковое заявление посредством размещения электронных документов в платформе онлайн арбитража. Непредставление отзыва ответчиком, надлежащим образом уведомленным об арбитражном разбирательстве онлайн, не препятствует проведению последнего.

В международной практике признается желательным, чтобы все сообщения в рамках процедуры онлайн арбитража передавались через платформу онлайн арбитража. Соответственно, стороны онлайн арбитража и сама платформа должны иметь специально указанный электронный адрес либо заполняемую электронную форму.

По оценке Рабочей группы ЮНСИТРАЛ, для повышения эффективности желательно, чтобы администратор урегулирования споров в режиме онлайн (в том числе и онлайн арбитража) оперативно подтверждал получение любых сообщений платформой урегулирования споров в режиме онлайн, уведомлял стороны о наличии любого сообщения, полученного такой платформой, а также информировал стороны о начале и завершении различных этапов процедуры. Само разбирательство дела обычно не происходит в режиме реального времени.

Особенности доказывания в онлайн арбитраже

Доказывание в онлайн арбитраже осуществляется по общим правилам, основанным на принципе состязательности. Если сторона, будучи должным образом уведомленной об онлайн арбитраже, не принимает в нем участия, то арбитр может продолжить разбирательство на основании представленных материалов. Если сторона, у которой арбитр запросил документы, вещественные или иные доказательства, не представляет их в установленный срок без уважительной причины, арбитр выносит арбитражное решение на основании имеющихся в его распоряжении доказательств. Арбитр также вправе сделать негативный вывод относительно позиции стороны, которая без уважительной причины не представила документы, которые имеются в ее распоряжении.

Природа онлайн арбитража определяет некоторые особенности доказательственной деятельности. По своей модели онлайн арбитраж тяготеет к так называемому *documents-only arbitration*, в ходе которого арбитрами исследуются только письменные доказательства.

Так, арбитражное разбирательство онлайн по регламенту РАА проводится только на основании документов в электронной форме, разме-

щенных в Системе РАА, которые презюмируются соответствующими оригиналам. Сторона онлайн арбитража вправе заявить о том, что документ, представленный другой стороной, не соответствует оригиналу, только после внесения дополнительного арбитражного сбора в размере 5% от общей суммы спора. Данный сбор предназначен для покрытия дополнительных расходов, связанных с проверкой такого заявления стороны онлайн арбитража, в том числе и выплатой дополнительного гонорара арбитру. После заявления стороны онлайн арбитража, что документ, представленный другой стороной, не соответствует оригиналу, арбитр принимает меры, направленные на проверку данного заявления, может потребовать у сторон онлайн арбитража представить оригиналы или должным образом заверенные копии таких документов. В случае, если в процессе арбитражного разбирательства заявление стороны о несоответствии копии документа оригиналу не подтвердится, на такую сторону возлагаются все арбитражные расходы по делу, вне зависимости от исхода разбирательства. Подобные правила стимулируют стороны к участию в доказывании в формах, позволяющих обеспечить эффективное рассмотрение дела в режиме онлайн.

Очевидным представляется значение процедуры раскрытия доказательств в электронной форме (так называемая процедура *e-discovery*) для онлайн арбитража. В некоторых странах она получила закрепление на законодательном уровне.

Так, в США соответствующие поправки в Федеральные правила гражданского судопроизводства были приняты еще в 2006 г. Многие арбитражные центры также утвердили соответствующие правила (например, в 2009 г. правила раскрытия доказательств в электронной форме были приняты Королевским Институтом Арбитров).

Разбирательство

Как правило, арбитражное разбирательство онлайн проводится без слушаний, на основании документов, представленных сторонами. В течение всего срока разбирательства стороны имеют право представлять дополнительные пояснения и документы. При необходимости арбитр может принять решение о проведении слушания с помощью средств видеоконференции или телеконференции. Нередко арбитр ведет аудио или видеозапись слушаний. В исключительных случаях проводятся слушания с непосредственным присутствием сторон онлайн арбитража.

Арбитр обязан уведомить стороны об окончании онлайн арбитража путем вынесения постановления о завершении разбирательства. После размещения постановления о завершении разбирательства дополнительные документы от сторон онлайн арбитража не принимаются, а арбитр приступает к вынесению арбитражного решения.

В любой момент разбирательства стороны онлайн арбитража вправе заключить мировое соглашение. В онлайн арбитраже PAA стороны могут прибегнуть к процедуре автоматизированных переговоров в Системе PAA. В случае если по результатам таких переговоров стороны достигнут согласия об урегулировании спора, арбитр выносит постановление о прекращении разбирательства или, если стороны его об этом попросят, об утверждении мирового соглашения в виде арбитражного решения на согласованных условиях (разд. 4.5 Регламента арбитража онлайн PAA). Автоматизированными являются обеспеченные информационно-коммуникационными технологиями переговоры, в ходе которых стороны общаются друг с другом через платформу урегулирования споров в режиме онлайн.

Решение онлайн арбитража

По результатам арбитражного разбирательства онлайн арбитр выносит мотивированное арбитражное решение. Решение онлайн арбитража может быть подписано и утверждено электронной подписью. Арбитражное решение направляется сторонам как правило администратором онлайн арбитража в виде электронной копии посредством размещения в платформе онлайн арбитража. Кроме того, либо сам арбитр, либо администратор направляет сторонам арбитражного разбирательства онлайн также и оригинал арбитражного решения, подписанный арбитром.

Неоднократно в самых разных юрисдикциях возникал вопрос о соответствии решений онлайн арбитража требованиям национального публичного порядка. Поводом для сомнений становились виртуальная природа разбирательства онлайн, невозможность определить место арбитража, а также практика вынесения решений без указания мотивов.

На наш взгляд, решение онлайн арбитража, вынесенное с соблюдением требований справедливой процедуры, соответствует национальному публичному порядку при условии, что оно было принято человеком, но не машиной. Сформированные автоматизированной системой без участия человека решения не отвечают общим началам

гражданской юрисдикции, основанной на мыслительной деятельности разумного существа. Такого рода «арбитражные» решения могут рассматриваться только как рекомендательные. В настоящее время в доктрине продолжаются исследования соответствия решений онлайн арбитража требованиям международного публичного порядка, ставится вопрос о регулировании разбирательства споров в режиме онлайн нормами так называемого киберправа (*Cyberlaw*) или *lex informatica* (по аналогии с *lex mercatoria*).

В завершение отметим, что объем трансграничных коммерческих сделок, совершаемых в электронной форме, растет из года в год. Стороны таких отношений, зарождающихся в киберпространстве, объективно нуждаются в разрешении возникающих между ними споров – быстром, эффективном и экономичном. Ответом на потребность в особом юрисдикционном механизме стал онлайн арбитраж. В ходе реформы арбитража российский законодатель сделал серьезные шаги на пути развития его онлайн версии, которые, на наш взгляд, могут стать основой для дальнейшего развития онлайн арбитража.

Пристатейный библиографический список:

1. *Berg van den A.J.* When Is an Arbitral Award Nondomestic Under the New York Convention of 1958? // Pace Law Review. 1985. N 6.

2. *Gibbons L.* Rusticum Judicium? Private «Courts» Enforcing Private Law and Public Rights: Regulating Virtual Arbitration in Cyberspace // Ohio-Northern Law Review. 1998. N 23.

