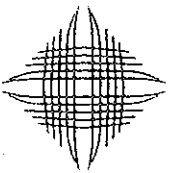
Библиотека «ЮрИнфоР»
Основана в 1994 г.

С. А. Бабкин

Право, применимое к отношениям, возникающим при использовании сети «Интернет»: основные проблемы

Москва
АО «Центр ЮрИнфоР»
2003



1. Общая характеристика отношений с иностранным элементом, возникающих при использовании сети «Интернет»

Уже из приведенных выше тезисов достаточно очевидно, что сеть «Интернет» по своей природе предполагает возникновение множества отношений с иностранным элементом. Вот какой пример приводит М. А. Якушев в статье «Интернет и право»[1]:

«Первый относится к области гражданско-правовых отношений. Стала вполне реальной покупка через сеть определенного товара, скажем, электронной версии каталога деталей самолета. Такого рода информация требуется французской авиакомпании. Продавцом выступает фирма, инкорпорированная в американском штате Невада и использующая сервер, физически находящийся в Англии и принадлежащий английской компании-поставщику. Расчеты производятся через сеть в эквивалентной американским долларам безналичной форме «электронных наличных», процессинговый центр которых (вирту-

[1] Законодательство. 1997. № 1

альный банк) расположен в Австралии и обслуживает, в частности, указанный английский сервер. Сделка заключается в формулярной форме, предложенной фирмой-продавцом. Ссылки на применимое право в формулярном контракте нет. Срок исполнения контракта — немедленно по окончании зачисления денежных средств на счет продавца (обычно максимум несколько часов). Способ исполнения — предоставление покупателю пароля доступа к базе данных, содержащей искомую информацию».

К этому примеру необходимо добавить, что вся изложенная в нем информация, если можно так выразиться, доступна только со стороны. Как мы отмечали, «Интернет» — это совокупность информационных ресурсов с анонимным доступом. Если во «внесетеовй реальности» каждый субъект в подавляющем большинстве случаев осознает, что он вступает в отношения, осложненные иностранным элементом, то при использовании Сети никто не может быть уверен, имеет он дело со своим соотечественником или нет. И это только верхний пласт проблемы. Как справедливо отмечает В. О. Калятин[2], в силу специфики передачи информации через Интернет отправитель и получатель взаимодействуют не напрямую, а через ряд посредников, осуществляющих передачу информации на различных участках сети. Отсюда, информационный обмен через сеть «Интернет» может осложниться еще одним иностранным элементом: *прохождением информации, по поводу которой возникли отношения, через территорию иностранных государств.*

[2] Проблемы установления юрисдикции в Интернете // Законодательство. 2001. № 5

Таким образом, иностранный элемент в отношениях, возникающих при использовании сети «Интернет» может быть представлен в различных вариациях. Самая традиционная связана с тем, что Сеть дает возможность неограниченно вступать в отношения субъектам права, находящимся в самых разных уголках планеты. В этом случае мы имеем классический вариант отношений, в которых участвует иностранное лицо. Более сложная проблема связана с проявлением иностранного элемента в основании или объекте правоотношения, возникающего в связи с использованием сети «Интернет». При этом, в обоих случаях проявляется специфика «Интернета» именно как системы информационных ресурсов. Действия с информацией могут, во-первых, послужить основанием возникновения правоотношения (заключение сделки с использованием электронных документов, деликт в виде распространения информации в цифровом формате, порочащей честь и достоинство и т. д.), а во-вторых, сама информация может быть объектом правоотношений, возникающих при использовании Сети (предоставление доступа к информации на возмездной основе, размещение информации на возмездной основе, объекты исключительных прав в цифровом формате и т. п.). При этом, наличие в отношениях иностранного элемента гипотетически может следовать из двух обстоятельств:

(1) Физическое размещение информации на территории иностранного государства. Речь идет о том, что носитель информации, доступ к которой возможен через сеть «Интернет», расположен на территории иностранного государства. При этом следует помнить, что информация может храниться в дискретной форме: конечные содержание и форму представления информации, которые полу-

чает пользователь сети, могут складываться из элементов, хранящихся на носителях в различных государствах, причем каждый из этих элементов может быть не способен давать воспринимаемые образы отдельно от других. Поясним при помощи, может быть, достаточно грубой аналогии. Можно представить себе разорванный листок бумаги, каждый клочок которого содержит фрагмент рисунка. Причем кусочки настолько малы, что каждый из них вообще не в состоянии пести информационной нагрузки. Кусочки можно сложить и получить вместе рисунок, который запросто может являться объектом авторских прав или конфиденциальной информацией. Принципиальная разница в том, что если складывать рисунок в реальном мире, все кусочки, из которых он состоит должны одновременно находиться в одном месте. В «Интернете» этого не требуется: «рисунок» может сложиться только на экране у пользователя при том, что исходные фрагменты будут продолжать находиться на территории различных государств мира.

(2) *Физическая передача информации через территорию иностранного государства.* Принципиально, что даже сам по себе факт прохождения информации через сети, расположенные на территории иностранного государства, не всегда возможно установить. Еще важнее, что для рядовых пользователей «Интернета» этот факт практически никогда невозможно предсказать. Причем передача информации через «Интернет» характеризуется следующими особенностями:

«а) соответствующий объем информации передается не единым блоком, а фрагментированно, в виде особым образом сформированных пакетов, снабженных данными, позволяющими определить место назначения пересы-

лаемого пакета; б) при передаче информации могут использоваться ресурсы любого фрагмента Интернета в зависимости от работоспособности и загруженности тех или иных соединений; в) конкретный маршрут каждого отдельного пакета заранее неизвестен»[3].

Сходная проблема — так называемое «кэширование» информации. Не вдаваясь в чисто техническую сторону проблемы, остановимся исключительно на юридически значимых свойствах процесса «кеширования». «Кеширование» — процесс, состоящий в создании резервных копий информации для целей облегчения работы с ней. Копии информации, созданные в процессе «кеширования», могут быть доступны для лица, имеющего доступ к соответствующему носителю, однако они в большинстве случаев создаются и удаляются программами без запроса пользователя. Пример «кеширования» — сохранение на жестком диске компьютера информации о web-странице, наличие которой сокращает время доступа к странице при использовании Сети (компьютер, обращаясь к удаленному ресурсу, идентифицирует изменения и «скачивает» только новую информацию, «складывая» ее с сохраненной информацией о web-странице). При этом характерно, что информации, хранящейся на жестком диске компьютера, может оказаться достаточно для вывода на экран точной копии web-страницы без обращения к сети. Однако сама эта информация сохраняется и изменяется даже без уведомления пользователя (на жестком диске информация о web-странице отражает только то ее состояние, которое было зафиксировано в момент последнего доступа).

[3] Калятин О. В. Проблемы установления юрисдикции в Интернете // Законодательство. 2001. № 5

Понимая, что технически «кеширование» может осуществляться самым различным образом, мы отметим, что с правовой точки зрения, оно может быть признано действием, отличным от размещения (распространения, создания копии) информации, только если:

— производится автоматически (пользователь не контролирует конкретное содержание копируемой информации и не может его определять, однако может устанавливать общий режим «кеширования»);

— производится в технических целях (создание копий должно быть обусловлено той или иной задачей, связанной с оптимизацией функционирования программы, получающей, передающей или размещающей информацию).

Достаточно подробное изложение некоторых технических деталей, приведенное выше, на наш взгляд, весьма существенно. От этих деталей в конечном счете зависит признание или непризнание наличия в правоотношениях иностранного элемента.

Безусловно, нельзя не считаться с тем, что информация в результате действия, послужившего основанием возникновения правоотношения, или информация как объект правоотношения фиксируется на носителе, расположенном на территории иностранного государства. Мы не рассматриваем сейчас вопрос о содержании коллизионных норм, рассчитанных на этот случай, однако берем на себя смелость утверждать: указанное обстоятельство (размещение соответствующей информации на носителе, расположенном на территории иностранного государства) свидетельствует о наличии в правоотношении иностранного элемента. Дело здесь в том, что *информация принципиально не может быть доступна через «Интернет» независимо от фактических действий, совершаемых*

в отношении носителя, на котором она зафиксирована. Грубо говоря, если отключить компьютер от электрической сети, ни один пользователь «Интернета» не в состоянии будет получить доступ к информации, записанной на его жестком диске.

Мы не случайно объединили выше передачу информации и ее «кеширование». На наш взгляд, ни передача информации через территорию иностранного государства, ни ее «кеширование» с использованием носителя, расположенного за границей, как таковые не добавляют в отношения иностранный элемент.

Относительно передачи информации основания для этого утверждения достаточно убедительно изложены В. О. Калятиным — правда, применительно к проблеме определения юрисдикции. Он отмечает:

«Представляется, что на этапе пересылки нельзя говорить о юрисдикции какого-то государства над движущейся информацией. Ее передача в пределах страны фактически сводится к мгновенному прохождению серии электрических импульсов по определенной линии связи в общем потоке передаваемых сигналов. И если соответствующее звено Интернета просто пересылает «транзитом» соответствующий пакет далее, деятельность упомянутого звена принципиально не отличается от передачи телефонного сигнала при международном звонке. Очевидно, что на отправителя не должна возлагаться ответственность, например, за содержание направленного им адресату документа в случае, если содержание по тем или иным причинам нарушает законодательство одной из стран, через территорию которых передается такая информация»[4].

[4] Калятин В. О. Проблемы установления юрисдикции в Интернете // Законодательство. 2001. № 5

Эта логика представляется правильной и при квалификации соответствующих отношений как «не отягченных» иностранным элементом: право не может обращать внимание на простую передачу импульсов по территории какого-то государства. Это обстоятельство не может иметь общественного, а значит, и юридического значения. При этом не следует путать простую передачу информации с несанкционированным доступом к передаваемой информации и (или) ее искажением. Если в последнем случае мы обнаруживаем деликт, то его совершение за границей — безусловно иностранный элемент в правоотношении.

С «кешированием» все несколько сложнее. Право стремиться разграничить «кеширование» и размещение (копирование) информации, главным образом, учитывая специфические цели последнего. Уже существует определенный опыт специфического правового регулирования создания «кеш-копий» по сравнению с любым иным копированием аналогичной по содержанию информации[5]. Мы считаем правильным *не придавать значения иностранного элемента просто факту наличия «кеш-копии» той или иной информации на носителе, расположенном в иностранном государстве.* Во всяком случае, любой иной подход потенциально способен необоснованно расширить и без того не узкий круг правоотношений с иностранным элементом, связанных с использованием Сети «Интернет» (самый банальный пример — «кеш-копии» web-страницы, хранящиеся на компьютерах всех обращавшихся к ней пользователей).

[5] См. об этом: Калятин В. О. Персональные данные в Интернете //Журнал российского права. 2002. № 5; Наумов В. Б. Право и Интернет: очерки теории и практики. М., 2002. С. 19

Из сказанного очевидно, что глобальный характер сети «Интернет» отнюдь не означает того, что всякое отношение, возникающее в связи с ней, есть отношение с иностранным элементом. Например, представим себе такую ситуацию: российский гражданин разместил в «Интернете» на сервере, физически находящимся в России, информацию, порочащую честь и достоинство другого российского гражданина. В правоотношениях, возникающих в связи с данным фактом, безусловно никакого иностранного элемента не обнаруживается.

Все изложенные выше тезисы мы склонны считать основой для признания или непризнания наличия в отношениях, связанных с использованием «Интернета», иностранного элемента. Однако совершенно очевидно, что еще большую важность представляет собой вопрос об общей характеристике этих отношений с точки зрения возможности их правовой регламентации. Далеко не все люди, вступающие в контакты между собой при помощи глобальной сети, вступают при этом также в *правоотношения*. Есть сферы, принципиально находящиеся вне сферы правового регулирования (общение между людьми как таковое, доступ к информации на безвозмездной основе и т. д. и т. п.). И очень важно, что в сознании многих людей «Интернет» воспринимается как «внеправовое» пространство именно потому, что если не большая, то значительная часть отношений, возникающих в его рамках, никак не регламентируются и, самое важное, не должны регламентироваться правом. Нас, разумеется, в большей степени интересует именно другая часть отношений: те, что, по крайней мере, нуждаются в правовом регулировании, независимо от того, насколько сегодня они правом урегулированы.

Скажем сразу, что достаточно бессмысленно перечислять все разновидности правоотношений, которые могут возникнуть в связи с использованием сети «Интернет». Во-первых, подобное перечисление невозможно без обращения к фундаментальному вопросу о пределах действия гражданско-правовых норм вообще (более-менее адекватно осветить этот вопрос в настоящем исследовании у нас просто нет возможности). Во-вторых, оно вряд ли может представлять собой ценность на более или менее длительном временном отрезке: меняются технические и программные средства, меняется практика их использования. К тому же во всем спектре юридических проблем «Интернета» нам интересны лишь вопросы, так или иначе связанные с международным частным правом.

В этой связи, как нам представляется, оптимально выделить основные типы отношений, урегулированных правом либо просто нуждающихся в правовой регламентации, возникающих в связи с использованием Сети «Интернет» и получивших распространение на практике. При этом такие типы отношений выделяются с учетом специфики правовой регламентации при появлении в них иностранного элемента.

Следует отметить, что попытки решить проблему классификации правоотношений, возникающих в связи с использованием сети «Интернет» уже предпринимались в литературе. В частности О. В. Калятин в статье «Проблемы установления юрисдикции в Интернете»[6] выделяет несколько разновидностей правоотношений, возникающих при использовании Сети.

[6] Законодательство. 2001. № 5

В первую очередь, *разграничиваются два вида отношений, с точки зрения используемого способа коммуникаций: пересылка определенного объема информации адресату средствами Интернета (отправитель (распространитель информации) должен в этом случае должен совершить некоторые активные действия для того, чтобы адресат получил сообщение) и открытие доступа к определенной информации в Интернете (в этом случае отправитель (распространитель информации) пассивно ожидает, пока потенциальный адресат совершит определенные действия для копирования информации, к которой отправитель открыл доступ). Первый вид коммуникаций автор условно называет активным, а второй — пассивным.* К активным коммуникациям, соответственно, относится, например, отправка электронного письма, к пассивным — помещение информации на сайте.

Эта классификация достаточно важна как вообще для юридических целей, так и для целей международного частного права. Активные коммуникации могут опосредовать собой все элементы самых различных правоотношений. При помощи активных коммуникаций могут заключаться сделки, совершаться деликты и нарушения исключительных прав. В этом случае использование «Интернета» встраивается в юридический факт, влекущий возникновение правоотношений. Активные коммуникации могут составлять предмет исполнения обязательства (например, адресат на возмездной основе получает информацию от своего контрагента). Самое важное, что модель отношений с использованием активных коммуникаций как таковая не содержит в себе ничего специфического, свойственного исключительно «Интернету». Общая логика отношений при использовании активных

коммуникаций та же, что и при аналогичных коммуникациях вне сети[7]. Например, принципы построения отношений с использованием электронной почты те же, что и при использовании обычной почты (мы ни в малейшей степени не стараемся умалить «электронную» специфику — просто она относиться здесь более к области учения о доказательствах, нежели к материальному праву). Даже проблема явления, именуемого spam, не есть что-то необычное. Сходные проблемы возникают у «пользователей» факсов и «железных», а не электронных почтовых ящиков. Аналогично и в области международного частного права. Активный тип коммуникаций предполагает отношения между определенными лицами и именно одно из этих лиц и является пресловутым иностранным элементом. Специфические проблемы здесь тоже существуют, однако их значение не столь велико.

Пассивные коммуникации по своей природе сами по себе не могут использоваться для заключения сделки (хотя в сочетании с активными — аналогично акцепту публичной оферты — вполне в состоянии решить эту задачу), но могут использоваться для исполнения обязательства (предоставление доступа к информационному ресурсу), а равно могут быть элементом деликта (например, при распространении сведений, порочащих честь и достоинство) или нарушения исключительных прав. Для права вообще пассивные коммуникации в «Интернете» представляют собой гораздо более сложное явление. Здесь возникает весь комплекс проблем, связанных с исключительными правами, с юрисдикцией и т. д. Сугубо в области международного частного права специфика пассивных ком-

[7] Определенную специфику может представлять собой анонимность этих коммуникаций.

муникаций двояка. Во-первых, результат их использования имеет экс-территориальное действие, то есть потенциально способен затронуть всех пользователей Сети, все государства, в которых есть возможность доступа к ней. Во-вторых, здесь иностранный элемент может проявиться через место нахождения носителя информации.

Таким образом, и с общеправой точки зрения, и с точки зрения международного частного права, выделение двух типов отношений, возникающих в связи с использованием Сети «Интернет» — в зависимости от способа коммуникации представляется оправданным.