3. IBA Guidelines on Conflicts of Interest in International Arbitration // IBA Publication. L., 2014.

4. *Jingzhou Tao* Arbitration Law and Practice in China. Hague, 2004.

5. *Kaufmann-Kohler G., Schultz T.* Online Dispute Resolution: Challenges for Contemporary Justice. Hague, 2004.

6. *Rubino-Sammartano M.* International Arbitration Law and Practice. NY, 2014. P. 1728.

7. *Solovay N., Reed C.* The Internet and Dispute Resolution: Untangling the Web. NY, 2003.

8. Руководство МСКА по толкованию Нью-Йоркской конвенции 1958 г.: пособие для судей. М., 2012.

9. Урегулирование споров в режиме онлайн применительно к трансграничным электронным коммерческим сделкам. Проект итогового

документа, отражающего элементы и принципы процедуры УСО. Рабочая группа III. Тридцать третья сессия. Нью-Йорк, 29 февраля – 4 марта 2016 года (сайте www.uncitral.org).

10. *Филипп М.* NetCase ICC // Legal Insight. 2014. № 8.

11. *Чупахин И.М.* Решение третейского суда: теоретические и прикладные проблемы. М., 2015.

Н. Руйе

СПОРЫ О ДОМЕННЫХ ИМЕНАХ: ВЫБОР МЕЖДУ ЧАСТНЫМИ ПРОЦЕДУРАМИ (UDRP И ПРОЧИМИ) И РАЗБИРАТЕЛЬСТВОМ В ГОСУДАРСТВЕННОМ СУДЕ

Аннотация. *Автор анализирует процедуры разбирательств в сфере доменных имен, которые создавались и имплементировались частными организациями в течение более 15 лет, и уделяет особе внимание их координации с процедурами по тому же предмету спора в государственных судах. В статье описываются и анализируются различные роли и соответствующая эффективность этих процеду.*

Ключевые слова: *доменное имя, частная процедура рассмотрения спора, UDRP, SWITCH, досудебное рассмотрение спора*

Доменные имена являются важным объектом, выполняющим функцию идентификации информационных ресурсов в сети Интернет. На настоящий момент в различных национальных юрисдикциях было рассмотрено огромное количество споров, связанных с регистрацией и использованием доменных имен[1].

Споры о доменных именах являются очень интересной темой, требующей глубокого погружения и позволяющей поразмышлять о фундаментальных вопросах структуры судебных разбирательств и их будущего.

Несмотря на то что в настоящий момент пользователи Интернета все реже используют доменные имена, чтобы найти необходимый веб-сайт в Интернете, предпочитая осуществлять поиск по ключевым словам через поисковую строку, например, в *Google*, *Bing* или *Yandex*, проблематика споров о доменных именах продолжает существовать. Этот факт подтверждается статистикой.

Большое количество споров о доменных именах было рассмотрено в рамках частной процедуры, которая регламентируется Единой политикой рассмотрения споров о доменных именах (англ. *Uniform*

[1] *Королев Д., Наумов В.* Процессуальный статус UDRP в России: возможности и парадоксы // Патенты и лицензии. М., 2003. № 4. С. 2–8.

Domain Name Dispute Resolution Policy; далее – *UDRP*). *UDRP* была принята 26.08.1999 Корпорацией Интернета по присвоению имен и номеров (англ. *Internet Corporation for Assigned Names and Number*; далее – *ICANN*), тогда американской некоммерческой организацией, на основе рекомендаций, внесенных Всемирной организацией интеллектуальной собственности (далее – ВОИС) в ходе Первого процесса по доменным именам в Интернете с целью реализации механизмов досудебного урегулирования споров, связанных с нарушением прав третьих лиц при регистрации и недобросовестном использовании доменных имен.

Применение *UDRP* ограничивается спорами о доменных именах общего назначения (*gTLD*) – таких, как *.biz*, *.com*, *.info*, *.net* и *.org*[1]. Частная процедура по *UDRP* проводится в четырех организациях, из которых самыми известными являются: Центр ВОИС по арбитражу и посредничеству (далее – Центр ВОИС), Северо-американский Национальный арбитражный форум (англ. *National Arbitration Forum*; далее – Американский форум) и Азиатский Центр. Центр ВОИС с момента начала деятельности по разрешению доменных споров в 1999 г. рассмотрел более 30 тыс. споров[2], что составляет около 3 тыс. споров в год[3]; Американский форум – около 20 тыс. споров, т.е. примерно 2 тыс. споров в год[4].

Согласно статистике Центра ВОИС, пятью «ведущими» сферами деятельности истцов являлись биотехнология и фармацевтика, банковское дело и финансы, Интернет и ИТ, розничная торговля, продукты питания, напитки и общественное питание. За период до конца 2014 г. сторонами споров о доменных именах, рассматриваемых в Центре ВОИС, были представители 177 стран[5].

Таким образом, очевидно, что частная процедура рассмотрения споров, связанных с доменными именами, востребована и активно используется различными компаниями.

---

[1] Сорок седьмая (22-я очередная) сессия Генеральной Ассамблеи ВОИС, Женева, 5–14 октября 2015 г., Информация о деятельности Центра ВОИС по Арбитражу и посредничеству

[2] По состоянию на 2017 г. рассмотрено 36 874 споров (http://www.wipo.int/amc/en/domains/statistics/cases.jsp).

[3] В 2015 г. было рассмотрено 2754 споров, в 2016 – 3036 споров.

[4] *Fast Facts: Domain Name Dispute Resolution, National Arbitration Forum*.

[5] Сорок седьмая (22-я очередная) сессия Генеральной Ассамблеи ВОИС, Женева, 5–14 октября 2015 г.

Отсюда возникает проблема соотношения частных процедур рассмотрения доменного спора и судебным разбирательством в государственном суде и выбора наиболее оптимального института рассмотрения этого спора. При этом возникает целый ряд вопросов: что может сделать сторона, проигравшая дело в частной процедуре; должна ли проигравшая сторона инициировать судебное разбирательство в государственном суде и есть ли у нее шанс выиграть?

Эти вопросы могут быть рассмотрены на примере практики рассмотрения споров о доменных именах в Швейцарии.

В Швейцарии существует две разновидности частных процедур для рассмотрения доменных споров: во-первых, это процедура по правилам *UDRP*, которая применяется в случае, когда швейцарские компании используют доменные имена, заканчивающиеся на *.com*, *.net*, *.org*, *.info* и т.д., и, во-вторых, иная процедура – для случаев, когда домен заканчивается на *.ch*.

В Швейцарии регистрацией доменных имен, заканчивающихся на *.ch*, занимается *SWITCH foundation*[1]. В ст. 24 Правил процедуры рассмотрения споров *SWITCH foundation*[2] закреплено: «(c) эксперт удовлетворяет требование в случае, если регистрация или использование доменного имени *представляет собой явное нарушение прав на различительный знак*, принадлежащий заявителю в соответствии с правом Швейцарии или Лихтенштейна.

(d) в частности, явное нарушение прав интеллектуальной собственности однозначно имеет место *при наличии следующих элементов*:

– как существование, так и нарушение прав на указанный различительный знак, исходя из формулировок текста закона или признанного толкования закона и представленных фактов; право и нарушение подтверждаются представленными доказательствами;

– ответчик не представил убедительным образом и не доказал необходимость предоставления ему защиты;

– нарушение прав в соответствии с формулировкой судебного иска обосновывает передачу или прекращение доменного имени».