В той же статье В. О. Калятин дает и иную классификацию. Предлагается разграничивать *отношения, замкнутые в «виртуальном мире» и выходящие за его границы.* При этом данное разграничение касается только обязательственных правоотношений. *Первый из названных типов имеет место тогда, когда по заключенной в электронной форме сделке предоставляются определенные внутрисетевые услуги (например, — доступ к информационного ресурса или, наоборот, возможность разместить информацию) либо цифровая копия объекта авторских прав (далее — «внутрисетевые отношения»). Второй — когда по заключенной «внутри» «Интернета» сделки в реальности, за пределами Сети предоставляются товары, работы или услуги, а равно — иные объекты (далее — «внесетевые отношения»).*

Скажем сразу, что это разграничение применимо для возмездных отношений, лишь если мы абстрагируемся от того обстоятельства, что уплата денежного эквивалента неизбежно будет производиться за пределами «Интернета» (хотя возможно и в электронном виде). В остальном, юридическое значение данного разграничения бесспорно. Если из сделки, заключенной в «Интернете» следует пе-

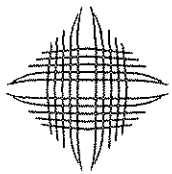
редача товаров, выполнение работ или оказание услуг в реальном мире, то задача, стоящая перед юриспруденцией упрощается. Право вообще должно определиться с приемлемостью соответствующей формы сделки и условиями ее применения, международное частное право — с законом, подлежащим применению к форме такой сделки. Если же сделка и совершается, и исполняется в «Интернете» (за исключением денежного платежа), то к уже названным проблемам добавляются иные. В первую очередь, значительную проблему составляет квалификация соответствующих отношений, особенно если не пытаться втиснуть их во «всеобъемлющие» рамки договора об оказании услуг. Для международного частного права эта проблема также ключевая, поскольку в конечном счете от ее решения зависит выбор применимого к отношениям сторон права. Однако в дополнение к ней появляется специфический иностранный элемент — место нахождения носителя информации.

Выделенные типы безусловно не могут охарактеризовать все многообразие отношений, возникающих в связи с использованием сети «Интернет». Прежде всего, необычайно важно охарактеризовать деликтные и исключительные правоотношения, возникающие в связи с его использованием.

Существо деликтных правоотношений, напрямую, зависит от типа коммуникаций. Единственный деликт, возможный при совершении действий с использованием пассивного типа коммуникаций, — распространение сведений, порочащих честь, достоинство и деловую репутацию. Активный тип таит в себе «большие возможности». Наряду с уже упомянутым вариантом, здесь возможно также причинение имущественного вреда (с помощью использования вредоносных программ и иным подобным

образом). Мы принципиально не будем вдаваться в технические детали: отметим лишь, что речь не обязательно идет об использовании электронной почты; причинение вреда может стать следствием загрузки той или иной программы с сайта — в том числе и без санкции пользователя. С точки зрения международного частного права, наибольшей интерес, кончено, представляет собой проблема места совершения деликта с использованием Сети «Интернет». Наконец, совершенно отдельная проблема — деликт в виде несанкционированного доступа к информации.

Использование объектов исключительных прав в «Интернете» также может осуществляться по обоим типам коммуникаций, причем активный тип здесь заведомо менее интересен — уж слишком похожи отношения по своей сути на традиционные (пользуясь уже приведенной ранее аналогией — можно рассылать на дом аудиокассеты с записью, а можно — рассылать на электронные почтовые ящики аудиофайлы). Основные проблемы, уже всерьез наболевшие и специально рассматриваемые в литературе, возникают в связи с пассивным типом коммуникаций. Основной вопрос из области международного частного права — принцип действия норм внутреннего законодательства и международных конвенций о правовой охране и режиме использования тех или иных объектов с учетом потенциальной возможности доступа к ним из любого государства; размещения его копии также на территории любого государства, а равно — одновременно на территории нескольких государств в виде неохраноспособных частей объекта. Наконец, с использованием объектов исключительных прав посредством пассивных коммуникаций связана стоящая особняком проблема доменного имени.



2. Проблема юрисдикции над отношениями, возникающими при использовании сети «Интернет»

Необходимо отметить, что именно проблема юрисдикции над отношениями по использованию Сети «Интернет», а не проблема определения применимого к ним права, сейчас наиболее часто поднимается в литературе. Для нас в этой связи важно четко определить соотношение названных проблем.

Применительно к рассматриваемой нами теме достаточно важно, что как таковое понятие «юрисдикции» может использоваться в двух различных значениях:

— как сфера действия суверенной власти государства во всех ее проявлениях (то есть законодательной, судебной, исполнительной);

— как международная подсудность, то есть как компетенция судов государства по разрешению определенных категорий гражданских дел, в том числе — с иностранным элементом[1].

[1] Лунц Л. А., Марышева Н. И. Международный гражданский про-

http://www.jurinfor.ru

Совершенно очевидна взаимосвязь двух приведенных значений термина «юрисдикция»: компетенция суда по рассмотрению гражданского спора, возникшего в связи с отношениями с иностранным элементом, следует из того, что на данные отношения распространяется суверенная власть государства.

Каково же соотношение проблемы юрисдикции (в широком и узком смысле слова) и применимого права в связи с отношениями, возникающими при использовании сети «Интернет». Совершенно очевидно, что речь идет *о двух различных проблемах.* Определение юрисдикции того или иного государства над определенными сетевыми отношениями само по себе не предрешает вопроса о применимом к таким отношениям праве. В самом деле, установив юрисдикцию, мы можем ответить на два вопроса: во-первых, на вопрос о том, суд какого государства должен рассматривать спор, а во-вторых — на вопрос о том, какие коллизионные нормы подлежат применению. Однако ни тот, ни другой ответ не определяет самого содержания коллизионных норм. Это, в частности, важно с той точки зрения, что коллизионные нормы могут запросто «привести» к праву иного государства, нежели государство суда, рассматривающего дела. Еще более рельефно различие можно почувствовать, если допустить, что соответствующие коллизионные нормы установлены международным договором, в котором участвуют все государства, задействованные в данном сетевом отношении.

цесс. М., 1976. С. 58, 60.; Международное право: Учебник. Отв. ред. О. М. Колосов, В. И. Кузнецов. М., 1996. С. 73–77; Звеков П. А. Международное частное право. Курс лекций. М., 1999. С. 440–447; Калятин В. О. Проблемы установления юрисдикции в Интернете // Законодательство. 2001. № 5 и др.

В этом случае, какую бы юрисдикцию мы не установили, результатом будет применение одних и тех же коллизионных правил. А если соответствующие отношения сами по себе урегулированы международным договором — то значение вопроса о юрисдикции кажется еще менее значимым.

Таким образом, в практическом плане определение юрисдикции может быть действием, предшествующим определению применимого права, — по крайней мере, в случае возникновения конфликта между участниками сетевых отношений. В теоретическом плане проблема установления юрисдикции над отношениями, возникающими при использовании сети «Интернет», и проблема определения применимого к ним права — абсолютно различные проблемы.

На сегодня в литературе вопроса внимание исследователей явно смещено в сторону проблемы юрисдикции. Проблема применимого права, взятая сама по себе, освещается явно менее пристально. И этому обстоятельству есть свои объяснения.

Первые несколько лет истории сети «Интернет» показали, что наибольший интерес для государства представляет собой возможность многочисленных нарушений запретов, носящих публично-правовой характер, при ее использовании. Причем перечень наиболее часто нарушаемых запретов также логичным образом проистекает из существа Сети как системы информационных ресурсов: речь идет о законодательных ограничениях свободы слова в части распространения порнографических материалов, материалов экстремистского толка, нормах об официальном государственном языке и т. п. Также весьма распространены нарушения норм публичного права в ча-

сти организации азартных игр в «виртуальном пространстве». Имелись случаи нарушений публично-правовых запретов и в рамках «внесетевых отношений» (см. выше) — например, нарушений ограничений оборота алкогольной продукции[2].

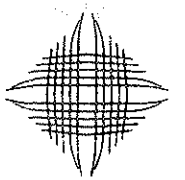
Тот факт, что общественные отношения, возникающие в связи с использованием сети «Интернет», оказались наиболее значимы именно с точки зрения публичного права, предопределил основное направление развития судебной практики и доктрины в области правового регулирования «Интернет-отношений» с иностранным элементом — первичной оказалась проблема юрисдикции, а не проблема применимого права. Ведь по общему правилу на отношения, регулируемые публичным правом, коллизионные нормы не распространяются. Появление в таких отношениях иностранного элемента само по себе не означает постановки вопроса о возможности применения иностранного права; точнее говоря, публично-правовые нормы, подлежащие или не подлежащие применению, будут определяться исходя из того, распространяется или нет юрисдикция соответствующего государства на отношения с иностранным элементом.

Однако у нас есть основания думать, что с течением времени ситуация изменится. Уже сегодня наметилась,

[2] Именно отношения, связанные с нарушением перечисленных публично-правовых запретов при использовании сети «Интернет», породили наиболее интересные и значимые на сегодня судебные прецеденты в области «интернет-права» (главным образом, речь идет о решениях американских судов). Достаточно полные обзоры таких прецедентов даны Наумовым В. Б. в работах: Право и Интернет: Очерки теории и практики. М., 2002. С. 12–23 и Суверенные сети //Компьютерра. 1999. № 43.

по крайней мере, одна область общественных отношений, серьезно затронутых развитием «Интернет-технологий», в которой явно приоритетное значение имеет частноправовое регулирование. Речь идет об отношениях, связанных с созданием и использованием объектов исключительных прав. По мере повышения экономической ценности информации, размещаемой в «Интернете», развития электронной торговли, расширении спектра и объема предоставляемых специфических «Интернет-услуг» (то есть услуг на «внутрисетевом» уровне), проблемы именно международного частного права встанут предельно остро и в этих областях.

В этой связи считаем крайне важным отметить, что в теоретическом плане проблема применимого права может быть рассмотрена вне связи с проблемой юрисдикции. Конечно, такое рассмотрение не является методологически безупречным подходом, однако в нашем случае он обусловлен скромными объемом и задачами настоящего исследования. Во всяком случае, можно сказать, что *общие методы правового регулирования «Интернет-отношений» с иностранным элементом касаются, если можно так выразиться, содержательной стороны юрисдикции государства.* Установив свое право регулировать соответствующие отношения с иностранным элементом, любое государство должно ответить на вопрос: *как* оно их будет регулировать, не исключая, при этом, возможности коллизионной отсылки к иностранному праву или применения международного договора.



3. Право, применимое к отношениям, возникающим в связи с использованием сети «Интернет»: основные общетеоретические подходы

Необходимо отметить, что практически общим местом современных отечественных научных исследований в области «Интернет-права» стало утверждение о необходимости заключения международных соглашений в области регулирования отношений, связанных с использованием Сети. При этом предлагается строить такие соглашения как на началах коллизионного, так и на началах материального права[1].

Сразу отметим: мы абсолютно согласны с тем, что, как и в любой иной сфере международных отношений, именно такой путь является оптимальным. При этом разумеется наиболее предпочтительна не фиксация коллизионных правил на уровне международных договоров,

[1] См.: Якушев М. А. Интернет и право // Законодательство. 1997. № 1; Леанович Е. Проблемы правового регулирования Интернет-отношений с иностранным элементом //http://www.russianlaw.net/law/doc/a102.htm; Наумов Б. В. Право и Интернет: Очерки теории и практики. М., 2002. С. 16–17 и др.

а использование таких договоров для унификации национального законодательства. При этом с учетом анонимности использования Сети, невозможности для участников «Интернет-отношений» с достоверностью установить наличие или отсутствие в них иностранного элемента, унификация национальных законодательств должна вестись по принципу унификации *гражданского*, а не *международного частного права*. То есть правовые нормы должны быть в идеале унифицированы безотносительно к наличию или отсутствию иностранного элемента в регулируемых отношениях.

Все сказанное не вызывает сомнений как своего рода «светлое будущее» правового регулирования «Интернет-отношений». Однако надо четко представлять себе, сколь огромны сложности, связанные с его «построением».

По оценке В. Б. Наумова лишь несколько десятков стран имеют «зачатки национального законодательства, касающегося использования глобального информационного пространства»[2]. В таких условиях надежды на более-менее быструю унификацию правовых норм, регламентирующих использование «Интернета» — подход, мягко говоря, чересчур оптимистический. До того, как возникнет сама возможность провести предметное обсуждение унификации на международном уровне, национальное законодательство в интересующей нас области должно сформироваться и на практике доказать свою способность решать поставленные перед ним задачи. А это процесс, который займет десятилетия, что явно мало сопоставимо с темпами развития «Интернета».

[2] Наумов Б. В. Право и Интернет: Очерки теории и практики. М., 2002. С. 12.

Несколько лучше обстоят дела в сфере возможной унификации норм о юрисдикции и коллизионных норм, однако и здесь перспектива более чем долгосрочная.

Кроме того, необходимо понимать, сколь тотальной должна быть унификация, если мы надеемся получить с ее помощью хоть какой-то значимый результат. Уже сегодня «Интернет» объединяет все страны мира, за исключением беднейших государств и некоторых государств тоталитарного толка. Если унификация произойдет на уровне одних лишь развитых стран, вероятнее всего мы получим бурное развитие «Интернет-оффшоров». То есть страны, не присоединившиеся к международным договорам, будут предлагать услуги по размещению серверов на их территории для осуществления той или иной деятельности в «Интернете», причем эта деятельность будет проходить вне сферы правового воздействия — в соответствующих государствах «Интернет-законодательства» просто не будет. В итоге, затратив колоссальные усилия на унификацию правовых норм, международное сообщество, прежде всего — развитые государства вернутся к тому положению, которое имеет место сегодня.

Таким образом, при всей своей привлекательности решение проблем международного частного права в сфере регламентации «Интернет-отношений» на уровне международных договоров — задача на очень и очень отдаленную перспективу, хотя, конечно, начинать работу в этом направлении развитым государствам и заинтересованным лицам надо уже сейчас.

Другим постоянно встречающимся утверждением касательно нормативного регулирования в сфере использования «Интернета» является тезис о том, что для Сети

оптимальной является саморегуляция[3]. При этом необходимо отметить, что саморегуляция, конечно, не означает регулирование «Интернетом» самого себя. Речь идет о том, что участники «Интернет-отношений» могут самостоятельно выработать систему нормативных предписаний и претворять ее в жизнь, при этом именно такой путь видится оптимальным.

Своего рода венцом идеи саморегуляции стала концепция «Lex electronica», предложенная Каримимом Бенихлефом и Фабьеном Желинасом[4]:

«Можно провести аналогию между условиями средневековой Европы и электронной среды. Разобщение можно обнаружить и в виртуальном пространстве, где принцип территориальности частично утрачивает свой смысл. Ни одно государство не сможет справиться в одиночку с управлением мира, учитывая, что действующие лица находятся вне его границ. Но как писал Хэдфилд, «потребность в правовой структуре для поддержания отношений в киберпространстве остается столь же фундаментальной, как и в Средневековье». Разработка lex electronica является, по сути, естественным продолжением lex mercatoria. Пользователи Интернета на данном этапе развития этого информационного средства не стро-

[3] См.: Глушенков А. Тезисы выступления на международной конференции «Актуальные проблемы права телекоммуникаций. Июль 1998 г. //http://www.legalhelp.ru/rus/articles/ag_2.html; Леанович Е. Проблемы правового регулирования Интернет-отношений с иностранным элементом //http://www.russianlaw.net/law/doc/a102.htm; Наумов В. Б. Право и Интернет: Очерки теории и практики. М., 2002 и др.

[4] Международный опыт разрешения в цифровой среде конфликтов, связанных с авторским правом //http://www.prologo.ru/FEM/fem12.html

ят иллюзий по поводу создания последовательной и всеобъемлющей системы установления норм. Поэтому представляется целесообразным ограничиться правовым регламентированием торговых операций, совершаемых в электронной среде, в частности с помощью установления норм частной торговли».

Какие же черты свойственны «Lex electronica» по мнению авторов концепции? Ну, во-первых, что уже очевидно из сказанного, эта нормативная система не может быть всеобъемлющей. Очень четко ограничивается сфера действия «Lex electronica»: торговля в «киберпространтсве», хоть и понимаемая в самом широком смысле. Единственное, но очень любопытное, дополнение к этой сфере — отношения, связанные с использованием доменных имен. И здесь авторы обращаются к практике ICANN (Internet Corporation for Assigned Names and Numbers), создавшей «замкнутую нормативную сферу» в области присвоения и использования доменных имен и самостоятельно разрешающую соответствующие споры[5].

Во-вторых, Бенихлеф и Желинас не отрицают того, что на нормы, выработанные в процессе саморегуляции, будут оказывать неизбежное влияние нормы националь-

[5] ICANN — организация, обладающая монополией на адресную систему «Интернета» в части родовых доменов первого уровня — то есть имен с «вненациональным» расширением — такими, как com, net и т. п. ICANN обладает правом, делегированным в свое время Властями США, которые изначально контролировали «Интернет-пространство». Это — право присваивать родовые домены верхнего уровня и определять процедуры их присвоения, передачи и т. д. Справедливости ради, отметим, что систем норм, касающихся родовых доменов верхнего уровня, ICANN создала не самостоятельно, а при участии иных организаций (об этом подробнее будет сказано далее).

ного и международного права, а равно судебная практика. Но это влияние не меняет, по их мнению, самой сути «Lex electronica» как нормативной системы, выработанной непосредственно участниками регулируемых ею же отношений.

В-третьих, любопытным дополнением к системе «Lex electronica» выглядит пропагандируемая Бенихлефом и Желинасом система внутрисетевых арбитражей, разрешающих споры в режиме on-line (то есть путем исследования электронных документов, представленных сторонами посредством активной коммуникации внутри Сети, и вынесения решения опять-таки в виде электронного документа). Весьма интересен предлагаемый обзор уже имеющегося (и достаточно значительного) опыта их функционирования.

Мы в целом склонны положительно относиться к идее саморегуляции и ее самому широкому воплощению в практику использования Сети «Интернет». Однако необходимо понимать, что между средневековым и современным обществом (в плане аналогии «Lex electronica» — «Lez mercatoria») существует огромная разница. Прежде всего, государственный суверенитет сегодня в целом значит гораздо больше, и всяким посягательствам на него публичные власти будут противиться. Усложнилась и нормативная система, выработанная государствами. Наконец, мир в целом крайне неоднороден. В «Интернет-отношения» вовлечены, например, столь разные страны как Китай и США с совершенно различными концепциями общества, государства и права.

«Lex electronica» по своему духу не в состоянии разрешить проблему соотношения деятельности в Сети и публично-правовых запретов, существующих на уровне

национальных правовых систем. «Lex electronica» не может быть признана оптимальным регулятором для абсолютных правоотношений (прежде всего — исключительных правоотношений), ведь как система норм она вырабатывается внутри Сети, а соответствующие отношения могут рождаться далеко за ее пределами и лишь в последующем становиться «сетевыми» Возьмем такой пример: автор написал музыкальное произведение. В последующем оно было незаконно размещено в Сети. Применение «Lex electronica» к отношениям между автором и нарушителем его прав было бы, мягко говоря, не совсем правильно с точки зрения интересов автора. Он может быть вообще принципиально против попадания созданного им произведения в Сеть. В этой связи не вызывает сомнения, что любая публичная власть встанет на защиту автора при любом попрании его интересов нормами «Lex electronica». Примерно аналогичным образом будет обстоять дело и при защите экономически слабых сторон общественных отношений (потребителей и т. п.). Наконец, последнее по счету, но не по значимости, замечание. На сегодня профессиональное использование «Интернета» — удел достаточно большого числа специалистов в своей области, но ничтожно малого числа жителей планеты Земля. Причем, ознакомившись со многими источниками как внутри Сети, так и за ее пределами, понимаешь, что мировоззрение профессионалов в области «Интернета» достаточно сильно отличается от общепринятого (которому, представляется, должна соответствовать любая правовая система). А именно от специалистов в технической сфере будет во многом зависеть и разработка, и практика претворения в жизнь «Lex electronica». Как крайний ре-

зультат, мы можем получить нормативную систему, сильно отклоняющуюся от общечеловеческих принципов права, нравственности, справедливости и т. п. (при этом мы не пытаемся выразить здесь какие-то негативные оценки; мы говорим только об отличиях, а не о том, что лучше, а что хуже). Возникает вопрос, насколько мир готов к такому эксперименту?

Таким образом, возможную сферу наиболее оправданного и эффективного применения «Lex electronica» мы видим во «внутрисетевых» отношениях, причем только в части, не затрагивающей интересы третьих лиц. В этом смысле всякий субъект, вступающий в такие отношения, будет, по крайней мере, осознанно принимать определенные правила игры. Что касается «внесетевых» отношений обязательственного типа, то, на наш взгляд, к ним в наибольшей степени применимы уже сложившиеся механизмы международного частного права, которые нуждаются лишь в минимальной корректировке. Сегодня создание в этой области новой нормативной системы выглядит как искусственное насаждение, построенное на том, что за основу берется не суть отношений, а их чисто внешняя форма.

Последним из обобщенных подходов к решению проблемы права, применимого к отношениям, возникающим в связи с использованием Сети, является провозглашение начала автономии воли главенствующим принципом международного частного права в сфере «Интернет-отношений»[6]. Не исключая в принципе применения этого

[6] См. в частности: Глушенков А. Тезисы выступления на международной конференции «Актуальные проблемы права телекоммуникаций». Июль 1998 г. //http://www.legalhelp.ru/rus/articles/ag_2.html;

начала к отношениям, связанным с использованием Сети, следует сделать оговорку о том, что *оно не в состоянии решить... наиболее важные проблемы в интересующей нас области.* Как таковое начало автономии воли мало эффективно во всех внедоговорных отношениях. Разумеется, даже в традиционном международном частном праве существуют случаи, когда оно находит применение и в них. Однако эти случаи все-таки имеют второстепенное значение. Но парадокс состоит в том, что даже в сфере договорных отношений, связанных с использованием сети «Интернет», начало автономии воли неспособно решить одну из наиболее важных проблем. Совершенно очевидно, что все сделки в интересующей нас сфере общественных отношений заключаются в электронном формате (кстати, не всегда при этом корректно говорить об «электронном документе»). Также очевидно, что никакой унификации норм национального законодательства о признании такой формы сделок и требованиях к порядку их заключения не существует. Когда она будет иметь место (и будет ли вообще) — можно только гадать. А именно на вопрос о праве, применимом к форме сделки, начало автономии воли не может дать ответа.

Таким образом, на сегодня ни путь международно-правовой унификации правового регулирования «Интернет-отношений», ни путь создания альтернативной нормативной системы типа «lex mercatoria», ни широкое использование принципа автономии воли по различным причинам не представляются адекватным решением насущных проблем в области определения права, применимого к отношениям с использованием Сети. В этой связи мы склонны рассматривать в качестве наиболее перспективного направления путь постепенной адаптации суще-

ствующих институтов международного частного права к специфике отношений в «виртуальном пространстве» «Интернета». При этом мы полностью разделяем точку зрения Е. Леанович, которая отмечает:

«...нет необходимости разрабатывать новые принципы правового регулирования Интернет-отношений. Эти отношения необходимо «локализовать», «ввести» в сложившуюся правовую систему и рассматривать в ее рамках, как правило, за счет раскрытия в законодательстве тех или иных понятий... а также необходимой модификации и корректировки положений действующих законов»[7].

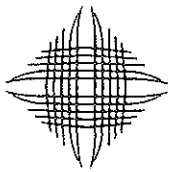
Более того, вслед за Е. Леанович, мы также склонны считать, что судебная практика по спорам в области использования «Интернета» чрезвычайно значима отнюдь не только для стран общего права[8]. И в России, и в других странах, не признающих прецедент в качестве источника права, именно суды и арбитражи потенциально способны быстрее всего внести необходимую корректировку в традиционные юридические механизмы. Роль, традиционно отводимая судебной практике в рамках правовой системы, здесь отодвигается на второй план: в любом случае существуют общие принципы, возможность применения тех или иных норм по аналогии и т. п. Это, конечно, не повод для бездействия законодателя, ибо для любой страны континентального права решение проблемы на уровне законодательства предпочтительнее любого иного. Однако, если смотреть на вещи более-менее реалистично, можно четко себе представить, сколь сложным будет процесс

[7] Проблемы правового регулирования Интернет-отношений с иностранным элементом //http://www.russianlaw.net/law/doc/a102.htm

[8] Там же.

адаптации позитивного права к потребностям «Интернет-технологий».

В двух следующих главах речь пойдет о возможностях корректировки международного частного права в целях более эффективного регулирования «Интернет-отношений». При этом мы ограничимся двумя наиболее значимыми (по нашему мнению) на сегодня направлениями: коллизионное право (самые важные коллизионные привязки из числа нуждающихся в адаптации при применении к отношениям, связанным с использованием Сети) и международная охрана исключительных прав.



4. Отношения по использованию сети «Интернет» и отдельные коллизионные привязки

Сразу отметим: мы не разделяем высказываемую в литературе вопроса точку зрения, согласно которой развитие «Интернет-отношений» требует выработки новых формул прикрепления (коллизионных привязок). Так, Е. Леанович предлагает ввести в оборот привязку, связанную с «местом нахождения сервера»[1]. Мы выше говорили о том, что место нахождения носителя информации само по себе может выступать иностранным элементом в отношениях, связанных с использованием сети «Интернет». Кроме того, вполне понятно, что государство, на территории которого располагается носитель информации, в силу своего территориального суверенитета может предъявлять определенные публично-правовые требования к такой информации, а равно распространять на нее нормы своего законодательства об охране исключительных прав.

[1] Леанович Е. Проблемы правового регулирования Интернет-отношений с иностранным элементом //http://www.russianlaw.net/law/doc/a102.htm

Но может ли место нахождения сервера (то есть носителя информации) стать более-менее широко распространенным критерием для определения применимого права? В первую очередь, следует понимать, что распространение норм с использованием такой привязки вызовет стремление выбирать «удобное право», а значит, развитие «интернет-оффшоров» и, в конечном итоге, серьезное снижение эффективности правового регулирования «интернет-отношений» любым из рассмотренных выше методов. Кроме того, по нашему убеждению, место нахождения сервера вполне может быть принято во внимание в рамках уже существующих формул прикрепления (закон места причинения вреда, закон места совершения сделки и т. п.; подробнее — см. далее по тексту). Наконец, в технической области использованию рассматриваемой привязки препятствует возможность «составления» объектов в цифровом формате с использованием серверов, находящихся в различных странах мира.

Вообще введение в аппарат международного частного права принципиально новых формул прикрепления должно быть тщательно обосновано. Во-первых, необходимо четко себе представлять объем коллизионной нормы или коллизионных норм, в которых эти формулы будут использоваться. Во-вторых, следует очень взвешенно подходить к вопросу о целях и эффективности применения соответствующих коллизионных правил. На сегодня ни уровень развития «Интернет-отношений», ни степень их зависимости от норм международного частного права не позволяют нам сделать вывод о том, что объективно существует потребность в новых типах коллизионных привязок.

Теперь рассмотрим особенности применения некоторых из уже выработанных в международном частном праве привязок к отношениям, связанным с использованием сети «Интернет».

Закон места совершения договора (lex loci contractus)[2]. В «Интернете» заключение сделки в тотальном большинстве случаев может происходить с помощью коммуникаций активного типа. При этом возможны два варианта: либо между сторонами происходит обмен сообщениями (аналогично традиционному «оферта-акцепт»), либо одна из сторон размещает предложение в Сети, и любой ее пользователь может принять предложение, в той или иной форме (установленной лицом, разместившем предложение)[3] выразив свою волю (аналогично акцепту публичной оферты).

Данная ситуация порождает проблемы двух уровней. Первый связан признанием (а равно условиями признания) или непризнанием в государствах, под юрисдикцией которых находятся контрагенты, заключившие договор, электронной формы сделки применительно к отношениям с иностранным элементом.

Так, например, *«при ратификации Конвенции ООН о договорах международной купли-продажи товаров (Вена,*

[2] Согласно ст. 1209 Гражданского кодекса РФ данная привязка (по общему правилу) определяет право, применимое к форме сделки.

[3] Такими формами могут быть как направление сообщения посредством электронной почты, так и ввод информации на том «сайте», где размещено предложение (в любом случае существо действий пользователя одинаково: направление информации с компьютера пользователя в адрес автора предложения при помощи средств «Интернет», если только сам оферент не оговорит обязательность «внесетеового» акцепта, что для нас менее интересно).

1980 г.) (далее — Венская конвенция) правительства Аргентины, Беларуси, Венгрии, Литвы, СССР, Украины, Чили, Эстонии заявили в соответствии со ст. 12 и 96 Конвенции, что любое положение ст. 11, ст. 29 или ч. 2 Конвенции, которое допускает, чтобы договор купли-продажи, его изменение или прекращение соглашением сторон либо оферта, акцепт или любое иное выражение намерения совершались не в письменной, а в любой иной форме, неприменимо, если хотя бы одна из сторон имеет свое коммерческое предприятие в их соответствующих государствах»[4].

Согласно п. 2 ст. 1209 Гражданского кодекса РФ «*форма внешнеэкономической сделки, хотя бы одной из сторон которой является российское юридическое лицо, подчиняется независимо от места совершения этой сделки российскому праву*[5]. *Это правило применяется и в случаях, когда хотя бы одной из сторон такой сделки выступает осуществляющее предпринимательскую деятельность физическое лицо, личным законом которого в соответствии со ст. 1195 настоящего Кодекса является российское право*».

Таким образом, в определенных случаях национальным законодательством вводятся обязательные требования к форме сделки с иностранным элементом и односторонние коллизионные нормы в отношении формы таких сделок. И здесь весьма существенно, где именно будет рассматриваться спор между участниками сделки, поскольку в зависимости от этого, в свою очередь, будут определяться коллизионные нормы, подлежащие

[4] Статус Венской конвенции // Справочная система «Гарант» со ссылкой на www.uncitral.org

[5] Которое, как известно, устанавливает обязательность письменной формы внешнеэкономической сделки под страхом ее недействительности (п. 3 ст. 162 Гражданского кодекса РФ).

применению. Например, российский суд признает недействительной внешнеэкономическую сделку, заключенную в электронной форме между российским и, допустим, австралийским юридическим лицом. Однако, на основе применения «своих» коллизионных норм австралийский суд может прийти к иному выводу. В то же время и он гипотетически может признать сделку недействительной, сославшись на норму, аналогичную содержащейся в п. 2 ст. 1192 Гражданского кодекса РФ[6].

Таким образом, при разрешении спора, возникшего в связи со сделкой, заключенной с использованием средств «Интернет», проблемы закона места совершения сделки может просто не возникнуть, поскольку суд, воспользовавшись односторонней коллизионной нормой и императивными требованиями к форме сделки «своего» права, признает сделку недействительной. Кстати, проблему не стоит ограничивать только лишь принципиальным признанием или непризнанием электронной формы сделки. Речь может идти и об условиях ее признания, которые тоже будут применяться к отношениям сторон на основании односторонней коллизионной нормы.

Таким образом, именно к сделкам, заключаемым в «Интернете», закон места совершения сделки часто не будет применяться в силу использования в националь-

[6] «При применении права какой-либо страны согласно правилам настоящего раздела суд может принять во внимание императивные нормы права другой страны, имеющей тесную связь с отношением, если согласно праву этой страны такие нормы должны регулировать соответствующие отношения независимо от подлежащего применению права. При этом суд должен учитывать назначение и характер таких норм, а также последствия их применения или неприменения».

ном праве односторонних коллизионных норм. В тех случаях, когда данный закон все-таки применяться будет, мы сталкиваемся с проблемой второго уровня, связанной с толкованием данной привязки. Во-первых, как мы уже отмечали, не должно придаваться юридическое значение тому факту, что передаваемая при заключении сделки информация может «проходить» через территорию множества государств. Во-вторых, всегда, когда для заключения сделки используется активный тип коммуникаций, мы имеем два оконечных устройства, расположенных в определенных государствах: компьютер оферента (то есть либо компьютер, на котором находится текст оферты, либо компьютер, с которого оферта была отправлена в сеть) и компьютер акцептанта (компьютер, с которого в сеть был направлен акцепт). Это обстоятельство, если отвлечься от находящейся за рамками нашего внимания проблемы доказательств, по сути уравнивает «Интернет-сделку» с любым договором «между отсутствующими» (то есть договором, заключаемым посредством разъединенных во времени волеизъявлений)[7]. Иными словами, мы не видим здесь принципиальной разницы между электронными и любыми иными средствами связи (включая традиционную почту).

Что же касается проблемы квалификации понятия «места заключения договора» как коллизионной привязки в случае заключения договора «между отсутствующими», то эта проблема для международного частного права не новая, и обсуждать ее здесь было бы неправильно. Отметим лишь, что, например, диспозитивное определение

[7] Гражданское право. Учебник. Отв. ред. Е. А. Суханов. М., 2000, изд. 2-е, перераб. и доп. т. 2, полутом 1. С. 169.

места заключения договора, данное в российском законодательстве (ст. 444 Гражданского кодекса РФ), вообще нивелирует значение того обстоятельства, что договор заключен с помощью средств «Интернет»[8].

Таким образом, само по себе применение коллизионной привязки «Закон совершения сделки» к «Интернет-отношениям», на наш взгляд, не вызывает каких-либо сложностей. Однако безусловно положительно мы бы оценили расширение сферы ее применения. Существующие односторонние коллизионные нормы по вопросу о форме сделок представляются нуждающимися в пересмотре именно в связи с развитием Сети. Государствам необходимо определиться со случаями, когда такие нормы направлены на защиту публичных интересов (например, необходимы для контроля за импортно-экспортными операциями) и ограничить их действие именно этими случаями. На все прочие ситуации односторонние коллизионные нормы лучше не распространять, поскольку они без весомых оснований понижают степень правовой защищенности участников «Интернет-отношений». Для органа, рассматривающего спор и вынужденного применять односторонние нормы, искусственно исключается возможность применения права, более либерального к вопросам формы сделок[9]. Как следствие, участники «Ин-

[8] «Если в договоре не указано место его заключения, договор признается заключенным в *месте жительства* гражданина или *месте нахождения* юридического лица, направившего оферту».

[9] Вполне понятно, что, если используется Закон места совершения сделки, контрагенты могут добиться применения к их отношениям наиболее либерального в отношении электронной формы сделок законодательства. Это может быть сделано за счет адекватного выбора места заключения договора. При этом, разумеется, если данное

тернет-отношений» вынуждены учитывать существование рассматриваемых норм при выборе места арбитража или при принятии решения об обращении в суд того или иного государства.

Закон места совершения деликта (lex loci delicti comissi)[10] . Как мы помним, основные деликты, совершаемые при использовании сети «Интернет», это либо уничтожение (искажение) информации, хранящейся на сервере или компьютере пользователя, либо распространение в «Интернете» сведений, порочащих честь, достоинство и деловую репутацию.