Таким образом, если спор связан с доменным именем, заканчивающимся на *.ch* для предъявления требования, необходимо, чтобы нарушение *было явным и фактически, и юридически*, т.е. факты, на ос-

[1] https://www.switch.ch/about/id/

[2] https://www.nic.ch/terms/disputes/rules_v1/#para24

новании которых заявитель строит свою правовую позицию, должны иметь надлежащее подтверждение.

В *UDRP* критерии для участия в процедуре закреплены в п. 4 (*a*). Согласно положениям этого пункта истец обязан доказать, что:

– доменное имя ответчика идентично или сходно до степени смешения с товарным знаком или знаком обслуживания, правообладателем которого является заявитель;

– у ответчика нет прав или законных интересов в отношении зарегистрированного доменного имени;

– доменное имя было зарегистрировано и используется ответчиком недобросовестно.

В п. 4 (*b*) *UDRP* содержится неисчерпывающий перечень признаков, которые позволяют говорить о том, что доменное имя зарегистрировано и используется ответчиком недобросовестно, например, в случае предложения доменного имени к продаже правообладателю (заявителю). В п. 4 (*c*) *UDRP* закреплен неисчерпывающий перечень признаков, по которым можно судить о наличии у ответчика законных прав и интересов в отношении доменного имени, например, в ситуации, когда он использует доменное имя в некоммерческих целях и не вводит пользователей в заблуждение относительно средств индивидуализации заявителя.

Так, решением административной группы Центра ВОИС в отношении доменных имен *vulcan-bit.biz*, *vulcan-bit.com*, *vulcan-bit.info*, *vulcan-bit.net* и *vulcan-bit.org*, требование заявителя об их передаче было удовлетворено, поскольку заявитель представил необходимые доказательства отсутствия у ответчика прав и законных интересов в спорных доменных именах. Было установлено, что ответчик зарегистрировал спорные доменные имена с целью последующего недобросовестного онлайн-бизнеса для получения прибыли путем использования репутации и популярности бизнеса заявителя, Таким образом, действия ответчика были недобросовестными, и заявитель доказал, что регистрация и использование спорных доменных имен были произведены ответчиком недобросовестно[1].

В другом решении Административной группы Центра ВОИС в отношении доменного имени *denso.com* требование заявителя о его передаче также было удовлетворено. Заявитель по данному делу доказал, что у ответчика нет прав и законных интересов в спорном доменном

[1] Решение Административной группы Центра ВОИС по делу No D2003-0482.

имени, что ответчик зарегистрировал и использовал доменное имя недобросовестно. Этот вывод был основан на том, что длительное время ответчик «держал» доменное имя, практически ничего не предпринимая для его использования[1].

Сказанное позволяет заключить, что названные признаки недобросовестности и добросовестности типичны для англосаксонского законодательства в том смысле, что они слишком общие, и соответственно их довольно легко обходить. Но, с другой стороны, перечни таких признаков не закрыты, а перечисленные в них случаи являются лишь примерами.

Таким образом, вышеуказанные критерии, разработанные для обеих частных процедур, недостаточны для вынесения окончательного судебного решения в обычных судебных разбирательствах.

Частная процедура по правилам *UDRP* применяется в отношениях между регистратором и его клиентом (регистрантом – лицом, на которое зарегистрировано доменное имя) с целью внесудебного урегулирования доменных споров. Следовательно, требования обязательной процедуры, установленные *UDRP*, не препятствуют заявителю передать доменный спор на рассмотрение компетентного государственного суда для вынесения судебного решения как до возбуждения этой процедуры, так и после ее завершения (п. 4 (*к*) *UDRP*). Следовательно, независимо от решения административной группы (комиссии) по доменному спору любая сторона может обратиться в государственный суд с соответствующим требованием.

Согласно положениям п. 4 (*к*) *UDRP*, если административная комиссия примет решение об аннулировании регистрации доменного имени или о передаче доменного имени, оно может быть приведено в исполнение через 10 рабочих дней после получения уведомления о таком решении. Если в течение этих 10 рабочих дней ответчик не представит официального документа, свидетельствующего о возбуждении судебного разбирательства по данному делу в государственном суде, решение будет исполнено.

В Швейцарии в ст. 10 Правил процедуры рассмотрения споров *SWITCH foundation* закреплены схожие правила: во-первых, в соответствии с п. (*a*) «настоящие Правила *не препятствуют сторонам передать спор на рассмотрение компетентного суда в целях получения независимого решения*» и, во-вторых, в силу п. (*c*) «если судебное разби-

[1] Решение Административной группы Центра ВОИС по делу No D2016-1635.

рательство возбуждено до или во время процедуры (альтернативного) урегулирования споров, орган урегулирования споров или в период его назначения посредник или эксперт принимает решение о приостановлении, прекращении или продолжении процедуры (альтернативного) урегулирования споров».

Статьей 26 Правил процедуры рассмотрения споров *SWITCH foundation* установлены следующие правила, касающиеся исполнения решений: « (a)...решение об аннулировании или передаче доменного имени, являющегося объектом спора, исполняется регистратором по истечении срока в 20 дней...

(b) если ответчик передает регистратору в этот 20-дневный срок... официальный документ, подтверждающий возбуждение судебного разбирательства... регистратор не исполняет решение до момента получения документа, который он считает достаточным доказательством отправления на новое рассмотрение, отклонения или возвращение без рассмотрения судебного иска.

(c) до момента исполнения решения или до окончательного прекращения судебного разбирательства в соответствии с пунктом (b) доменное имя остается заблокированным».

В связи со сказанным возникает вопрос, каковы будут шансы на то, что решение государственного суда окажется другим.

Как видно из изложенных положений Правил процедуры рассмотрения споров *SWITCH foundation*, для того, чтобы комиссия приняла решение о передаче доменного имени, необходимо, чтобы заявитель представил очевидные доказательства обоснованности своих требований: факты должны быть подтверждены доказательствами, а предъявляемое требование четко аргументировано с опорой на нормы материального права. Аналогичная ситуация наблюдается и применительно к *UDRP*: решение о передаче доменного имени будет принято только тогда, когда ситуация будет предельно ясной, поскольку такое решение может быть принято лишь при отсутствии у ответчика любых законных интересов в отношении доменного имени.

С учетом этого сложно будет убедить государственный суд, что у ответчика больше прав на доменное имя, нежели у заявителя, когда комиссия приняла решение о передаче прав на доменное имя заявителю, признав, что у ответчика нет законного интереса в данном доменном имени. Представляется, что ответчик сможет убедить государственный суд только в том случае, если докажет, что он вообще не мог участвовать в частной процедуре рассмотрения доменного спора.

Изучение практики швейцарских судов показало, что подобных случаев не было – решение комиссии о передаче доменного имени заявителю почти всегда является действительно окончательным и впоследствии подтверждается государственным судом.

Статистика Центра ВОИС показывает, что решение о передаче доменного имени было принято в более чем 20 тыс. споров.

Но в тех случаях, когда в передаче доменного имени заявителю был отказано, есть реальный шанс выиграть дело в государственном суде. В практике швейцарских судов такие случаи были.