Исходя из этого, можно поставить основной вопрос следующим образом: как определить место причинения вреда в указанных случаях? На наш взгляд, не должно признаваться существенным место нахождения носителя информации, которая была искажена или уничтожена, а равно место размещения информации, порочащей честь, достоинство и деловую репутацию. Возможности «Инетернета» таковы, что, во-первых, достаточно легко разместить соответствующую информацию на носителе, расположенном в государстве, не обладающим развитым законодательством в области возмещения вреда; во-вторых —

понятие будет толковаться органом, рассматривающим спор, аналогично ст. 444 Гражданского кодекса РФ, возможности сторон в плане влияния на право, применимое к форме их договора, окажутся сведены практически на нет. Если же ключевым моментом будет являться, например, место получения акцепта, то такие возможности, напротив, очень и очень велики (в «Интернете» не составит особой проблемы организовать получение акцептов на компьютере, расположенном в другом государстве).

[10] Согласно ст. 1219 Гражданского кодекса РФ по общему правилу применяется к обязательствам, возникающим вследствие причинения вреда.

при распространении через Сеть вредоносных программ место хранения информации, которая может быть искажена/уничтожена вообще непредсказуемо. В то же время исходное действие, влекущее причинение вреда, — помещение в сеть (либо непосредственно пересылка пользователю) вредоносной программы производиться в одном, вполне определенном государстве, где располагается оконечное устройство (компьютер), с которого осуществляется такое помещение (пересылка). Аналогично, кстати, всегда существует оконечное устройство, с которого производиться помещение в Сеть информации, порочащей честь, достоинство и деловую репутацию.

В силу этого мы считаем наиболее целесообразным *в качестве места причинения вреда рассматривать именно место нахождения оконечного устройства (компьютера), с которого производиться помещение в сеть либо рассылка вредоносных программ или информации, порочащей честь, достоинство и деловую репутацию.* Однако совершенно очевидно, что данный подход, сам по себе, в отсутствие специальных коллизионных норм, не способен адекватно защитить людей от недобросовестного использования «Интернета». Например, российское законодательство с учетом практики его применения, известно своим достаточно специфическим отношением к возмещению морального вреда. В этом смысле, если принять предложенную выше концепцию, причинять моральный вред, используя сеть «Интернет», гораздо безопаснее с территории России, нежели, например, из Соединенных Штатов Америки. Вряд ли эту ситуацию можно назвать справедливой.

Сказанное делает актуальным применение к «Интернет-отношениям» *специфических коллизионных привя-*

зок, касающихся причинения вреда. В качестве примера рассмотрим уже существующие коллизионные нормы части 3 Гражданского кодекса РФ.

Согласно п. 1 ст. 1219 Гражданского кодекса РФ *в случае, когда в результате действия или иного обстоятельства, послужившего основанием требования о возмещении вреда, вред наступил в другой стране, может быть применено право этой страны, если причинитель вреда предвидел или должен был предвидеть наступление вреда в этой стране.* Это правило представляется чрезвычайно удачным именно для «Интернет-отношений». Оно позволяет свести на нет попытки причинителей вреда уйти от ответственности или существенно снизить ее размер за счет удачно выбранного права в ситуациях, когда вред осознанно наносится либо конкретным гражданам иностранного государства, либо неопределенному кругу пользователей «Интернета». При этом, на наш взгляд, следует презюмировать, что любое лицо, причиняя вред с использованием средств «Интернет», должно предвидеть возможность его наступления в любой стране мира.

В силу п. 1 ст. 1221 Гражданского кодекса РФ:

«К требованию о возмещении вреда, причиненного вследствие недостатков товара, работы или услуги, по выбору потерпевшего применяется:

1) право страны, где имеет место жительства или основное место деятельности продавец или изготовитель товара либо иной причинитель вреда;

2) право страны, где имеет место жительства или основное место деятельности потерпевший;

3) право страны, где была выполнена работа, оказана услуга, или право страны, где был приобретен товар».

Следует признать, что эта норма весьма привлекательна с точки зрения защиты потребителей услуг в сети «Интернет» (в рамках «внутрисетевых» отношений[11]). По крайней мере, они могут выбирать между тремя правовыми системами, причастными к соответствующему отношению с иностранным элементом.

На примере коллизионных норм российского законодательства, касающихся деликтных отношений, можно очень ясно увидеть, что существующие предписания (общее, о законе места причинения вреда и специальные, которые были только что рассмотрены) вполне применимы к отношениям, связанным с причинением вреда при использовании сети «Интернет». Для этого достаточно их адекватного толкования судами, рассматривающими соответствующие споры.

Закон, регулирующий статут («существо») отношения[12]. Эта коллизионная привязка интересна нам с точки зрения возможности ее применения к «внутрисетевым» отношениям обязательственного типа, вытекаю-

[11] Причинение вреда вследствие недостатков товара, работы или услуги, полученных в рамках «внесетевых» отношений для целей настоящего исследования особого интереса не представляет.

[12] Согласно п. 1 и 2 ст. 1211 Гражданского кодекса РФ: «При отсутствии соглашения сторон о подлежащем применению праве к договору применяется право страны, с которой договор наиболее тесно связан. Правом страны, с которой договор наиболее тесно связан, считается, если иное не вытекает из закона, условий или существа договора либо совокупности обстоятельств дела, право страны, где находится место жительства или основное место деятельности стороны, которая осуществляет исполнение, имеющее решающее значение для содержания договора». Для отдельных видов договора конкретизирующие данную норму правила установлены п. 3–5 той же статьи.

http://www.jurinfor.ru

шим из сделок, прямо непоименованных в законодательстве. Речь идет о следующих договорах (разумеется, интерес представляют случаи, когда договоры являются возмездными — иначе, на наш взгляд, отношения сторон вообще не регулируются правом):

— (1) договор, в соответствии с которым одна сторона предоставляет другой стороне доступ к информационным ресурсам;

— (2) договор, в соответствии с которым одна сторона обязуется перед другой стороной разместить определенную информацию в Сети;

— (3) договор, в соответствии с которым одна сторона обязуется предоставить другой стороне возможность размещать на определенном носителе, дополнительно — под определенным доменным именем, некоторый объем информации, доступный пользователям Сети (здесь могут быть различные технические ограничения — от условия о том, что доступ будет иметь не более чем один человек одновременно, до условия о максимальном числе пользователей одновременно и т. п.).

Рассмотрим вопрос о том, *с каким правом каждый из названных договоров наиболее тесно связан*. При этом мы понимаем, что все они могут быть подведены под конструкцию договора возмездного оказания услуг, как она зафиксирована в российском законодательстве. Однако неслучайно в п. 3 ст. 1211 Гражданского кодекса РФ договор возмездного оказания услуг не указан. Соответствующие отношения столь разнообразны, что просто нельзя вывести некое общее правило — даже с традиционными оговорками о том, что из существа отношений может вытекать иное.

Договор первого типа (предмет — доступ к информационному ресурсу). Здесь, на наш взгляд, имеет место наиболее тесная связь договора со страной, в которой находится исполнитель. Для отношений сторон вообще несущественно, где будет располагаться носитель, содержащий соответствующий информационный ресурс. Заказчик платит деньги за то, чтобы с помощью средств «Интернет» получать определенный набор информации, и где она физически находится — для заказчика вообще неважно. Кроме того, исполнитель может менять место расположения предоставляемой им информации (не меняя оговоренных условий доступа), однако, что особенно важно, в любом случае управление информационным ресурсом осуществляется исполнителем через Сеть с оконечного устройства, контролируемого им и, соответственно, расположенного в том государстве, где исполнитель ведет деятельность[13].

Договор второго типа (размещение информации). Ситуация примерно та же. Заказчику интересна лишь доступность информации в Сети (с теми или иными техническими параметрами). Исполнитель может самостоятельно определять, на каком сервере ему удобно произвести размещение, и это, при условии соблюдения оговоренных технических параметров, вообще не касается заказчика. При этом, разумеется, размещение информации осуществляется опять-таки из места, в котором исполнитель осуществляет свою деятельность.

[13] Мы оставим в стороне проблему различия места нахождения контрагента и места ведения им деятельности, поскольку она не представляет собой ничего специфического для «Интернет-отношений».

http://www.jurinfor.ru

Договор третьего типа (предоставление «дискового пространства» для размещения информации — так называемый «хостинг»). Общее для договоров данного типа то, что их предметом не является размещение определенной информации. Могут быть оговорены лишь определенные ограничения в отношении размещаемой информации (ее содержания и объема), но в целом содержание и форма представления информации определяются заказчиком. Условия доступа к информации могут быть, как уже отмечалось, самые разные. В частности, может быть оговорено размещение информации с открытым доступом под определенным доменным именем; просто хранение файлов на сервере с закрытым доступом (для доступа к файлам требуется введение пароля); управление доступом к информации со стороны заказчика и т. д.

В контексте нашей темы наиболее существенно, что исполнение договоров рассматриваемого типа в ряде случаев может быть наиболее тесно связано не со страной нахождения исполнителя, а со страной фактического нахождения сервера, на котором размещается информация, ибо в большинстве случаев стороны договариваются о размещении информации на определенном сервере и даже используемое доменное имя может быть несущественно (то есть исполнитель может оговорить свое право web-страницу, обеспечивающую доступ к информации). В этом случае основная задача исполнителя состоит в обеспечении надлежащего функционирования сервера, и соответствующие обязательства могут исполняться лишь по месту его фактического нахождения.

Весьма важно, что все рассмотренные выше «внутрисетевые» договоры могут носить *«потребительский» ха-*

рактер. А в международном частном праве отношения с участием граждан-потребителей часто регулируются специфическим образом. Вот что предусмотрено в п. 1 ст. 1212 Гражданского кодекса РФ:

«Выбор права, подлежащего применению к договору, стороной которого является физическое лицо, использующее, приобретающее или заказывающее либо имеющее намерение использовать, приобрести или заказать движимые вещи (работы, услуги) для личных, семейных, домашних и иных нужд, не связанных с осуществлением предпринимательской деятельности, не может повлечь за собой лишение такого физического лица (потребителя) защиты его прав, предоставляемой императивными нормами права страны места жительства потребителя, если имело место хотя бы одно из следующих обстоятельств:

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

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

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

Согласно п. 2 ст. 1212 Гражданского кодекса РФ при отсутствии соглашения сторон о подлежащем применению праве и при наличии указанных выше обстоятельств к договору с участием потребителя применяется право страны места жительства потребителя. При этом, в си-

лу п. 3 той же статьи, что для нас особенно интересно, рассмотренные правила не применяются к договорам об оказании услуг, если услуги выполняются исключительно в иной стране, нежели страна места жительства потребителя.

Любопытно, что все перечисленные нормы оказываются непригодными для регулирования «Интернет-отношений». Если речь идет об использовании Сети — все события, поименованные в п. 1 ст. 1212 Гражданского кодекса РФ могут происходить в совершенно различных государствах, в том числе не совпадающих ни с государством нахождения потребителя, ни с государством нахождения его контрагента. Что касается места оказания услуг, то его вообще определить, как мы отмечали выше, не всегда возможно, да и в любом случае оно окажется несущественным.

Относительно международного опыта в области хотелось бы сослаться на уже упоминавшуюся выше статью Карима Бенихлефа и Фабьена Желинаса. Авторы по поводу «Интернет-отношений» с участием граждан-потребителей отмечают:

«Во-первых, что касается выбора применимых законов, то в Римской конвенции еще до появления Интернета было предусмотрено, что «в результате выбора сторонами применимого закона потребитель не может лишаться охраны, которую ему обеспечивают обязательные положения закона той страны, резидентом которой он является». Применение этого режима к договорам с потребителями, заключаемым на расстоянии, при помощи телекоммуникационных средств, как, например, Интернета, подтверждено Директивой 1997 г., касающейся дого-

воров, заключаемых на расстоянии и защиты интересов потребителей. Этот режим, по всей видимости, означает, что потребитель при сделках через Интернет пользуется защитой закона своей страны, а местонахождение ни продавца, ни его торговых представителей не имеет значения»[14].

Хотя этот подход гораздо более удобен для применения к «Интернет-отношениям», нежели нормы ст. 1212 Гражданского кодекса РФ, мы бы не спешили считать его адекватным регулируемым отношениям. Если вспомнить об анонимности доступа к ресурсам Сети, положению лица, оказывающего услуги потребителям можно только посочувствовать: такое лицо может столкнуться с очень жесткими нормами иностранного законодательства, совершенно не рассчитывая на возможность их применения. В этой связи нам кажется целесообразным определенным образом ограничить возможность применения к «Интернет-отношениям» права страны проживания потребителя:

— всякое лицо, оказывающее услуги в «Интернете», может оговорить при заключении договора, что доступ к услугам вправе получить лишь лица, проживающие в определенных государствах; если потребитель проигнорировал эти ограничения и вступил в отношения с исполнителем, «право страны потребителя» к таким отношениям не применяется;

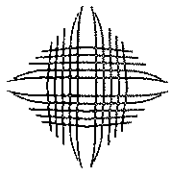
— исполнитель может потребовать от потребителя указать до заключения договора страну проживания; ес-

[14] Международный опыт разрешения в цифровой среде конфликтов, связанных с авторским правом //http://www.prologo.ru/FEM/fem12.html

ли в последующем окажется, что исполнитель был введен в заблуждение, «право страны потребителя» не подлежит применению;

— исполнитель вправе при заключении договора оговорить, что предоставляемая информация или носитель, на котором размещается информации потребителя, находится в определенном государстве, и отношения сторон подчиняются исключительно праву этого государства; если исполнитель указал достоверные сведения, такая оговорка должна быть признана имеющей юридическую силу.

На наш взгляд, подобные правила должны быть либо выработаны судебной практикой, либо включены в национальные законодательства. Их появление определенно способствовало бы развитию цивилизованного рынка «Интернет-услуг».



5. Международно-правовая охрана интеллектуальной собственности и отношения, связанные с использованием сети «Интернет».

Принципиально важными моментами нам представляются следующие. Во-первых, «Интернет» ставит массу вопросов перед правом интеллектуальной собственности как таковым. Попытки найти их правовое разрешение предпринимаются пока еще очень редко. Между тем, необычайно важной представляется *выработка соответствующей системы норм на международном уровне*. Ведь любое регулирование на уровне национального законодательства практически бессмысленно. Если, например, в праве европейских стран и праве США будет по-разному регламентироваться использование объектов исключительных прав в Сети, то ни те, ни другие нормы не будут иметь стопроцентного эффекта. Лица, осуществляющие деятельность в США, будут предоставлять доступ к объектам европейским пользователям в соответствии с законодательством США и наоборот. Объяснение достаточно простое: территориальный суверенитет применительно к «Интернет-отношениям» не работает; пы-

таться регламентировать исключительные правоотношения, возникающие в связи с использованием Сети, только на своей территории бессмысленно[1]. Во-вторых, в связи с развитием Сети резко упало значение международных договоров в области защиты авторских прав. Если раньше неприсоединение к ним отдельных не столь развитых государств не имело существенного значения, то теперь такое значение колоссально. Для соответствующих государств нарушение прав авторов произведений, не пользующихся охраной на их территории, может стать солидным источником дохода. И совершенно бессмысленными будут установленные ранее режимы охраны произведений на территории множества стран мира. Нескольких исключений — то есть государств, не присоединившихся к международным договорам, вполне достаточно для того, чтобы произведение лишилось охраны в Сети, а значит — на территории всей планеты. У проблемы есть два решения. Первый — вводить ограничения для пользователей (могут быть использованы самые различные юри-

[1] В области международно-правового регулирования отношений по использованию объектов интеллектуальной собственности в «Интернете» уже сделаны определенные шаги. Так, в 1996-м году Всемирной организацией интеллектуальной собственности были разработаны два договора: Договор по авторскому праву и Договор по исполнениям и фонограммам («Интернет-договоры»). Однако ни тот, ни другой не вступил в силу (для вступления любого из них в силу требуется ратификация 30 государствами; Договор по авторскому праву подписан представителями 51 государства и ратифицирован 22 государствами; Договор по исполнениям и фонограммам — подписан 50 государствами и ратифицирован 20; ни тот, ни другой договор не подписан Россией) (Рузакова О. А., Дмитриев С. В. Авторские и смежные права в Интернете //Законодательство. 2001. № 9)

дические конструкции — у нас сейчас нет возможности вдаваться в детальный анализ). Однако они и обременительны (в любом случае на пользователя будет возложена обязанность проверять легальность доступа к объекту с точки зрения «своего» права), и мало эффективны, учитывая анонимность доступа к Сети и великое множество ее пользователей в развитых странах. Второй — вводить ограничения в отношении стран, не участвующих в международных договорах в области авторского права. Этот путь кардинально изменит саму природу «Интернета». В конечном счете, он просто перестанет быть глобальной компьютерной сетью. Для того, чтобы осуществить такой вариант потребуется серьезная политическая воля. К тому же мы не исключаем и появления серьезных сложностей технического толка.

Данный раздел был бы неполным без краткого обращения к вопросам правовой регламентации присвоения и использования родовых доменов верхнего уровня (о том, что это такое, было сказано выше по тексту). Сам интернациональный характер деятельности в этой области заставил прибегнуть нормотворчеству на международном уровне; а то обстоятельство, что полномочиями по распределению указанных доменных имен обладает частная организация (ICANN) существенно облегчило процесс нормотворчества, выведя его на внегосударственный уровень.

Еще в 1997 г. ВОИС по просьбе Правительства США инициировала процесс выработки рекомендаций по разрешению споров между владельцами товарных знаков и администраторами доменов в доменах.com,.net,.org. В этой работе приняли участие представители 196 стран. В Итоговом отчете ВОИС, опубликованном 30 апреля

1999 г., содержатся советы, касающиеся порядка самой регистрации, введения единого порядка разрешения споров о доменных именах и создания новых доменных имен верхнего уровня, вопросов соотнесения интеллектуальной собственности и доменных имен. На основе Итогового отчета была разработана Единая политика разрешения споров, являющаяся обязательной и неотъемлемой частью договоров регистраторов с клиентами в доменах.com,.net,.org.

Единая политика разрешения споров была одобрена ICANN 26 августа 1999 г. на совещании в Сантьяго. На сегодняшний день ICANN уполномочила четыре организации рассматривать подобные споры в доменах.com,.net,.org. Статьи 38–43 Итогового отчета и его Приложение VIII предусматривают возможность использования данных рекомендаций в национальных доменах (если в правилах предусмотрен заявительный порядок и не существует каких-либо ограничений по регистрации доменных имен) с учетом национального законодательства[2].

[2] Герцева Е. Н. Проблемы квалификации недобросовестного использования доменных имен в Интернете // Законодательство. 2000. № 11.

2 07 - 61
167

2

Микаэл Дашян

Право информационных магистралей

Law of information highways

вопросы правового регулирования в сфере Интернет

Wolters Kluwer
Москва
Волтерс Клувер 2007

СР62

РОССИЙСКАЯ ГОСУДАРСТВЕННАЯ БИБЛИОТЕКА 2007

УДК УДК [004.738.5:34](470+571)
ББК 67.401.114(2Рос)
Д21

Сведения об авторе: Дашян Микаэл Самвелович — юрист, экономист. С 2002 г. — Президент благотворительного общественного фонда содействия развитию информационно-коммуникационных технологий «ПРАВО И ИНТЕРНЕТ». Автор более 70 публикаций по правовым вопросам (в том числе в сфере правового регулирования Интернет).

Дашян, Микаэл Самвелович.

Д21 Право информационных магистралей (Law of information highways): вопросы правового регулирования в сфере Интернет / М.С. Дашян. — М. : Волтерс Клувер, 2007. — 288 с. — ISBN 978-5-466-00307-9 (обл.).

Агентство CIP РГБ

Книга представляет собой описание и систематизацию наиболее актуальных проблем и их возможных эффективных решений в сфере правового регулирования отношений в Интернет.

На основе анализа законодательства и судебной практики России и других государств автор рассматривает вопросы правового регулирования отношений в Интернет и иных инфокоммуникаций (информационных магистралей). Выявляемые тенденции развития права дополняются практическими рекомендациями, которые выходят далеко за пределы традиционно обсуждаемых вопросов защиты авторских прав в Интернет и доменных имен.

Книга предназначена для руководителей организаций и инвесторов, финансовых аналитиков, юристов, пользователей всемирной сети Интернет.

УДК [004.738.5:34](470+571)
ББК 67.401.114(2Рос)



ISBN 978-5-466-00307-9 (обл.)

© Дашян М.С., 2007
© Волтерс Клувер, 2007

Предисловие

...Очередная законодательная инициатива по регулированию отношений в Интернет — и сразу же возникают ожесточенные споры о важности регламентации этих отношений и контраргументы противников такого регулирования, видящих в нем не что иное, как нарушение основных принципов демократии и приближения «оруэлловского» апокалипсиса...

...Очередное судебное разбирательство, связанное с вопросами Интернет, — и нередко мы сталкиваемся с диаметрально противоположными судебными решениями. Проигравшая сторона обвиняет суды в непоследовательности и некомпетентности, а также во всех остальных смертных грехах, а победители скромно пеняют на необходимость более детального законодательного регулирования...

...Очередной инвестиционный проект в сфере Интернет. Несмотря на высокую доходность и быструю окупаемость он признается не самым конкурентоспособным. Причина проста — отсутствие четкого и понятного законодательства и противоречивое применение права...

К сожалению, стремительное развитие инфокоммуникационных технологий создало для ПРАВА принципиально новые вызовы. Причем самый главный вызов — это вопрос возможности регулирования ПРАВОМ принципиально новых по своей сущности отношений — отношений в информационных магистралях сервисов Интернет и иных сетей, в том числе стремительно набирающей обороты мобильной телефонии.

Раздел II. Международное право

...Международное право сводится к известной степени нравственной воли во взаимных отношениях народов, и поддержание этого нравственного порядка составляет дело чести всего человечества[1].

Артур Шопенгауэр

5. Интернет в международном праве

5.1. Основные документы

С ростом интеграции информационных систем роль международного регулирования сферы Интернет увеличивается. С помощью Интернет заинтересованные лица могут получить продукты, как на национальных рынках, так и за рубежом.

Одним из самых наглядных проявлений глобальной природы отношений в сфере Интернет и информационно-коммуникационных технологиях в целом стало решение, в том числе и правовыми методами, проблемы 2000 года (компьютерного сбоя тысячелетия). Решением проблемы занимались не только на внутригосударственном уровне в разных государствах, но и сообща на международном, поскольку ин-

[1] *Шопенгауэр А.* Избранные произведения. М., 1992. С. 139–141.

формационные и телекоммуникационные пространства отдельных стран теснейшим образом связаны сегодня между собой[1].

На сегодняшний день существует несколько международно-правовых документов, напрямую регулирующих сферу Интернет.

Первым документом в достаточно условном списке является **Окинавская хартия** глобального информационного общества (принята 20 июля 2000 г. на о. Окинава)[2]. Государства, заключившие хартию[3], провозглашают, что к глобальному информационному обществу нужно стремиться. Устойчивость глобального информационного общества основывается на стимулирующих развитие человека демократических ценностях, таких как свободный обмен информацией и знаниями, взаимная терпимость и уважение к особенностям других людей.

Конвенция Совета Европы о преступности в сфере компьютерной информации *ETS* № 185 (подписана от 23 ноября 2001 г. в г. Будапешт, далее — Конвенция о киберпреступности)[4] охватывает сферу преступлений, совершаемых в глобальных компьютерных сетях посредством информационно-коммуникационных технологий. В указанной конвенции регламентируются виды преступлений в киберпространстве (нормы материального уголовного права), а также процессуальные вопросы, в частности, определение юрисдикции, вопросы обыска и выемки компьютерных данных и т.д.

Несмотря на то, что конвенция принята Советом Европы, она открыта для подписания как государствами — членами Совета Европы, так и не являющимися его членами государствами, которые участвовали в ее разработке. Например, в конвенцию вошли такие государства, как Россия, США и Япония. Для присоединения к конвенции необ-

[1] См. например: Коммюнике глав государств и правительств стран «Группы 8-ми» (Подписано в г. Кельне 18–20 июня 1999 г.).

[2] Дипломатический вестник. 2000. № 8. С. 51–56.

[3] К государствам, заключившим Хартию, относятся: Великобритания, Германия, Италия, Канада, Россия, США, Франция, Япония.

[4] СПС «КонсультантПлюс».

ходимо согласие остальных государств – участников Конвенции о киберпреступности (ст. 37).

Отношения в Интернет и других глобальных компьютерных сетях напрямую регламентируются приведенными международными документами.

Кроме того, в перечень международно-правовых актов, относящихся к сфере Интернет, входит множество документов, некоторые из которых приняты даже до возникновения компьютерной сети *ARPANET*, предшествовавшей появлению Интернет. Например, Конвенция Совета Европы о защите прав человека и основных свобод ETS № 5 (заключена 4 ноября 1950 г. в г. Риме)[1], Конвенция о международном праве опровержения (одобрена 16 декабря 1952 г. Резолюцией 630 (VII) Генеральной Ассамблеи ООН)[2], Международный Пакт о гражданских и политических правах (принят 16 декабря 1966 г. Резолюцией 2200 (XXI) Генеральной Ассамблеи ООН)[3] и многие другие документы.

В список обсуждаемых международных документов следует обязательно включить и документы, принятые ЮНЕСКО: Конвенцию «Об охране нематериального культурного наследия» (принята 17 октября 2003 г. в г. Париже)[4], Конвенцию «Об охране и поощрении разнообразия различных форм культурного самовыражения» (принята 20 октября 2005 г. в г. Париже)[5], а также Рекомендацию «О развитии и использовании многоязычия и всеобщем доступе к киберпространству» (принята 17 октября 2003 г. в г. Париже)[6].

Указанные документы гарантируют международную поддержку (охрану и поощрение) культурного разнообразия[7], нематериального

[1] СЗ РФ. 1998. № 20. Ст. 2143 (с послед. изм.).

[2] Международное частное право. Сборник документов. М., 1997. С. 538–542. (Россия не участвует.)

[3] Бюллетень Верховного Суда РФ. 1994. № 12. С. 5–11.

[4] <www.unesco.ru/docs/intangible-convention.pdf>.

[5] < http://www.ifap.ru/ofdocs/cppdce.pdf>.

[6] <www.unesco.ru/docs/multilingv-ciberspace-recom-rus.pdf>.

[7] Под «культурным разнообразием» понимается многообразие форм, с помощью которых культуры групп и обществ находят свое выражение. Эти формы самовыражения передаются внутри групп и обществ и между ними. Культурное разнообразие проявляется не только через применение различных средств, с помощью которых культурное наследие человечества выражается, расширяется и передается благодаря многообразию форм культурного самовыражения, но и через различные виды художественного творчества, а также производства, распространения, распределения и потребления продуктов культурного самовыражения, независимо от используемых средств и технологий (ст. 3 Конвенции «Об охране и поощрении разнообразия различных форм культурного самовыражения»).

культурного наследия[1], принятие необходимых мер для уменьшения языковых барьеров и активизации интерактивного общения между людьми через Интернет путем содействия созданию и обработке образовательного, культурного и научного содержания в цифровом формате, а также подхода к этому содержанию, с тем чтобы все культуры имели возможность для самовыражения и доступа к киберпространству на всех языках, включая языки коренного населения[2].

Также в этот список с рядом оговорок могут быть внесены документы, связанные с Международным Союзом Электросвязи – МСЭ (Конвенция МСЭ, подписана 22 декабря 1992 г. в г. Женева[3]; Устав МСЭ, принят 22 декабря 1992 г. в г. Женева[4]); ряд международно-правовых актов, касающихся охраны интеллектуальной собственности[5]; и иные международно-правовые документы, которые так или

[1] Под «нематериальным культурным наследием» понимаются обычаи, формы представления и выражения, знания и навыки, а также связанные с ними инструменты, предметы, артефакты и культурные пространства, признанные сообществами, группами и, в некоторых случаях, отдельными лицами в качестве части их культурного наследия. Такое нематериальное культурное наследие, передаваемое от поколения к поколению, постоянно воссоздается сообществами и группами в зависимости от окружающей их среды, их взаимодействия с природой и их истории и формирует у них чувство самобытности и преемственности, содействуя тем самым уважению культурного разнообразия и творчеству человека. Для целей настоящей конвенции принимается во внимание только то нематериальное культурное наследие, которое согласуется с существующими международно-правовыми актами по правам человека и требованиями взаимного уважения между сообществами, группами и отдельными лицами, а также устойчивого развития (ст. 2 Конвенции «Об охране нематериального культурного наследия»).

[2] Пункт 1 Рекомендации «О развитии и использованию многоязычия и всеобщем доступе к киберпространству».

[3] СЗ РФ. 1996. № 48. Ст. 5370.

[4] Там же.

[5] Подробнее см.: *Чудинов Г.В.* Защита объектов интеллектуальной собственности // Новости искусственного интеллекта. 2002. № 3.

иначе относятся к областям информационных технологий, массовых коммуникаций, средств массовой информации и т.д. При такой инкорпорации главным условием выступает возможность отнесения конкретного международно-правового акта к достаточно обширной сфере отношений в Интернет.

5.2. Интернет в рамках СНГ: становление нормативной базы

В рамках Содружества Независимых Государств также был принят ряд документов, касающихся вопросов Интернет, информационных технологий, охраны интеллектуальной собственности. Обратим внимание на некоторые из них:

В ст. 2 Соглашения между Правительством Российской Федерации и Правительством Республики Казахстан о развитии сотрудничества в области связи и информатизации, заключенном 19 июня 2000 г. в г. Москве[1], устанавливается, что Стороны соглашения обязуются проводить согласованную политику в международных организациях, регулирующих распределение адресного пространства для национальных сегментов сети Интернет. Также стороны поручат соответствующим органам исполнительной власти проработать вопрос создания регионального органа, координирующего распределение адресного пространства Интернет.

8 ноября 1999 г. для Российской Федерации вступило в силу[2] Соглашение о свободном доступе и порядке обмена открытой научно-технической информацией государств — участников СНГ, заключенное 11 сентября 1998 г. в г. Москва[3]. Соглашение включает в себя положения об информационных ресурсах общего пользования.

При этом под информационными ресурсами совместного пользования понимается «совокупность информационных ресурсов, находящихся под юрисдикцией государств — участников Соглашения о межгосударственном обмене научно — технической информацией

[1] Бюллетень международных договоров. 2001. № 11. С. 50–51.

[2] См.: Постановление Правительства РФ от 26 октября 1999 г. № 1196 // СЗ РФ. 1999. № 44. Ст. 5324.

[3] Российская газета. Экономический союз. 1998. 19 дек.

и определенных ими в качестве элементов, обеспечивающих межгосударственный обмен научно-технической информацией в той части, которую государство определяет как достаточную для осуществления обмена» (ст. 1). К данным информационным ресурсам относятся:

- созданные совместно сторонами до 1991 г.;
- созданные после 1991 г. и предоставляемые сторонами в совместное пользование;
- формируемые совместно сторонами.

В Соглашении указывается порядок предоставления информационных ресурсов совместного пользования. В данную категорию входят:

- свободный доступ к фондам научно-технической информации;
- использование межбиблиотечного абонемента сторон;
- вхождение в компьютерные информационные сети, базы и банки данных совместного пользования;
- обращение к справочным электронным каталогам и адресно-справочным базам данных совместного пользования.

1 июня 2001 г. в г. Минске было заключено Соглашение о сотрудничестве государств — участников Содружества Независимых государств в борьбе с преступлениями в сфере компьютерной информации[1]. В документе был закреплен список преступлений, относящихся к данной сфере. В него вошли:

- осуществление неправомерного доступа к охраняемой законом компьютерной информации, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование информации, нарушение работы ЭВМ, системы ЭВМ или их сети;
- создание, использование или распространение вредоносных программ;

[1] Содружество. Информационный вестник Совета глав государств и Совета глав правительств СНГ. 2001. № 1 (37). С. 138–145.

- нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети лицом, имеющим доступ к ЭВМ, системе ЭВМ или их сети, повлекшее уничтожение, блокирование или модификацию охраняемой законом информации ЭВМ, если это деяние причинило существенный вред или тяжкие последствия;
- незаконное использование программ для ЭВМ и баз данных, являющихся объектами авторского права, а равно присвоение авторства, если это деяние причинило существенный ущерб.

Сотрудничество между государствами в области данных преступлений осуществляется непосредственно через компетентные органы. Формами такого сотрудничества может быть обмен информацией; исполнение запросов о проведении оперативно-розыскных мероприятий, иных процессуальных действий; планирование и проведение скоординированных мероприятий и операций по предупреждению, выявлению, пресечению, раскрытию и расследованию преступлений в сфере компьютерной информации; оказание содействия в подготовке и переподготовке кадров; создание **информационных систем**, обеспечивающих выполнение задач по предупреждению, выявлению, пресечению, раскрытию и расследованию преступлений в сфере компьютерной информации; а также обмен информацией о национальном законодательстве, проведение совместных научных исследований и иные взаимоприемлемые формы (ст. 5).

5.3. Интернет: Альтернативная модель международно-правового развития

Можно предположить, что оптимальной формой решения комплекса вопросов, связанных с юридизацией статуса Интернет, станет международное соглашение об использовании глобальной сети Интернет, открытое для подписания всеми заинтересованными государствами. Так, например, при подписании такого соглашения в рамках Содружества Независимых Государств можно предусмотреть в качестве одного из условий возможность любого другого зарубежного государства присоединиться к указанному соглашению.

В преамбуле соглашения необходимо указать, что стороны:

- сознают, что в интересах всего человечества глобальная компьютерная сеть Интернет должна и впредь использоваться исключительно в мирных целях и не должна стать ареной или предметом международных разногласий;
- признают существенный вклад, внесенный в научные и образовательные процессы благодаря международному сотрудничеству при использовании сети Интернет;
- убеждены в том, что установление прочного фундамента для продолжения и развития такого сотрудничества на основе свободы использования Интернет в научной, образовательной и иных социально полезных областях отвечает интересам науки и прогресса всего человечества;
- убеждены также в том, что соглашение, обеспечивающее использование Интернет только в мирных целях и продолжение международного согласия в сфере Интернет, будет содействовать осуществлению целей и принципов Устава Организации Объединенных Наций, Окинавской хартии глобального информационного общества, основополагающих принципов международного права.