Например, ассоциация, осуществляющая рекламу горнолыжного курорта Сан-Мориц, два раза пыталась получить решение о передаче ей домена *stmoritz.com*, а комиссия отказывалась удовлетворять ее требование о передаче домена. Однако в 2009 г. государственный суд вынес решение о передаче этого домена ассоциации, обосновав свое решение тем, что ответчик (пользователь) мало использовал сайт для компаний, расположенных в Сан-Морице.

Другой интересный случай. Школа в кантоне Цуг – «Институт Монтана» зарегистрировала и использовала несколько лет домен *montana.ch*. Однако коммуна Монтана, когда решила создать свой веб-сайт в Интернете и обнаружила существование веб-сайта *montana.ch*, потребовала его передачи. Несмотря на то что комиссия явно отказала бы в передаче доменного имени ввиду добросовестного и законного использования, Верховный суд принял решение в пользу коммуны из-за риска смешения и того факта, что школа могла бы использовать другой домен, например, *institut-montana.ch*.

Еще в одном случае комиссия отказала в передаче домена заявителю, когда посредник (брокер) в страховой области использовал домен *axa-assurance.ch*. Эксперт Центра ВОИС установил, что ситуация не является очевидной, поскольку этот посредник действительно продает страховые продукты компании *AXA*, и отказал в передаче домена. Однако суд кантона Цюриха, установив при рассмотрении данного дела, что этот брокер предлагал страховые продукты не только *AXA*, но и продукты других страховых компаний, пришел к выводу о том, что компания *AXA* вправе запретить брокеру использование этого домена.

Вышеизложенное демонстрирует, что случаев, когда заявитель проигрывает при рассмотрении дела в рамках частной процедуры рассмотрения доменных споров, а затем выигрывает дело в государственном суде, в Швейцарии немного.

На практике, если ситуация достаточно сложная, заявитель в большинстве случаев обращается сразу в государственный суд. Поэтому многие практикующие юристы в Швейцарии, точно зная, какие критерии используются в *UDRP* и аналогичных частных процедурах, уже изначально решают, когда следует обращаться именно в государственный суд, а когда – использовать частную процедуру рассмотрения доменных споров.

Исходя из критического анализа практики споров о доменных именах можно заключить, что процедуры по правилам *UDRP* и аналогичные им частные процедуры имеют множество достоинств. Одними из них являются оперативность рассмотрения дел (несколько месяцев) и оперативность исполнения решений (домен передается по истечении 10-дневного срока со дня вынесения решения) – это позволяет характеризовать процедуры как «упрощенные мини-процессы». Как было указано выше, Центр ВОИС освободил государственные суды от более чем 20 000 судебных процессов, что экономит ресурсы аппаратов юстиции и помогает правообладателю. При этом стороны сохраняют право обратиться непосредственно в государственный суд, например, в более сложных и нестандартных ситуациях.

Резюмируя, следует сказать, что с точки зрения юридической системы рассматриваемые частные процедуры являются возможной моделью для развития действующих альтернативных механизмов внесудебного урегулирования споров.

Пристатейный библиографический список:

Королев Д., Наумов В. Процессуальный статус UDRP в России: возможности и парадоксы // Патенты и лицензии. М., 2003. № 4.

КОРОТКО ОБ АВТОРАХ

АЛИ Максим Зафарович

Родился 10 сентября 1990 г. в г. Шебекино Белгородской обл.

В 2012 г. с отличием окончил юридический факультет Санкт-Петербургского Гуманитарного университета профсоюзов.

В 2010–2011 гг. – юрисконсульт в Санкт-Петербургском Гуманитарном университете профсоюзов.

В 2012 г. присоединился к команде «Качкин и Партнеры» в должности помощника юриста, в 2014–2017 гг. – работал в должности юриста.

С 2017 г. – старший юрист юридической фирмы «Максима Лигал».

Сфера специализации включает консультирование по вопросам регулирования интеллектуальной собственности/информационных технологий.

Автор многочисленных публикаций в профессиональных юридических и деловых изданиях, сборниках материалов конференций. Активный участник международных, общероссийских и региональных научно-практических и деловых конференций, посвященных, в частности, вопросам интеллектуальной собственности, *IT*-сектору и электронной коммерции.

E-mail: maksim.ali@kachkin.ru

АФАНАСЬЕВ Дмитрий Викторович

Родился 2 августа 1974 г. в г. Москве.

Окончил магистратуру МГИМО (У) МИД России, получив степень магистра юриспруденции по программе международного права и права Европейского союза, а также Российскую школу частного права при Президенте РФ, получив степень магистра частного права.

В 2006–2009 гг. работал в Администрации Президента РФ в Государственно-правовом управлении Президента РФ. В 2009–2013 гг. являлся советником Управления частного права Высшего Арбитражного Суда РФ. В 2013–2015 гг. работал начальником отдела анализа и обобщения судебной практики, законодательства и статистики Суда по интеллектуальным правам.

С 2015 г. – руководитель-координатор Экспертного совета Комитета Государственной Думы по информационной политике, информационным технологиям и связи.

Автор монографий «Подача жалобы в Европейский Суд по правам человека» (2012 г.), Международные договоры в сфере интеллектуальной собственности (актуальный обзор многосторонних соглашений) (2017 г.; в соавторстве); «Защита деловой репутации в случаях ее диффамации или неправомерного использования (в сфере коммерческих отношений)» (2015 г.; в соавторстве); «Порядок рассмотрения жалоб в Европейском Суде по правам человека» (2013 г.; в соавторстве), а также ряда статей в сборниках научно-практических статей и ведущих юридических журналах.

E-mail: d@ipclub.in, da@ipclub.in

БЕЛОВ Вадим Анатольевич

Доктор юридических наук (2004), доцент (1998–2007), профессор кафедры гражданского (2007–2011), коммерческого права и основ правоведения юридического факультета МГУ им. М.В. Ломоносова (с 2011); арбитр Лондонского международного коммерческого арбитража (LCIA) (с 2014).

Родился 5 августа 1971 г. в г. Кирове Калужской области.

В 1993 г. окончил с отличием юридический факультет МГУ им. М.В. Ломоносова. В 1996 г. защитил кандидатскую диссертацию на тему «Ценные бумаги как объекты гражданских прав: Вопросы теории» (научный руководитель – д. ю. н., профессор С.М. Корнеев). Победитель конкурса молодых ученых МГУ (1998), конкурсов «Традиции и развитие» МГУ в номинации «Творческий успех» (2004) и «Педагогический успех» (2011). Лауреат Национальной премии Объединения корпоративных юристов России в номинации «Публикация года» (2011). Докторская диссертация – «Проблемы цивилистической теории российского вексельного права».

Сфера научных интересов – теоретические вопросы коммерческого (торгового) права, международное и иностранное торговое право, правовое регулирование купли-продажи, акты *NLM*, ценные бумаги, вексельное право, обязательственное право, теория правоотношений.

Автор 90 книг и более 400 статей по различным проблемам гражданского и коммерческого (торгового) права общим объемом около 3000 п.л.

БЕМБЕЕВА Баира Саныловна

Родилась 3 сентября 1997 г. в г. Элисте Республики Калмыкия.

В настоящее время является студенткой 4-го курса бакалавриата факультета права Национального исследовательского университета «Высшая школа экономики».

В 2016 г. в составе сборной команды университета заняла 2-е место в Конкурсе им. Ф.Ф. Мартенса по международному гуманитарному праву. С 2017 г. состоит в составе сборной команды университета Модели Европейского Суда по правам человека.

Сфера профессиональных интересов: права человека, международное публичное право, конституционное право, избирательное право.

E-mail: bsbembeeva@mail.ru

БОГУСТОВ Андрей Алексеевич

Родился 20 апреля 1973 г. в Латвии.

В 1996 г. окончил юридический факультет Гродненского государственного университета им. Янки Купалы (г. Гродно, Республика Беларусь). В 2012 г. в Институте законодательства и сравнительного правоведения при Правительстве РФ защитил кандидатскую диссертацию на тему «Ценные бумаги как объекты прав в гражданском праве стран – участников СНГ (сравнительно-правовой анализ)».

В настоящее время – доцент кафедры международного права Гродненского государственного университета им. Янки Купалы.

Сфера научных интересов: сравнительное правоведение в сфере частного права стран СНГ и Восточной Европы, право ценных бумаг, право интеллектуальной собственности.

Автор около 150 научных публикаций, в том числе одной монографии, четырех учебных пособий и 30 статей в ведущих научных журналах России, Беларуси и Украины.

E-mail: bogustow@mail.ru

ДЕЙНЕКО Алексей Геннадьевич

Родился 10 марта 1988 г. в г. Москве.

В 2009 г. с отличием окончил факультет философии и права Государственной классической академии им. Маймонида. В 2012 г. защитил в Российской государственной академии интеллектуальной собственности кандидатскую диссертацию на тему «Гражданско-правовое регулирование доведения произведений до всеобщего сведения

с использованием информационно-телекоммуникационных сетей в Российской Федерации».

С 2009 г. ведет курсы лекций по дисциплинам «Конституционное право», «Авторское право», «Патентное право», «Правовые информационные системы».

С 2011 г. состоит на государственной гражданской службе в Администрации Президента Российской Федерации. Имеет классный чин Государственного советника Российской Федерации 3 класса.

Сфера научных интересов: конституционное право России и зарубежных стран, авторское право, право интеллектуальной собственности, авторские права в киберпространстве, информационное право, правовые проблемы общественного контроля, межотраслевые и междисциплинарные исследования.

Автор более 20 публикаций по вопросам конституционного права и права интеллектуальной собственности, в том числе одной монографии и двух учебных пособий.

E-mail: alexey-deyneko@mail.ru

ГАВРИЛОВ Евгений Владимирович

Родился 18 июля 1987 г. в г. Красноярске.

В 2009 г. с отличием окончил Юридический институт КрасГАУ. Прошел дополнительное обучение в магистратуре Юридического института Сибирского федерального университета (магистерская программа «*Цивилист: iustitia et ius*»), получив степень магистра юриспруденции.

С 2010 г. находится на государственной гражданской службе Красноярского края, с 2013 г. – в юридическом отделе экспертно-правового управления Законодательного собрания Красноярского края.

Сфера научных интересов: нематериальные блага и личные неимущественные права, защита деловой репутации, компенсация нематериального вреда юридическим лицам, способы защиты гражданских прав, правовой статус коренных малочисленных народов Севера, Сибири и Дальнего Востока Российской Федерации, правовые проблемы в сфере образования.

Автор более 300 юридических публикаций в научных журналах, газетах, сборниках материалов конференций, изданных в России, Республике Беларусь, Украине, Казахстане, Армении.

E-mail: gavrilov@zakon.ru

ГЛОНИНА Вера Николаевна

Родилась 18 марта 1997 г. в г. Москве.

В 2014 г. поступила на юридический факультет МГУ им. М.В. Ломоносова. В настоящее время – студентка 3-го курса (профиль: гражданско-правовой), стажер в юридической фирме «Городисский и партнеры».

Сфера профессиональных интересов: право интеллектуальной собственности, конкурентное право, гражданское право, сравнительное правоведение в сфере частного права.

Автор ряда статей по вопросам права интеллектуальной собственности и конкурентного права, опубликованных в журналах и сборниках («Интеллектуальная собственность. Авторское право и смежные права», «Конкуренция и право», «Журнал суда по интеллектуальным правам»).

E-mail: glonina.vera@yandex.ru

ЕМАНОВА Наталья Сергеевна

Родилась 15 марта 1990 г. в г. Барнауле Алтайского края.

В июне 2012 г. закончила юридический факультет Алтайской академии экономики и права. С сентября 2012 г. является аспирантом юридического института ФГАОУ ВО «Южно-Уральского государственного университета (НИУ)».

Сфера профессиональных интересов: электронная торговля, интернет-право.

Автор более 19 статей по электронной торговле, среди которых: «Порядок заключения электронного договора розничной купли-продажи» (Юрист. 2015. № 3), «Момент заключения электронного договора розничной купли-продажи» (Юрист. 2016. № 24).

E-mail: natashaemanova@mail.ru

КОЗЛОВА Марина Юрьевна

Родилась 6 мая 1972 г. в Волгограде.

В 1994 г. с отличием окончила Волгоградский государственный университет по специальности «юриспруденция». В 2002 г. защитила кандидатскую диссертацию, посвященную исследованию антимонопольных ограничений принципа свободы договора.

Кандидат юридических наук, доцент.

В настоящее время является ведущим научным сотрудником Института права Волгоградского государственного университета.

Ею опубликовано более 80 работ, в том числе монографий, учебно-методических пособий, статей в журналах, рекомендуемых ВАК РФ, а также индексируемых в базе данных *Scopus*.

E-mail: kozlova@volsu.ru

КУРОЧКИН Сергей Анатольевич

Родился 2 ноября 1979 г. в г. Свердловске.

В 2001 г. окончил Уральскую государственную юридическую академию.

С 2003 г. – преподаватель, старший преподаватель, доцент кафедры гражданского процесса Уральской государственной юридической академии (университета).

Кандидат юридических наук, доцент.

Автор ряда публикаций, посвященных третейскому разбирательству, международному коммерческому арбитражу, а также широкому спектру вопросов, связанных с гражданским и арбитражным процессом. Среди них монографии и учебные пособия: «Третейское разбирательство гражданских дел в Российской Федерации: теория и практика» (2007), «Государственные суды в третейском разбирательстве и международном коммерческом арбитраже» (2008), «Частные и публичные начала в цивилистическом процессе» (2012), «Международный коммерческий арбитраж и третейское разбирательство» (2013) и др.

ЛАРИОНОВА Валерия Андреевна

Родилась 1 июня 1995 г. в г. Братске.

В 2017 г. закончила факультет права Национального исследовательского университета «Высшая Школа Экономики». В настоящий момент является студенткой 1-го курса магистратуры программы «Право информационных технологий и интеллектуальной собственности» факультета права Национального исследовательского университета «Высшая Школа Экономики».

С 2016 г. работает референтом по правовым вопросам компании Dentons (Москва, Россия), где занимается вопросами интеллектуальной собственности.

Автор ряда опубликованных научных статей.

E-mail: valarionova@edu.hse.ru

НАМ Кирилл Вадимович

Родился 29 июня 1973 г. в г. Красноярске.