Также в документе должны быть закреплены и основные положения, указанные в Окинавской хартии глобального информационного общества, такие, как:

- призыв ко всем как в государственном, так и в частном секторах ликвидировать международный разрыв в области информации и знаний;
- подтверждение приверженности, государств, заключающих соглашение, принципу: «все люди повсеместно, без исключения должны иметь возможность пользоваться преимуществами глобального информационного общества», а также принципов свободного обмена информацией и знаниями, взаимной терпимости и уважения к особенностям других людей, повышения уровня доступности власти для всех граждан.

В тексте соглашения необходимо закрепить принадлежность Интернет всему человечеству, использование в мирных целях (за исключением, оборонительных действий), возможность каждого желающего

использовать сервисы Интернет. В то же время, необходимо указать, в каких случаях может быть ограничено право граждан и организаций на доступ в Интернет. В частности, по нашему мнению, такими основаниями может быть угроза безопасности (экономической, информационной и т.д.), а также нарушение общепринятых норм морали и нравственности. При этом важно упомянуть недопущение ограничений в использовании Интернет в связи с политическими, культурными, научными основаниями.

Нужно заметить, что подобная предлагаемой правовой модели концепция была положена в основу Соглашения о создании международной системы и организации космической связи «Интерспутник», заключенного 15 ноября 1971 г. в г. Москве[1].

Внимательный читатель здесь может предъявить автору претензии в отсутствии четко выраженного мнения, ведь в предыдущих главах указывалось, что Интернет не может быть признан международной организацией, не может иметь единого административного центра, и тем более, места пребывания. Но подчеркнем, что при подготовке соглашения об Интернет необходимо не просто переписать все положения об «Интерспутнике» или иные документы. Необходима кропотливая работа, связанная с анализом уже имеющихся правовых моделей, их эффективности, целесообразности, а также соответствия научно-технической природе сети Интернет.

Так, необходимо принятие положений, аналогичных положениям об «Интерспутнике», касающихся: сотрудничества с международными организациями; правоспособности; не распространения норм соглашения, на государства, не подписавшие его. Также весьма эффективным может оказаться принятие нормы, аналогичной норме о возможности присоединения к договору любого государства, не подписавшего этот документ. Единственным условием присоединения становится подача в специально учрежденный межправительственный орган официального заявления о поддержании целей и принци-

[1] Ведомости ВС СССР. 1972. № 34. Ст. 317.

пов провозглашенных в соглашении и принятии на себя соответствующих обязательств[1].

Однако признание в навязываемом правительствам, подписывающим соглашение, порядке Интернет международной организацией, нормативное установление ее местонахождения, признание ее юридическим лицом может отрицательно сказаться на основополагающих принципах международного права и Глобального информационного общества[2].

Также нужно подчеркнуть, что заключение подобного соглашения об Интернете в рамках СНГ может одновременно решить ряд актуальных проблем:

Во-первых, возникнут предпосылки для решения проблемы создания специальной законодательной и иной правовой базы, регулирующей непосредственно отношения в сфере Интернет на внутригосударственном уровне.

Во-вторых, будут разрешены вопросы, связанные с явной недостаточностью принятых в рамках СНГ документов, требованиям современности. Ведь, в сравнении с работой Европейского Союза или Организации экономического сотрудничества и развития (ОЭСР), в рамках СНГ уделяется недостаточно внимания вопросам Интернет.

В-третьих, принятие соглашения, связанного Интернет, даже при очевидной декларативности его содержания, может привлечь инте-

[1] См., для примера: ст. 22 Соглашения о создании международной системы и организации космической связи «Интерспутник»:
«1. Правительство любого государства, не подписавшее настоящее Соглашение, может присоединиться к нему. В этом случае правительство подает Совету Организации официальное заявление о том, что оно разделяет цели и принципы деятельности Организации и принимает на себя обязательства, вытекающие из настоящего Соглашения.
2. Документы о присоединении к Соглашению сдаются на хранение правительству-депозитарию».

[2] Нужно заметить, что многие юристы подчеркивают тот факт, что Интернет не может являться юридическим лицом. См.: *Малахов С.В.* Гражданско-правовое регулирование отношений в глобальной компьютерной сети Интернет: Дис. ... канд. юрид. наук. М., 2001. С. 59; *Якушев М.В.* Интернет и право // Законодательство. 1997. № 1. С. 66.

рес к принявшему документ международному образованию, а также его членам: России, Украине и другим государствам, со стороны остальных членов международного сообщества, что может существенно отразиться на инвестиционном климате, укреплении старых и налаживании новых межгосударственных связей, организации международного взаимодействия в сфере противодействия киберпреступности (в том числе кибертерроризма)[1].

6. «Территория» Интернет

6.1. Юрисдикция или компетенция

Особую актуальность приобретают вопросы применения национального права того или иного государства, определения компетенции публично-правовых образований при регулировании отношений в Интернет, а также определения юрисдикции[2].

Данные проблемы достаточно глубоко исследованы отечественными и зарубежными правоведами. В работах Виктора Наумова, Стефана Уилске, Томаса Ли, Дарелла Менте и многих других, они обозначены как «проблемы юрисдикции»[3].

В.Б. Наумов весьма точно охарактеризовал сущность данной проблемы: «в настоящее время несколько десятков стран имеют зачатки национального законодательства, касающегося использования глобального информационного пространства. Международные соглашения по этому вопросу отсутствуют, обычаи использования Сети весьма противоречивы — а значит, спорных ситуаций становится все больше, и постепенно формируется судебная практика по данным общественным отношениям»[1].

Что же понимается в юриспруденции под понятием «юрисдикция»? Юрисдикция возникает в тех случаях, когда необходимо решить спор о праве или когда нарушены правовые предписания (юридические дела, обусловленные позитивными обстоятельствами, не охватываются юрисдикцией). Юрисдикция как процесс — это способ разрешения правовых конфликтов. Все виды юрисдикций объединяет одно — юридический способ охраны общественных отношений, заключающийся в рассмотрении компетентным органом юридического дела по существу и принятия решения по нему[2].

Понятие «юрисдикция» применяют в международном праве для обозначения суверенных прав власти государства на своей территории, а в уголовном и гражданском процессах, судоустройстве — для характеристики подсудности тех или иных категорий дел[3].

Однако наиболее часто термин юрисдикция используется в международном частном праве, а также активно используется в процессуальном праве США и других зарубежных государств. Принимая во внимание публично-правовой характер многих отношений в Интернет, следует отметить, что для российского права термин «юрисдикция» не в полной мере отражает всю палитру рассматриваемого вопроса. Поэтому весь рассматриваемый в настоящей главе комплекс правовых проблем мы предлагаем обозначить не как юрисдикционные проблемы, а как проблемы определения компетенции в сфере Интернет.

---

1 Подчеркнем, что высказанная точка зрения основана исключительно на субъективном мнении автора.

2 В работе термин «юрисдикция» рассматривается в его традиционном понимании, если специально не оговорено иное (юрисдикция — от лат. *jurisdictio* — судопроизводство; совокупность правомочий соответствующих государственных органов разрешать правовые споры и решать дела о правонарушениях. См.: Юридическая энциклопедия. М., 2000. С. 504).

3 См: *Наумов В.Б.* Право и Интернет: Очерки теории и практики. М., 2002. С. 12–13; *Menthe D.* Jurisdiction In Cyberspace: A Theory of International Spaces // Mich. Telecomm. Tech. L. Rev.69 1998. 4. <www.mttlr.org/html/volume_four.html/menthe.html>; *Wilske S., Schiller T.* International Jurisdiction in Cyberspace:Which States May Regulate the Internet? // <www.law.indiana.edu/fclj/pubs/v50>; *Lee. T.* In Rem Jurisdiction in Cyberspace // Wash. L. Rev. 1997. 75.

1 *Наумов В.Б.* Право и Интернет: очерки теории и практики. С. 12.

2 См.: *Фиалковская И.Д.* Административная юрисдикция в области обеспечения прав человека: Проблемы теории и правового регулирования: Дис. ... канд. юрид. наук. М., 1997. С. 10–25.

3 См.: *Тихомиров Ю.А.* Теория компетенции. М., 2001. С. 54.

И. М. Рассолов

3

2 09 - 35 / 274

ПРАВО И ИНТЕРНЕТ

Теоретические проблемы

2-е издание, дополненное

Издательство «Норма»
Москва, 2009

Ф5-1
432 б1к-1

РОССИЙСКАЯ ГОСУДАРСТВЕННАЯ БИБЛИОТЕКА 2009

УДК 341.9
ББК 67.412.2
Р24

Рецензенты:

Сектор информационного права Института государства и права РАН (заведующая сектором доктор юридических наук, профессор **И. Л. Бачило**);

Кафедра информационного права, информатики и математики Российской правовой академии Министерства юстиции РФ (заведующий кафедрой доктор юридических наук, профессор **А. В. Морозов**);

А. С. Брод — директор Московского бюро по правам человека, член Общественной палаты РФ.

Рассолов И. М.

Р24 Право и Интернет. Теоретические проблемы / И. М. Рассолов. — 2-е изд., доп. — М. : Норма, 2009. — 384 с.

ISBN 978-5-91768-003-3

В издании представлен новый в отечественной юриспруденции подход к проблемам взаимодействия права и киберпространства. На основе новейших российских и зарубежных разработок по теории права и информационному праву автором предложена новая концепция права виртуального пространства (интернет-права), обозначены основные принципы и условия действия права в киберпространстве. Значительное место в работе уделяется анализу влияния права на цифровой мир, а также классификации отдельных видов преступлений, совершенных с использованием Интернета.

Для студентов, аспирантов и преподавателей вузов, а также для всех, кто интересуется вопросами правового регулирования Интернета.

2007463475

УДК 341.9
ББК 67.412.2

В оформлении обложки использован рисунок «Аура Земли», автор — профессор Версальской архитектурной школы *С. Г. Порада.*

© Рассолов И. М., 2003
© Рассолов И. М., 2009, с изменениями
© ООО «Юридическое издательство НОРМА», 2009

ISBN 978-5-91768-003-3

Предисловие

Интернет прочно вошел в нашу повседневную жизнь, стал ее неотъемлемой частью. Сегодня трудно представить, что совсем недавно его еще не было. Не было тех фантастических возможностей, которые он нам предоставляет в любой области. Например, товарооборот в российском сегменте Интернета в 2008 г. составил порядка 8 млрд долл. США.

Но вместе с Интернетом возник и новый тип общественных отношений — интернет-отношения. Деятельность в Сети рождает множество проблем — этических, экономических, социальных и правовых. И все их нужно исследовать и упорядочить. Поэтому мне представляется интересной книга молодого исследователя И. М. Рассолова «Право и Интернет».

В работе впервые предпринята попытка представить интернет-право как современное направление юридической науки. Для обоснования этого положения автору потребовалось проанализировать целый круг проблем: исследовать понятие и содержание интернет-права в свете современной юридической науки; охарактеризовать отношения, регулируемые интернет-правом; рассмотреть общую концепцию Интернета с точки зрения информационного права; исследовать понятие, основные черты и формы проявления права виртуального пространства; изучить поведение субъектов в цифровой среде; исследовать отдельные проблемы правосознания и правовой культуры участников интернет-отношений.

В исследовании предложено решение важных проблем в сфере защиты интеллектуальной собственности. Одна из таких проблем — пресечение распространения контрафактной продукции. Автор справедливо указывает, что существующий механизм правового регулирования защиты интеллектуальной собственности (литературной, худо-

риусу отпечатанное или переведенное на другой носитель произведение. В случае возникновения проблем субъект (автор) сможет представить суду опечатанный конверт, содержащий произведение, с проставленной на нем датой. Свидетельские показания, а также доказательства, представляемые провайдером, суд также должен принимать во внимание.

Мы предлагаем помимо правовых средств защиты исключительных прав использовать здесь также технологии, наделяющие электронный документ возможностью саморазрушения в случае его незаконного использования.

§ 3. Совершенствование законодательства об ответственности за качество информации, распространяемой во всемирной сети Интернет

Проблема качества информации давно обсуждается в теории права, в том числе в аспекте применения средств кибернетики, математических методов и технических комплексов[1]. Однако эта проблема в аспекте совершенствования законодательства об ответственности за качество информации, которая распространяется во всемирной сети Интернет, исследовалась лишь в общем виде[2]. Поэтому остановимся на некоторых ее аспектах в контексте идей интернет-права, и в первую очередь — на проблеме ответственности субъекта за качество информации, распространяемой в сети Интернет.

Известно, что все информационное наполнение и использование сети Интернет в коммерческих и некоммерческих целях осуществляется посредством услуг организа-

[1] См. об этом: *Венгеров А. Б.* Категория «информация» в понятийном аппарате юридической науки. С. 70—76; *Кудрявцев Ю. В.* Ценность правовой информации // Правоведение. 1977. № 1. С. 45—51; *Он же.* Избыточность правовой информации // Советское государство и право. 1978. № 12. С. 53—60; *Бачило И. Л.* Информация как предмет правоотношений. С. 17—25; *Шебанов А. Ф.* Содержание и цели правовой информации // Правовая информация / Отв. ред. *А. Ф. Шебанов, А. Р. Шляхов, С. С. Москвин.* М., 1974. С. 7—16.

[2] См. об этом: *Семилетов С. И.* Информация как особый нематериальный объект права // Государство и право. 2000. №5. С. 67—74; *Корзников А. М., Носова И. А.* Указ. соч. С. 64—67.

ций, обеспечивающих доступ к сети Интернет, размещение и передачу информации в сети Интернет, так называемых провайдеров.

Провайдер — специализированная организация, оказывающая услуги по доступу в Сеть, размещению и передаче информации в Сети.

В ст. 3 проекта федерального закона «Об электронной торговле» употребляется термин «информационный посредник» — «лицо, которое от имени другого лица отправляет, получает или хранит электронные документы или предоставляет другие услуги в отношении данных документов». Таким образом, это физическое или юридическое лицо, оказывающее услуги по передаче (получению), хранению электронных сообщений, предоставлению доступа к сетям электросвязи и информационным системам.

В настоящее время провайдер — это основной поставщик услуг в сети Интернет. Среди услуг, которые предоставляют провайдеры, для данного исследования интересны следующие (базовые услуги): организация доступа в сеть Интернет; предоставление свободного дискового пространства на сервере для размещения сайта, принадлежащего другому лицу (хостинг).

С точки зрения права, чтобы стать пользователем Сети, необходимо заключить с провайдером договор об оказании услуг по доступу в Сеть (т. е. установить с провайдером необходимые интернет-отношения). Для сеанса доступа в Интернет провайдер предоставляет пользователю IP-адрес (число, состоящее из четырех частей), который позволяет однозначно идентифицировать каждый компьютер в Интернете. IP-адрес необходим для маршрутизации запросов пользователя, когда с этого адреса на сервер провайдера поступает запрос пользователя, — компьютер провайдера осуществляет поиск в сети Интернет полученных данных и отправляет найденную информацию на IP-адрес пользователя. Отсюда возникло определение провайдера как информационного посредника.

Информационное наполнение сети Интернет осуществляется посредством заключения договора хостинга. По своей правовой природе договор хостинга схож с догово-

ром аренды: провайдер за определенную плату предоставляет лицу свободное дисковое пространство на своем сервере, а указанное лицо размещает на нем сайт.

Нужно отметить, что действия информационных провайдеров по оказанию услуг характеризуются следующими чертами: провайдер не инициирует интернет-отношение, не выбирает содержание передаваемой информации и ее получателя, не влияет на содержание информации, но хранит информацию только в пределах времени, определяемого техническими стандартами и протоколами, исходя из нужд передачи информации.

Указанная многомерность отношений, а также тот факт, что провайдер имеет техническую возможность в любой момент воздействовать на интернет-отношения своих пользователей, определили появление института ответственности провайдеров.

Изучение законодательства разных государств показало, что в них проблема ответственности провайдеров решается по-разному. Причем здесь можно выделить три основных подхода к решению данной проблемы: 1) провайдер несет ответственность за все действия пользователей вне зависимости от наличия у него как у субъекта права знания о совершаемых действиях; 2) провайдер не несет ответственности за пользователей в том случае, если выполняет определенные условия, связанные с характером предоставления услуг и взаимодействием с субъектами информационного обмена и лицами, чьи права нарушаются действиями пользователей и 3) провайдер не отвечает за действия пользователей.

В Китае и странах Ближнего Востока, например, используется первый подход, в Европе — второй. Так, в Европейской директиве по электронной коммерции от 28 февраля 2000 г.[1] (разд. 4, ст. 12—15) проработано наи-

[1] Директива 2000/31/ЕС Европейского парламента и Европейского Совета о некоторых правовых аспектах услуг информационного общества, в том числе электронной коммерции на внутреннем рынке (вступила в силу 8 июня 2000 г.). Текст на русском языке опубликован в издании: *Шамраев А. В.* Указ. соч. С. 317—327.

более детально решение проблемы указанного вида юридической ответственности.

Директива устанавливает, что провайдер не несет ответственности за передаваемую информацию в случае, если он не инициирует ее передачу, не выбирает получателя информации и не влияет на целостность передаваемой информации. При этом допускается временное хранение передаваемой информации для осуществления необходимых технических действий по ее передаче. Утверждается, что провайдер не несет ответственности за действия пользователей при предоставлении услуг хостинга, если он не был осведомлен об их противозаконной информационно-правовой деятельности и после получения информации об этом прекратил размещение или доступ к информации. Аналогичное положение устанавливает и Федеральный закон «Об информации, информационных технологиях и о защите информации» (ст. 17).