В 1995 г. окончил юридический факультет Томского государственного университета. В 1997 г. окончил Российскую школу частного права при Исследовательском центре частного права при Президенте РФ. В 1998 г. в Институте законодательства и сравнительного правоведения при Правительстве РФ защитил диссертацию на соискание ученой степени кандидата юридических наук. В 2017 г. получил степень LL.M в университете г. Гейдельберга (Германия).

В настоящее время занимается научно-исследовательской деятельностью в Институте иностранного и международного частного и экономического права университета г. Гейдельберга (Германия).

Автор ряда научных публикаций.

E-mail: 6964889@gmail.com

ОСТАНИНА Елена Александровна

Родилась 15 сентября 1977 г. в г. Челябинске.

В 1999 г. закончила Южно-Уральский государственный университет. В 2007 г. защитила кандидатскую диссертацию на тему «Сделки с отлагательным и отменительным условием как основание приобретения вещного права».

В настоящее время доцент Челябинского государственного университета.

Автор ряда публикаций, среди которых «Сделки как основание приобретения вещного права» (Правоведение. 2007. № 1), «Зависимость правовых последствий сделки от отлагательного и отменительного условий» (М.: Юстицинформ, 2010).

ПЕЧЕНЫЙ Олег Петрович

Родился 31 мая 1976 г. в Днепропетровской области.

В 1998 г. окончил с отличием Национальную юридическую академию Украины им. Ярослава Мудрого (г. Харьков).

Доцент, кандидат юридических наук.

С 2000 г. и по настоящее время преподает на кафедре гражданского права Национального юридического университета им. Ярослава Мудрого (г. Харьков).

Сфера научных интересов: наследственное право; общее учение об обязательствах; вопросы ответственности в гражданском праве; проблемы общей теории гражданского права.

Автор более 100 публикаций, среди которых практический комментарий к Гражданскому кодексу (2012), коллективные монографии из серии «Харьковская цивилистическая школа» («Защита субъективных гражданских прав и интересов» (2015), «Грани наследственного права» (2016), «О договоре» (2017) и пр.), ряда научных статей, включая публикации в сборниках серии «Анализ современного права».

Email: rdash@km.ru

РОЖКОВА Марина Александровна

Родилась 23 июля 1969 г. в Москве.

Доктор юридических наук.

Эксперт Российской Академии Наук, член Экспертного совета Комитета Государственной Думы по информационной политике, информационным технологиям и связи, эксперт Российского фонда фундаментальных исследований, президент IP CLUB, член Комитета по нормативно-правовому регулированию Координационного центра национального домена сети Интернет, руководитель авторского коллектива и ответственный редактор сборников серии «Анализ современного права».

Автор около 300 опубликованных работ, в том числе книг: «Международные договоры в сфере интеллектуальной собственности (актуальный обзор многосторонних соглашений)» (в соавторстве), «Интеллектуальная собственность: основные аспекты охраны и защиты», «Защита интеллектуальных прав: законодательные ошибки при определении статуса и компетенции специализированных органов, разрешающих дела в сфере промышленной собственности», «Защита деловой репутации в случаях ее диффамации или неправомерного использования (в сфере коммерческих отношений)» (в соавторстве), «Актуальные проблемы унификации гражданского процессуального и арбитражного процессуального законодательства» (в соавторстве), «Интеллектуальная собственность: некоторые аспекты правового регулирования» (в соавторстве), «Юридические факты гражданского и процессуального права: соглашения о защите прав и процессуальные соглашения», «Договорное право: соглашения о подсудности, международной подсудности, примирительной процедуре, арбитражное (третейское) и мировое соглашения» (в соавторстве), «Средства и способы правовой защиты сторон коммерческого спора», «Мировая сделка: использование в коммерческом обороте» и т.д.

Email: rozhkova-ma@mail.ru

Web-сайт: rozhkova.com

РУЙЕ Николя

Родился 23 мая 1975 г. в г. Сан-Морис (Швейцария).

Получил юридическое образование в университете Лозанны, закончив его в 1997 г., степень доктора юридических наук – в 2001 г.

С 1997 г. работал судебным секретарем окружного суда Лозанны и ассистентом в Центре корпоративного права и интеллектуальной собственности. Проходил первую адвокатскую практику в юридической компании «Гросс и партнеры» (2000–2003) и присоединился в 2003 г. в качестве партнера к юридической компании *MCE Avocats – Rechtsanwälte – Attorneys-at-law* (Лозанна, Локарно, Фрейбург и Цюрих).

Автор следующих монографий: «О договорах, которые нарушают публичное право» (на нем., 2002, 571 с.); «Швейцарское обязательственное право и Принципы европейского контрактного права» (на фр., 2007, 998 с.); «Швейцарское акционерное общество (коммерческое право, закон о слиянии, налоговое и биржевое право)» (на фр., 2008, 825 с.; 2017, 941 с.); «Банковское дело в Швейцарии» (на нем., 2010 г.; на фр., 2011 и англ. – в 2013 г.). Также является соавтором и соиздателем комментария к наследственному праву (2012, 1145 с.). Написал общее введение в международное предпринимательское право (*International Business Law*, Цюрих/Гонконг, 2015, 618 с.). Текущие монографические работы – о лицензионном договоре.

Является профессором предпринимательского права в Школе Бизнеса Лозанны с 2004 г. Также с 2006 г. преподавал международное торговое право в Академии Народного Хозяйства (Институте бизнеса и делового администрирования). С 2005 по 2012 г. преподавал в Университетском Институте Курт Бош. Представлял швейцарские национальные отчеты в Ассоциации друзей французской юридической культуры об ответственности юристов (Хошимин, 2011), о приобретении власти в корпорациях (Сантьяго-де-Чили, 2012), о соотношении между имматериальными благами и договорным правом (Барселона, 2014), третьих лицах и договоре (Панама, 2015), инвестициях (Берлин, 2016), о концептах в частном праве (Торино, 2017).

РУМЯНЦЕВ Игорь Александрович

Родился 21 сентября 1996 г. в г. Санкт-Петербурге.

В 2013 г. закончил с отличием Санкт-Петербургское суворовское военное училище. В 2014 г. поступил на юридический факультет Санкт-Петербургского государственного университета, на данный момент учится на 3-м курсе.

Является победителем Второго Всероссийского молодежного конкурса работ по праву информационных технологий и интеллектуальной собственности (IP&IT LAW – 2017) с работой «Блокчейн: перспективы правого регулирования».

С 2017 г. работает в должности юриста в ООО «Магнат Профешнл».

Сфера профессиональных интересов: IT/IP, гражданское право, корпоративное право.

РУСАНОВА Юлия Владимировна

Родилась 17 сентября 1995 в г. Омске.

В настоящее время является студенткой 1-го курса магистратуры факультета права Национального исследовательского университета «Высшая школа экономики».

Сфера профессиональных интересов: право интеллектуальной собственности, трудовое право, конкурентное право.

САМСОНОВА Александра Юрьевна

Родилась 8 августа 1994 г. в Москве.

Окончила с отличием международно-правовой факультет МГИМО (У) МИД России в 2016 г. В настоящее время студентка магистратуры МГИМО (У) МИД России по направлению «Международное частное и гражданское право».

Email: ayusamsonova@gmail.com

СЕМЕНОВА Анастасия Александровна

Родилась 25 мая 1996 г. в г. Москве.

В 2014 г. поступила на Международно-правовой факультет МГИМО (У) МИД России. Участник и победитель многочисленных студенческих конкурсов по праву. Автор ряда публикаций в сборниках студенческих работ и статей в блоге на сайте *zakon.ru*. Соавтор статей научно-творческого студенческого объединения «Абстрактный Колобок».

Сфера научных интересов: авторское право, интеллектуальная собственность, сравнительное правоведение, история права.

Email: anastasiiya.semenova@gmail.com

ТИМОШЕНКО Ольга Викторовна

Родилась 17 мая 1997 в г. Перми.

С 2015 г. учится на юридическом факультете МГУ им. М.В. Ломоносова.

Сфера научных интересов: международное частное право, аспекты договорного права в Интернет-пространстве, юрисдикция в сети Интернет.

ЧЕРЕМИСИНОВА Мария Евгеньевна

Родилась 19 июля 1974 г. в Москве.

С отличием окончила юридический факультет Государственного университета нефти и газа им. И.М. Губкина.

Аспирант Института законодательства и сравнительного правоведения при Правительстве Российской Федерации (ИЗиСП).

С 2011 г. – заведующий отделом научных изданий ИЗиСП.

Сфера научных интересов: защита интеллектуальных прав, развитие интернет-отношений.

Публикации: «Социальные интернет-сети: правовые аспекты» (в соавторстве) // Журнал российского права. 2012. № 5. С. 14–24; «Социальные интернет-сети как элемент информационного общества» // Правовые инновации в сфере противодействия коррупции: сборник материалов Первого Евразийского антикоррупционного форума и VII Международной школы-практикума молодых ученых-юристов (Москва, 30–31 мая 2012 г.) / под ред. Л.В. Андриченко, А.М. Цирина. М., 2012. С. 618–624; «Понятие и особенности социальных интернет-сетей» – § 1 гл. 8 монографии «Правовое пространство и человек» / отв. ред. Ю.А. Тихомиров, Е.В. Пуляева, Н.И. Хлуденева. М., 2012. С. 186–191; «Правовая культура: новые аспекты» – гл. 9 монографии «Правовое пространство и человек» / отв. ред. Ю.А. Тихомиров, Е.В. Пуляева, Н.И. Хлуденева. М., 2012. С. 218–235; «Формирование правовой модели информационного общества» – § 3 гл. 2 разд. I монографии «Правовые модели и реальность» / отв. ред. Ю.А. Тихомиров, Е.Е. Рафалюк, Н.И. Хлуденева. М., 2014. С. 45–66 (РИНЦ); «Правовые риски в сфере регулирования интернет-отношений» – п. 1.7 разд. I коллективной монографии «Риски в сфере публичного и частного права» / под науч. ред. Ю.А. Тихомирова, М.А. Лапиной. М., 2014. С. 67–81.

ЧУРИЛОВ Алексей Юрьевич

Родился 4 июля 1992 г. в г. Томске.

В 2014 г. окончил юридический институт Национального исследовательского института Томского государственного университета (НИИ ТГУ). С 2014 г. – аспирант кафедры гражданского права юридического института НИ ТГУ.

Автор ряда работ, среди которых: «К вопросу о правовой природе криптовалюты» (Хозяйство и право. 2016. № 9. С. 93–99); «Сравнительный анализ правового положения третьих лиц в договорных отношениях по праву России и Англии» (Закон. 2017. № 1. С. 48–57), «Договор в пользу третьего лица: вопросы доктрины» (Актуальные проблемы экономики и права. 2016. Т. 10. № 4 (40). С. 96–106).

Сфера научных интересов: обязательственное право, право информационных технологий, право интеллектуальной собственности.

ШАФЕЕВ Кирилл Азизавич

Родился 11 сентября 1995 г. в Харькове, Украина.

В 2016 г. с отличием окончил Европейский гуманитарный университет (Вильнюс, Литва) по программе «Международное право» (magnacumlaude).

На данный момент магистрант Вильнюсского университета по программе International and European Union Law, LL.M.

Сфера научных интересов: право международной ответственности, право Европейского союза, право интеллектуальной собственности, право прав человека.

Email: kiryl.shafeyeu@gmail.com

ХАРИТОНОВА Юлия Сергеевна

Родилась 28 июня 1975 г. в Москве.

С отличием закончила юридический факультет Московского государственного университета им. М.В. Ломоносова.

Доктор юридических наук, профессор.

В настоящее время профессор кафедры предпринимательского права Юридического факультета Московского государственного университета им. М.В. Ломоносова.

Автор более 150 работ по различным проблемам гражданского и предпринимательского права.

Сфера научных интересов – теоретические вопросы предпринимательского права, правовое регулирование управления, корпоративное управление, обязательственное право, право интеллектуальной собственности.

ХОХЛОВ Евгений Сергеевич

Родился в 1984 г. в г. Коврове Владимирской обл.

В 2006 г. окончил юридический факультет МГУ им. М.В. Ломоносова. В 2006–2009 гг. проходил обучение в аспирантуре Института государства и права Российской академии наук.

С 2006 по 2012 г. являлся юристом московских офисов ряда международных юридических фирм (*Linklaters, Clifford Chance, DLA Piper*). С 2012 г. является партнером юридической фирмы *Antitrust Advisory*, которая специализируется в сфере конкурентного права.

С 2013 г. является преподавателем кафедры конкурентного права Московской государственной юридической академии им. О.Е. Кутафина (МГЮА).

Имеет большое количество публикаций в сфере конкурентного права как в российских, так и зарубежных изданиях. В 2015–2016 гг. выступил одним из редакторов научно-практического комментария к Закону о защите конкуренции (отв. ред. И.Ю. Артемьев).

Является членом Ассоциации антимонопольных экспертов и Экспертного совета ФАС России по развитию конкуренции в области информационных технологий. В 2008 и 2011 гг. был награжден почетными грамотами ФАС России за большой личный вклад в проведение государственной политики в области развития конкуренции и плодотворное сотрудничество с антимонопольными органами.

В 2015 г. был награжден медалью ордена «За заслуги перед Отечеством» II степени за вклад в развитие антимонопольного регулирования в России.

TABLE OF CONTAINS

Valeriya A. Larionova

DATA BROKER AS A NEW SUBJECT OF CYBER LAW IN THE ERA OF BIG DATA

Abstract. *This article deals with the analysis of the data broker activities as a new subject of law. It draws our attention to key characteristics of the profiling institution, which is based on the processing of personal data. Much attention is given to the legal status of these companies. Attempts are made to analyze the issue of data broker qualification as key subjects of cyber law.*

Key words: *data broker, personal data, profiling, Big Data, cyber law, transparency.*

Maxim Z. Ali

ACCESS RESTRICTION TO INFORMATION RESOURCES IN THE INTERNET (PRACTICAL PROBLEMS OF RECOGNITION INFORMATION AS PROHIBITED FOR PUBLISHING)

Abstract: *The article based on the example of real court cases on sites' "blocking" contemplates the difficulties which courts deal with in determining the grounds for recognition information as prohibited for publishing. In addition it analyzes the accurateness of compliance with procedural norms and principles used while considering such cases.*

Keywords: *court practice, websites' blocking, information publishing.*

Uliya S. Haritonova

CONTEXT (BEHAVIORAL) ADVERTISING AND THE LAW: POINTS OF INTERSECTION

Abstract. *the Dissemination of information, called targeted, contextual or behavioural advertising involves the collection and analysis of data to determine interests, values, well-being of the subject. The limitation of the concept of personal data subject and their content in the Russian law is not allowed to defend themselves with the application of the relevant law. To protect the rights of persons in case of infringement to the collection, storage and processing of data about them it is advisable to use a used in the practice of the constitutional Court of the Russian Federation the concept of legal interests.*

Keywords: *personal data; right to privacy; personal data protection; private interests; advertising; contextual advertising; the strong-willed actions of the subject.*

proposed to consider the specifics of the law relations developing in the information and telecommunications networks, and possible methods of their legal regulation.