В настоящее время в ряде стран мира приняты предметные законы, касающиеся института ответственности провайдеров. Так, в шведском законе, регулирующем ответственность владельцев электронных досок объявлений (Act (1998:112) on Responsibility for Electronic Bulletin Boards)[1], устанавливается, что таковые обязаны удалять сообщения третьих лиц в том случае, если содержащаяся в них информация нарушает ряд норм уголовного и гражданского законодательства (в части авторского права). Похожая на европейскую, но менее детальная схема ответственности при нарушении авторских прав определена в американском Digital Millenium Copyright Act (DMCA)[2], принятом в 1998 г. В Англии действует Defamation Act[3], принятый в 1996 г., который регулирует ответственность интернет-провайдеров за достоверность размещаемой на их сайтах информации.

[1] См.: {http://www.media.parlament.org.ua/uploads/files/f252.pdf}.

[2] См.: *Wilbur M. K.* DMCA: The Digital Millenium Copyright Act. Lincoln (Nebraska). 2001. {http://www.copyright.gov/legislation/dmca.pdf}.

[3] *Sandford C., Boyle F.* Defamation Act 1996: The New Law (Impact Series). Newcastle upon Tyne, 1997. {http://www.opsi.gov.uk/acts/acts1996/1996031.htm}.

На сегодняшний день в российском законодательстве четко не определены механизмы привлечения к ответственности провайдеров за размещение на обслуживаемых ими сайтах недостоверной информации, а также не установлена возможность предъявления к ним претензий за качество размещаемой информации.

О сложившейся судебной практике в этой области говорить сложно.

Поэтому необходимо законодательное разрешение проблемы ответственности информационных провайдеров в России и в странах СНГ. В ходе совершенствования российского законодательства в данной области можно использовать схему и формулировки ст. 18 Рекомендаций по организации деятельности лиц в сфере интернет-коммерции в Российской Федерации[1], разработанных рабочей группой по электронной коммерции Комитета Государственной Думы по экономической политике и предпринимательству в 2000 г.

На наш взгляд, изменения и дополнения в российское законодательство должны вноситься по принципу, в соответствии с которым провайдер должен нести ответственность за качество информации, размещаемой на его сервере, в случае если:

1) данная информация размещалась по его инициативе и (или) за его счет;

2) провайдер был осведомлен или имел возможность быть осведомленным о содержании информации, размещаемой на его сервере;

3) преднамеренные или непрофессиональные (противоречащие профессиональной подготовке, работе и возможности) действия провайдера повлекли размещение незаконной информации на его сайте.

Таким образом, ответственность провайдера наступает в зависимости от наличия его вины в размещении информации, нарушающей права третьих лиц.

Бремя доказательства отсутствия вины провайдера следует возложить на самого провайдера, который должен

[1] См.: {www.rfc.ru/duma/recom_ic.doc}.

привлекаться в судебный процесс в качестве ответчика, а в случае отсутствия его вины ненадлежащий ответчик должен заменяться лицом — автором вредной информации (провайдер остается в процессе в качестве третьего лица).

Такой механизм привлечения к ответственности будет вполне оправдан, если учесть, что фактически информация размещена на дисковом пространстве сервера, принадлежащего провайдеру (т. е. источник противоправной информации — компьютер провайдера).

В этом случае провайдеры сами будут заинтересованы в более тщательной проверке информации.

Необходимо законодательно закрепить право провайдера по результатам проверки:

— или блокировать информацию, для выявления противозаконности содержания которой не требуется специальных знаний;

— или информировать компетентные органы о наличии сомнительной информации для более тщательной и компетентной проверки.

На наш взгляд, потенциал провайдера необходимо использовать в интересах упрощения процедуры по сбору доказательств в судебном процессе.

В случае привлечения провайдера к ответственности последний будет заинтересован в поиске надлежащего ответчика — автора вредной информации, тем более что организационные и технические возможности провайдера позволяют ему осуществлять поиск как никому лучше.

Кроме того, необходимо обязать провайдеров регулярно копировать информацию с лог-файла, бережно хранить и предоставлять ее при первом требовании заинтересованных и компетентных государственных органов.

Обобщая сказанное, можно утверждать, что проблема ответственности провайдеров — это особенно острая и насущная проблема государственной политики не только в области Интернета, но и вообще в интернет-праве. От того, как будет определена и регламентирована роль провайдеров в информационных общественных отношениях в сети Интернет, зависит дальнейшее развитие сети Ин-

тернет, а также нового направления юриспруденции — интернет-права.

Исследование показало, что заметные осложнения вызывают возникающие в виртуальном пространстве интернет-отношения, отягощенные иностранным элементом. Они имеют место, когда электронная сделка либо заключается гражданами разных государств, либо ущерб в результате использования сайта причинен на территории иностранного государства, либо информация, размещенная на сайте, нарушает законы иностранного государства об охране прав интеллектуальной собственности и т. д.

На практике довольно часто распространена ситуация, когда потребитель информации, владелец информационного ресурса и хост-провайдер являются гражданами разных государств. При возникновении между сторонами судебного разбирательства встают следующие проблемы:

1) юрисдикции какого государства подчинено правоотношение (т. е. суд или компетентный орган какого государства вправе рассматривать дело);

2) право какого государства подлежит применению (традиционно в международном частном праве используются коллизионные привязки для определения применимого права — «закон места нахождения», «закон места заключения», «закон места причинения» и т. д. Однако в настоящее время они все более приобретают совершенно иное звучание в связи с интернет-отношениями и используются в сочетании с таким критерием, как «место нахождения сервера»[1]).

Как правило, у субъектов интернет-отношений с иностранным элементом есть возможность выбрать применимое право и место рассмотрения спора. Однако не во всех

[1] Данная привязка для определения применимого права (место физического нахождения сервера, на котором размещена информация) принимается во внимание как американскими, так и европейскими юристами. Впервые такая схема была предложена в 1999 г. экспертами американской правительственной группы по электронной торговле и ОЭСР. С 2005 г. она признается наиболее реализуемой идеей в сфере электронной торговли, в частности в вопросе взимания налога на прибыль в данной сфере. Об этом подробнее: *Тедеев А. А.* Указ. соч. С. 247.

случаях этот способ будет эффективен. Стороны не всегда смогут по объективным (выбор применимого права возможен в основном в договорных отношениях) или субъективным причинам (стороны просто могут не договориться) совершить свой выбор.

Правовое регулирование в данной новой области только начало складываться, и пути его развития пока еще не определены. Результатом такой неопределенности может явиться то, что принятие решения судом о рассмотрении спора по отношениям, связанным с Интернетом, а также о выборе применимого права и его содержании будет зависеть от осведомленности судей в вопросах специфики интернет-отношений и от способности с учетом этой специфики дать адекватное толкование законов судом и применимой норме права.

В связи с этим показательным является судебное дело в отношении сайта «Ингушетия.ру». Уголовное дело возбудили по заявлению прокуратуры Ингушетии из-за статьи журналиста газеты «Ангушт», размещенной на этом информационном ресурсе. В апреле 2008 г. Московский городской суд отказался рассматривать дело о признании сайта экстремистским и запрете его деятельности. Мосгорсуд посчитал производство дела неподсудным и перенаправил его в Кунцевский районный суд по месту регистрации владельца сайта. В свою очередь, Кунцевский районный суд г. Москвы посчитал, что это дело находится в его юрисдикции, несмотря на то, что сайт зарегистрирован в США, а деятельность ресурса связана с территорией Ингушетии. Таким образом, российский суд провозгласил сразу несколько важных принципов, которые легли в основу судебной практики в России. Суд установил подсудность данных споров исходя из принципа фактического присутствия ответчика на территории страны суда, провозглашая закон своей территории по данному делу. Уголовное дело возбудили по ч. 1 ст. 282 УК РФ по месту жительства владельца доменного имени (защита в ходе прений отрицала, что предполагаемый субъект преступления является владельцем самого сайта).

Кроме того, Мосгорсуд посчитал, что сайт «Ингушетия.ру» не является СМИ, что вытекает из критериев определения подсудности и отсутствия предварительного письменного предупреждения, которое обычно направляется учредителю и (или) редакции (главному редактору) до закрытия СМИ по Закону «О средствах массовой информации» (ст. 16).

В любом интернет-споре с иностранным элементом в первую очередь возникает вопрос о том, в суд какого государства подать иск. Поэтому остановимся более подробно на характеристике возможных правовых коллизий, которые могут возникнуть при решении юрисдикционных проблем интернет-отношений.

Если принцип автономии воли сторонами в выборе суда не применяется, работает механизм международного частного права, который известен во всех правовых системах мира.

Механизмы и процедурные нормы, по которым решаются подобные вопросы, в рамках каждой национальной юрисдикции различаются и имеют специфику. По процессуальным вопросам в международном частном праве традиционно применяется правило lex fori, по которому каждый суд применяет свое собственное право. В разных государствах правила определения международной подсудности имеют характерные черты и особенности. Тем не менее национальность или место нахождения ответчика — основной критерий, которым руководствуются суды при решении вопроса о наличии своей компетенции рассматривать интернет-спор.

Основанием такого правила исторически выступает фактор физического присутствия или физической досягаемости ответчика для суда. Однако бурное развитие высоких технологий, сложность определения места и времени совершения сделки (интерактивного обмена данными), уже не позволяет этому условию играть решающую роль. Экстерриториальность Сети дает возможность преступнику нарушать законы государства без физического нахождения на его территории. Следовательно, суду для надлежащего обеспечения правопорядка на своей территории необходимо расширять правила юрисдикции и за основу брать уже не закон ответчика, а, как считает Е. Б. Леанович, «фактическую связь спорного отношения с государством суда»[1].

Интересна практика судов США, где темпы развития рынка телекоммуникаций — основная причина массового рассмотрения подобных интернет-споров в судах.

До настоящего времени в США основным принципом решения юрисдикционных проблем являлась так называемая персональная юрисдикция (personal jurisdiction), в соответствии с которой суд обладает компетенцией по рассмотрению интернет-спора в отношении физического или юридического лица, если оно физически присутствует на его территории. Однако сегодня этот принцип дополнен, а порою напрямую заменен принципом минимальных контактов, т. е. связь ответчика с определенной территорией может служить оправданием для юрисдикции суда этой территории, и само физическое пребывание (статус резидента) ответчика не является определяющим условием юрисдикции американских судов[2].

В этом случае можно вести речь о так называемой универсальной юрисдикции США, экстерриториальности закона, распространении его действия на граждан и вне пределов того штата, в котором был издан данный закон. Среди подобных критериев следует особо выделить различные юридические факты, в основном действия. Например, факт заключения сделки (договор поставки товара, оказания услуг); владение и пользование недвижимостью; наличие постоянного счета в американском банке, по которому производится расчет с кредитором; причинение имущественного вреда на соответствующей территории. Поэтому в интернет-спорах американские суды признают наличие своей юрисдикции, принимая во внимание

---

[1] *Леанович Е. Б.* Проблемы правового регулирования Интернет-отношений с иностранным элементом // Белорусский журнал международного частного права и международных отношений. 2000. № 4. С. 39—44.

[2] Там же.

только существование определенных связей правоотношения с территорией США — даже в том случае, если ответчик не является резидентом этой страны.

Простое размещение на сайте информации о товарах и услугах, постоянное обращение к ней американских граждан может быть рассмотрено как основание для вывода о наличии юрисдикции (если, например, лицо не ограничивает доступ к размещаемым в Интернете сообщениям резидентам США или размещаемая информация доступна на английском языке). Тем не менее, как справедливо считает В. Б. Наумов, «в США начинают понимать, что потенциальный доступ к сайту посредством Интернета не порождает автоматически ответственности владельца сайта за несоблюдение закона какого-либо штата. Для наступления ответственности необходим непосредственный информационный контакт, порождающий прямые фактические коммерческие отношения, осуществление которых необходимо доказать»[1].

Изучение показало, что в европейских странах вопросы международной подсудности решаются в основном исходя из критерия физической досягаемости ответчика. М. М. Богуславский условно выделяет три основные системы определения подсудности: 1) по закону гражданства (Франция); 2) по закону домицилия (Германия)[2] и 3) по признаку фактического присутствия ответчика на территории страны суда (Великобритания). Кроме того, позитивное право и судебная практика европейских государств предусматривают возможность судебного разбирательства в отношении субъектов (лиц), не являющихся гражданами и не находящихся на их территории. Это происходит в том случае, когда спорное правоотношение тем или иным образом связано с судом государства[3]. На-

[1] *Наумов В. Б.* Суверенные сети // Компьютерра. 1999. № 43. С. 22—23.

[2] Домицилий — место постоянного жительства физического лица или официальной регистрации юридического лица. Выделяется несколько видов домицилия: домицилий происхождения (домицилий отца); домицилий в силу закона (жена имеет тот же домицилий, что и муж, даже если проживает в другой стране) и др.

[3] См.: *Богуславский М. М.* Указ. соч. С. 398—437.

пример, в качестве таких критериев связи может выступать нахождение имущества, факт заключения сделки или причинения вреда ответчиком на территории государства суда. Однако каким образом специфика правоотношений в Интернете может повлиять на изменение основных правил определения подсудности в европейских государствах, судить пока сложно.

Можно предложить решение проблемы определения юрисдикции путем межгосударственного согласования применяемых критериев. Для этого возможны следующие способы:

1) заключение международного соглашения об определении вопросов юрисдикции в отношении деятельности с использованием сети Интернет, в котором необходимо определить критерии отнесения к юрисдикции государства для каждого распространенного типа отношений;

2) частичное устранение проблем путем унификации материального законодательства. Если однородные интернет-отношения будут защищаться в различных государствах в одинаковой степени, выбор юрисдикции будет не принципиален (например, по Конвенции о киберпреступности);

3) заключение международного соглашения, определяющего применимое право к различным ситуациям (например, право страны нахождения сервера, на котором размещен сетевой информационный ресурс). Такой способ будет эффективен лишь при одновременной унификации законодательства различных стран, иначе недобросовестное лицо (субъект интернет-отношений) сможет заранее «подобрать» для себя удобное право.

Основой для подобного соглашения по вопросам подсудности в рамках СНГ может выступать Соглашение от 20 марта 1992 г.[1] о порядке разрешения споров, связанных с осуществлением хозяйственной деятельности, которое ратифицировано постановлением Верховного Совета РФ от 9 октября 1992 г. № 3620-I. Среди подобных

[1] Информационный вестник Совета глав государств и Совета глав правительств СНГ «Содружество». 1992. № 4.

коллизионных привязок ст. 4 Соглашения выделяет: постоянное место жительства; место нахождения на день предъявления иска; место осуществления хозяйственной деятельности ответчика; место нахождения имущества в спорах о праве собственности на недвижимое имущество; место исполнения обязательства из договора, являющегося предметом спора и т. д.

Как один из вариантов решения вышеизложенных проблем можно предложить создать специальный международный правовой режим для Интернета. Данный способ представляется достаточно сложным, однако некоторый опыт уже имеется — достаточно вспомнить специальные правовые режимы Мирового океана, Антарктики, космического пространства.

Однако нельзя не понимать, что опыт в установлении специального правового режима в отношении неизменных объектов окружающего мира не сравним с возможными усилиями установления правового режима в отношении постоянно и свободно развивающегося организма системы Интернет.

В свете изложенного остановимся на проблемах применения в Интернете специального режима юридической ответственности, установленного для прессы и аудиовизуального распространения информации во Всемирной сети.

В логике эволюции Интернета и права наиболее простое и быстрое решение состоит в том, чтобы переместить на Интернет (определенным образом приспособив) специальный режим редакционной ответственности, установленный для прессы (печати) в наиболее развитых странах (в частности, во Франции). Основным ответственным субъектом здесь признаются лица, обладающие специальными знаниями в этой сфере (например, ответственный редактор или выпускающий редактор). Данный режим отличается от общего некоторым количеством специфических характеристик. Общий режим ответственности существует параллельно этому специфическому режиму. Редакционная ответственность применяется только за правонарушения, совершенные в сфере прессы и установленные специальным французским Законом о свободе прессы от 29 июля 1881 г. (гл. IV)[1].

Итак, возникает вопрос: может ли телеинформатика заимствовать режим специальной юридической ответственности, установленный для прессы и аудиовизуального распространения данных?

Французский законодатель пожелал установить принцип особой ответственности для печати, содержащий оговорку в общем праве, чтобы упростить свои возможные уголовные преследования. Система здесь основывается на принципе полной субсидиарной ответственности, определяя автоматически априорное ответственное лицо. Таковыми являются ответственный редактор (выпускающий редактор); за неимением его — автор, за неимением автора — владелец типографии, затем продавцы и распространители (ст. 42 упомянутого Закона).

Чтобы выступать ответственным лицом, редактор (выпускающий редактор) должен иметь возможность контролировать распространяемые сообщения. Режим субсидиарной ответственности применяется только тогда, когда вредная информация явилась объектом предварительной фиксации и по своему назначению была предназначена для широкой публики, являлась публичной, т. е. когда о ней имелась запись. В силу этого в случае выбросов информации непосредственно в Сеть определенным лицом юридическая ответственность накладывается на того, кто совершил такие действия.