Keywords: *legal theory, Internet, Cyberspace, copyright, information law, intellectual property.*

Vadim A. Belov

DIGITAL PRIVATE LAW & RIGHTS: REFLECTIONS ON THE CHANGES, ALREADY HAS MADE IN THE PRIVATE LAW BY THE DEVELOPMENT OF THE WORLD WIDE WEB, AND ABOUT THE REFORMS, SOON AND INEVITABLY FOR THE SAME REASON ITS PENDING

Abstract. *The article is devoted to the review of the key shifts in private law institutions caused by the advent and development of the global computer network Internet, as well as those coming changes that (for the same reason) will have to take place. In particular, the article draws attention to the de facto death of the future copyright and related rights in their traditional form, immense complexity, related to the implementation and protection of patent rights and means of individualization, fundamental changes in contract law and property law, in terms of subjects, objects and legal facts. According to the author, in the near future we will also transform notions about objective law and the subjective rights of their respective replacement digital counterparts.*

Keywords: *Internet law, scientific and technological progress and law, exclusive rights, means of individualization, contract law, law of property.*

Elena A. Ostanina

MMOG-PLAYERS AS CONSUMERS

Abstract. *Contracts about massive multiplayer online games are characterized as clickwrap agreements. The author insists that the citizen who participates in an MMOG, is a consumer.The article deals with court practice of the United States, Germany and Russia on questions of the protection of consumers in such contracts.*

Keywords: *multiplayer online game, consumer, clickwrap agreement.*

Andrej A. Bogustov

ELECTRONIC CONTRACTS IN THE NATIONAL LEGISLATION OF EU COUNTRIES: POLAND CASE-STUDY

Abstract. *The article provides the analysis of the legal regulation of electronic contracts in the Polish legislation. It is concluded, that the regulation of the pro-*

cedure of the e-contracts formation and conducting, reflects the main trends in the contemporary contract law development, which includes the differentiation of the legal regulations depending on the specific characteristics of the contract parties and contract subject-matter, as well as the limitation of the principle of freedom of contract in the interests of a consumer, as the economically disadvantaged party of a contract.

Keywords: *e-contract, freedom of contract, offer, consumer.*

Oleg P. Pecheniy

IMPACT OF INTERNET-ENVIRONMENT ON TRANSACTIONS ABOUT PROPERTY DISPOSAL IN CASE OF DEATH OF PHYSICAL PERSON

Abstract. *In the article the features of impact of digital environment on the inherited relations are analyzed. The problems of orders in case of death are lighted up and definition of their forms. The problems of disposal by digital assets in case of death are affected. The analysis of current legislation about electronic commerce is conducted, proper directives of European Union. Possibility of the use of electronic digital signature in the field of inheritance is researched.*

Keywords: *inheritance; internet-environment; inherited law; electronic signature.*

Olga V. Timoshenko

CLICK-WRAP AND BROWSE-WRAP AGREEMENTS: A NEW LEVEL OF CONTRACT LAW EVOLUTION IN THE INTERNET

Abstract. *The article is focused on the analysis of the matters related to the legal nature of «click-wrap» and «browse-wrap» agreements. The author tries to determine whether click- and browse-wrap agreements are contracts, what are the nuances of their conclusion, and what problems can arise when formulating the text of such agreements. These questions are considered taking into account the legislation, doctrine and foreign jurisprudence.*

Keywords: *click-wrap agreements, browse-wrap agreements, Internet, contract, user, website.*

Maria E. Cheremisinova

SOCIAL INTERNET-NETWORK AS A SUBJECT OF LEGAL RELATION

Abstract. *The article is devoted to legal aspects of the process of formation of legal status of participants in social Internet networks. Potential legal risks*

associated with the use of Internet networks are identified. The social network is seen as a complex social structure and the subject of study of the philosophical, social and legal science. This approach allows us to search for means of legal regulation of relations formed by the use of telecommunications networks taking into account the social conditionality of legal mechanisms, technological, spatial specifics of the resources themselves.

Keywords: *Social Networking, Legal Status of Participants of Social Networks, Self-regulation, Terms of use, Restrictions on the Rights of Internet Users*.

Natalya S. Emanova

ELECTRONIC TRADING ON SOCIAL NETWORKS: TOPICAL ISSUES

Abstract. *The author investigates a question of the legal guarantees provided to the buyer the Internet – shop on social network, and also ways of protection of the rights by the buyer on social network.*

Keywords: trade, electronic trading, signs of electronic trading, social network, VKontakte, Facebook.

Vera N. Glonina

COPYRIGHT PROTECTION IN THE DIGITAL ENVIRONMENT: THE PROBLEM OF THE LEGAL REGULATION OF HYPERLINKING

Abstract. *The autor writes about the problem of legal regulation of hyperlinking in the Internet. Including the problem of hyperlinking to unauthorised copyrighted material. The author goes on to analyze the foreign and domestic legal theory, legislation and case law on the issue. Author concludes that it is necessary to set out conditions for liability in hyperlinking in the Internet.*

Keywords: *copyright, comparative law, hyperlink, liability of internet intermediaries, communication to the public*.

Yulia V. Rusanova

CREATIVE COMMONS LICENSES

Abstract. *This study focuses on the issue of Creative Commons licenses. The research considers CC licenses as an alternative or addition to the traditional copyright law. In addition, the author pays attention to the question of advisability of supplementing Russian legislation, in particular, the Civil Code of the Russian Federation, with provisions of licenses of Creative Commons.*

Keywords: *Creative Commons licenses, copyright, related rights.*

online arbitration as a pragmatic legal mechanism supplemented with modern communication and data storage facilities, which includes resolving a dispute by the arbitrators and subsequent rendering a binding arbitral award. Special emphasis was devoted to the legal aspects of the online arbitration, the delineation of online arbitration's effective application sphere and the issues of online arbitration conduct.

Keywords: *online arbitration, arbitration agreement, seat of arbitration, dispute resolution, delocalization, arbitral proceedings, arbitral award.*

Nicolas B. Rouiller

DISPUTES ON DOMAIN NAMES: A CHOICE BETWEEN PRIVATE DISPUTE RESOLUTION PROCEDURES (UDRP AND OTHERS) AND STATE COURT PROCEDURES

Abstract. *The author analyses the procedures about domain name dispute resolution, which have been created and implemented by private bodies for over 15 years, and in particular their coordination with procedures on the same subject matter before courts of justice of the State. The different roles and the respective efficiency of these procedures are described and assessed.*

Keywords: *domain name, private dispute resolution procedure, UDRP, SWITCH, pretrial dispute resolution.*

СОДЕРЖАНИЕ