При решении вопроса об уголовной ответственности субъекта (лица) французский суд считает, что электронные правонарушения не подпадают под специальный режим, установленный для прессы, в тех случаях, когда электронные службы не создают публикации в прессе (сетевые издания) и не обладают определенными признаками (написанное сообщение, периодичность и др.). Таким образом, к большинству правонарушений в киберпро-

[1] Текст опубликован в издании: La loi de 1881 à l'aube du III-e millénaire // Revue thématique de droit de la communication LEGICOM. P., 2003. № 28. {http://www.laboucherie.com/pdf/presse.pdf}.

странстве, преследуемых по французскому закону, применяются нормы общего (неспециального) права. В тех же случаях, когда интерактивные службы предлагают консультацию по базам данных, содержание которых уже записано, это способно повлечь ответственность выпускающего редактора исходя из специального режима ответственности, установленного для прессы.

Итак, на основе правового режима, установленного для французской прессы, структура субъектов ответственности может выглядеть следующим образом:

— ответственный редактор (выпускающий редактор), принявший решение об издании информации запретного содержания;

— автор вредного сообщения;

— типография, ответственная за юридическую целостность информации, сюда же относится и сервер размещения;

— распространитель или средство просмотра: провайдер или транспортер.

Примерно по такому же пути пошла и российская судебная практика по делам о защите чести и достоинства граждан и юридических лиц. В отсутствие специального режима ответственности для прессы следует руководствоваться положениями п. 5 постановления Пленума Верховного Суда РФ «О судебной практике по делам о защите чести и достоинства, а также деловой репутации граждан и юридических лиц». В нем устанавливается, что если оспариваемые сведения были распространены в средствах массовой информации, то надлежащими ответчиками являются автор и редакция соответствующего средства массовой информации. Если эти сведения были распространены в СМИ с указанием лица, являющегося их источником, то это лицо также является надлежащим ответчиком. При опубликовании или ином распространении не соответствующих действительности порочащих сведений без обозначения имени автора (например, в редакционной статье) надлежащим ответчиком по делу является редакция соответствующего средства массовой информации, т. е. организация, физическое лицо или группа физических лиц, осуществляющие производство и выпуск данного средства массовой информации. В случае если редакция СМИ не является юридическим лицом, к участию в деле в качестве ответчика может быть привлечен учредитель данного средства массовой информации.

Если истец предъявляет требования к одному из надлежащих ответчиков, которыми совместно были распространены не соответствующие действительности порочащие сведения, суд вправе привлечь к участию в деле соответчика лишь при невозможности рассмотрения дела без его участия (ст. 40 ГПК РФ).

В случае, когда сведения были распространены работником в связи с осуществлением профессиональной деятельности от имени организации, в которой он работает (например, в служебной характеристике), надлежащим ответчиком в соответствии со ст. 1068 ГК РФ является юридическое лицо, работником которого распространены такие сведения. Учитывая, что рассмотрение данного дела может повлиять на права и обязанности работника, он может вступить в дело в качестве третьего лица, не заявляющего самостоятельных требований относительно предмета спора на стороне ответчика, либо может быть привлечен к участию в деле по инициативе суда или по ходатайству лиц, участвующих в деле (ст. 43 ГПК РФ).

Учитывая вышеуказанные положения, если ввести этот специальный режим юридической ответственности (установленный некоторыми странами для прессы) в отношении Интернета, уровни ее наложения можно представить следующим образом.

1. Первым юридическим звеном в цепи здесь будет издатель информации — владелец сайта (он также первым здесь несет ответственность).

2. На втором месте — автор, который может отождествляться с издателем в случае, если издатель издает себя лично, т. е. когда речь идет об индивидуальном издателе (это второй уровень ответственности).

3. На третьем месте находится платформа технического посредничества — хост-провайдер (это третий уровень ответственности).

Вместе с тем здесь не включен в систему ответственности сервис-провайдер, так как его действия ограничиваются только тем, что он приводит в контакт пользователя с Сетью — без осуществления консультированного сервиса и без издательского контроля за содержанием этой информации. Напротив, если говорить о системе общей (неспециальной) юридической ответственности, то ответственность может налагаться и на этих лиц.

Преимущества этой системы следующие:

— жертвы правонарушения всегда будут уверены в том, что смогут найти ответственное лицо. Таким образом, это гарантирует некоторую защиту их прав;

— автоматизм субсидиарной ответственности — на самом деле является простым и известным механизмом, осуществление которого позволит судьям избегать длинных судопроизводств;

— в действительности будут исключены из каскада ответственности сервис-провайдеры и транспортеры (передатчики) информации, они освобождаются от любой редакционной ответственности за исключением случая, если суд докажет обратное.

Неудобства системы таковы:

— если сделать ответственным за распространение противозаконной информации заочно (за неимением выбора) хост-провайдера, есть риск нанести ущерб развитию Интернета. В большинстве случаев владельцы серверов не несут никакой редакционной ответственности по отношению к информации, размещаемой на их технической «площадке». Например, многие серверы, так называемые зеркала, заимствуют информацию, произведенную вне страны, порой даже на другом языке. Такие страницы информации не находятся под контролем владельцев сервера. Большой и существенный риск состоит в том, что часть работы в Сети оставит национальную территорию и переметнется на территории других государств;

— система субсидиарной юридической ответственности с предварительно устанавливаемыми ответственными лицами предполагает исчерпывающее знание об этих субъектах, об их функциях и действиях, т. е. то, что в Интернете до конца невозможно проверить (в том числе из-за высокой скорости процедуры);

— субсидиарная ответственность потребует предварительной фиксации сообщения (послания); в таком случае будет налицо формализм, который должен адаптироваться для открытых сетей (что противоречит его характеру сегодня);

— презумпция невиновности субъекта (лица) может быть поставлена под сомнение, что противоречит принципам построения нашей правовой системы.

Другое предложение состоит в том, чтобы применять к открытым информационно-коммуникационным сетям, таким как Интернет, систему общей (неспециальной) юридической ответственности. Действительно, эти сети ввиду их специфичности (экстерриториальности, децентрализации среды и изменчивости роли ее участников, присутствии в различных секторах экономики) составляют новое информационное пространство, отличное от печати и аудиовизуального распространения. Для такой планетарной инфраструктуры, как Интернет, будет, возможно, нецелесообразным введение особенных юридических правил и процедур, так как противоправные деяния, совершенные в Сети, не только предусматривают наложение юридической ответственности на специалистов, но и касаются любого пользователя.

В этих случаях необходимо учитывать два предложения, которые будут обозначены в § 4 настоящей главы. Кроме того, в определенном порядке все субъекты (автор, издатель, распространитель, хост-провайдер, сервис-провайдер) могли бы преследоваться как главные авторы, соавторы или «сообщники», если, скажем, они сознательно поместили на публичное обозрение незаконную, противоправную информацию, нарушающую интересы граждан и общественный порядок. Соответствующие органы обязаны будут устанавливать их участие в правонарушении и анализировать как смягчающие, так и отягчающие обстоятельства применительно к каждому из участников Сети. Столь гибкое решение позволяет действительно устанавливать реальную ответственность каждого лица за

совершение правонарушения. Оно исходит из принципа презумпции невиновности и будет доказывать виновное намерение субъекта. Такое решение соответствует, конечно, прагматическим и конкретным принципам функционирования Интернета.

Данная система юридической ответственности не будет накладывать на хост-провайдеров, иных распространителей информации обязательство следить априори за сообщениями, циркулирующими в Сети. Вместе с тем если окажется, что после уведомления надлежащих органов они сохранили доступ противозаконной «службы» к Сети и их виновное намерение будет доказано, то данные субъекты будут нести соответствующую ответственность.

Наряду с этим такая система сможет создать среди субъектов положение, согласно которому ни один из них, а также передатчики (транспортеры) не будут априори освобождены от любой ответственности. Такой подход не будет способствовать уходу операторов с национальной территории.

Учитывая идеи, упомянутые выше, кажется, что альтернатива будет носить скорее политический, нежели технический характер. На наш взгляд, предпочтительнее второе решение.

В этой сфере также важно развивать международно-правовое сотрудничество, в том числе и по линии судебных органов.

К тому же мнению пришли участники римско-лионской группы[1]. Министры внутренних дел стран — участниц Большой восьмерки отметили, что противодействие использованию сети Интернет в незаконных целях возможно только при активном международном сотрудничестве и выработке унифицированных международных подходов; необходимо убеждать государства в скорейшей ратификации Конвенции по борьбе с киберпреступностью; противодействие преступности в сфере высоких технологий возможно только при активном сотрудничестве с контент-провайдерами. Участники римско-лионской группы признают, что такое сотрудничество лишь первый шаг.

[1] Помимо министров внутренних дел стран Большой восьмерки в римско-лионскую группу входят представители Австралии, Испании, Швейцарии.

Европейские эксперты в рамках работы ОБСЕ считают важным:

1) активно присоединяться и исполнять международные решения, в первую очередь Конвенцию по борьбе с киберпреступностью. Соблюдать резолюции Совета Европы и решения Интерпола по данному вопросу;

2) разработать кодексы поведения для провайдеров (Code of practice), а также правовые механизмы взаимодействия провайдеров с правоохранительными органами в сфере борьбы с киберпреступностью;

3) создать единый европейский и зональные центры по мониторингу соответствующей информации.

Как мы уже подчеркнули, международное частное право и международное уголовное право уже сегодня предлагают многочисленные решения по вопросу правового регулирования виртуального пространства, информации в Сети. Действительно, общие механизмы выдачи преступника иностранному государству и международной правовой помощи в сфере уголовного права уже сегодня могут применяться в отношении преступлений, совершенных в электронной среде Интернета (по Конвенции о киберпреступности).

Так, в Европе давно уже действуют соглашения о выдаче преступников иностранному государству. Некоторые из них Россия подписала и ратифицировала. Среди них, например, Европейская конвенция о выдаче от 13 декабря 1957 г.[1], Европейская конвенция о взаимной правовой помощи по уголовным делам от 20 апреля 1959 г.[2] До не-

[1] Федеральный закон от 25 октября 1999 г. № 190-ФЗ «О ратификации Европейской конвенции о выдаче, Дополнительного протокола и Второго дополнительного протокола к ней» // СЗ РФ. 1999. № 43. Ст. 5129. Конвенция вступила в силу для Российской Федерации 9 марта 2000 г. Официальный перевод текста Конвенции на русский язык см.: СЗ РФ. 2000. № 23. Ст. 2348.

[2] Федеральный закон от 25 октября 1999 г. № 193-ФЗ «О ратификации Европейской конвенции о взаимной помощи по уголовным делам и

давних пор не существовало детального договора между Россией и США по данному вопросу. Действовало лишь Соглашение от 22 ноября 1935 г.[1] Только 17 июня 1999 г. был подписан Договор между Российской Федерацией и США о взаимной правовой помощи по уголовным делам[2]. Развивая это сотрудничество, следует в ближайшее время подписать еще один специальный договор между Россией и США о взаимной выдаче преступников, который затрагивал бы и сферу Интернета. Это окажет положительное воздействие на рынок интернет-услуг, тем более что некоторые соглашения между государствами вполне состоятельны в вопросах коллизионного права в этой сфере. Например, Конвенция о юрисдикции и приведении в исполнение судебных решений по гражданским и коммерческим делам 1988 г.[3] предоставляет жертве клеветы широкий выбор гражданских процедур, которые позволяют ей защитить свои права. Исполнение судебных решений осуществляется автоматически в странах — участницах данного Соглашения.

Российским юристам еще предстоит выработать свою точку зрения по проблеме юридической ответственности лиц, совершивших правонарушения в мировом виртуальном пространстве и в сфере компьютерной информации, анализируя гл. 28 УК РФ и другие национальные нормы права. Рекомендация Совета Европы от 11 сентября 1995 г. № R (95) 13 относительно проблем уголовных процедур, связанных с технологией обработки информации, могла бы послужить базой для такой правовой работы[1]. Следует подвергнуть всестороннему анализу этот нормативный акт в целях совершенствования отечественной правоприменительной практики в сетях. Вероятно, соответствующие законодательные изменения могли бы быть успешно внесены и в другие международные акты. Скорейшее присоединение России к Конвенции о киберпреступности решило бы многие проблемы в сфере уголовного права, способствовало бы выработке понятийного аппарата теории права и государства. Тем более, как нам представляется, теперь это лишь вопрос времени[2].

Дополнительного протокола к ней» // СЗ РФ. 1999. № 43. Ст. 5132. Конвенция и Дополнительный протокол к ней вступила в силу для Российской Федерации 9 марта 2000 года. Официальный перевод текста Конвенции и Дополнительного протокола к ней на русский язык см.: СЗ РФ. 5 июня 2000 г. № 23. Ст. 2349.

[1] Соглашение в форме обмена нотами между Союзом Советских Социалистических Республик и Соединенными Штатами Америки о порядке исполнения судебных поручений (Москва, 22 ноября 1935 г.) // Сборник действующих договоров, соглашений и конвенций, заключенных СССР с иностранными государствами. Вып. IX. М., 1938. С. 79—84.

[2] Федеральный закон от 3 ноября 2000 г. «О ратификации договора между Российской Федерацией и Соединенными Штатами Америки о взаимной правовой помощи по уголовным делам» // СЗ РФ. 2000. № 45. Ст. 4401.

[3] Текст Конвенции опубликован: Международные конвенции о взаимодействии судов и судебно-правовом сотрудничестве по гражданским и коммерческим делам. (Библиотечка журнала «Вестник ВАС РФ». Специальное приложение к № 10, октябрь 2000 г.). М., 2000. С. 29—64. Российская Федерация в настоящей Конвенции не участвует.

§ 4. Совершенствование законодательства об ответственности в сфере борьбы с киберпреступностью

Сегодня как никогда ранее в интернет-праве актуальна проблема совершенствования законодательства в сфере борьбы с киберпреступностью. Это прежде всего обусловлено тем, что с первого дня существования всемирного виртуального пространства в него стали проникать правонарушители самых разных мастей, в том числе и злостные преступники.

Появляются новые формы и виды преступных посягательств в сфере высоких технологий. Преступники все ча-

[1] См. более подробно: Преступления в сфере компьютерной информации: квалификация и доказывание / Под ред. *Ю. В. Гаврилина*. М., 2003.

[2] Сначала Россия приняла решение подписать Конвенцию о киберпреступности с заявлением. Президент РФ подписал распоряжение от 15 ноября 2005 г. № 557-рп «О подписании Конвенции о киберпреступности» (СЗ РФ. 2005. № 47. Ст. 4929). Однако в марте 2008 г. Россия отказалась поставить свою подпись под этим документом. См.: Распоряжение Президента РФ от 22 марта 2008 г. № 144-рп «О признании утратившим силу Распоряжения Президента РФ от 15 ноября 2005 г. № 557-рп "О подписании Конвенции о киберпреступности"».

ПРОБЛЕМЫ УСТАНОВЛЕНИЯ ЮРИСДИКЦИИ В ИНТЕРНЕТЕ

Кандидат юрид. наук,
юрист московского
представительства фирмы
«Фрешфилдс Брукхаус Деринге» ***В.О. Калятин***

В последнее десятилетие XX в. в мире сформировалась новая среда общественного взаимодействия – глобальная компьютерная сеть Интернет. Одной из особенностей осуществления практически любой деятельности в Интернете является потенциальная возможность выхода за пределы государственных границ, что порождает одно очень распространенное заблуждение: многие уверены в том, что любая активность в сети вообще не подлежит правовому контролю. Внимательное изучение ситуации, однако, показывает, что практически во всех развитых странах все чаще повторяются попытки урегулировать конфликты, связанные с использованием Интернета, с помощью правового инструментария данной страны. Таким образом, конфликт различных юрисдикций становится неизбежным – ведь вследствие глобального характера «всемирной паутины» действия, совершаемые в этой сети, могут затрагивать интересы лиц, находящихся в разных частях мира.

Понятие юрисдикции многозначно. В рамках международного публичного права это понятие означает «сферу суверенной власти государства по законодательству, суду, управлению», в то время как в области международного частного права термин «юрисдикция» употребляется в смысле международной подсудности, т. е. компетенции судебного аппарата данного государства по разрешению определенного рода гражданских дел»[1]. При этом второе значение вытекает из первого: способность судебных органов рассматривать споры является следствием права суверенной власти государства.

Анализируя деятельность с использованием электронных коммуникаций, важно учитывать вероятность того, что она противоречит интересам какого-либо государства в различных областях его ведения. Иначе говоря, наряду с возможностью разрешения судом гражданско-правовых споров необходимо помнить и о возможности применения определенным компетентным органом административного и уголовного законодательства такого государства.

Виды потенциальных конфликтов деятельности, осуществляемой посредством Интернета, с определенным правопорядком многообразны. Так, возможно нарушение документом, помещенным на интернет-сайт, исключительных прав иных лиц, о которых владелец документа может и не подозревать. И даже если этот документ не охраняется авторским правом в стране проживания его владельца, нельзя исключить того, что в какой-то другой стране ситуация прямо противоположная. Столь же вероятно, что обозначения, включаемые в документ, охраняются в иной стране как товарные знаки или знаки обслуживания. Другим примером может быть конфликт содержания документа с законодательством какой-то страны: так, это содержание может рассматриваться как оскорбляющее национальные, религиозные, политические и т. д. чувства граждан. В случаях, когда законодательство какой-то страны допускает патентную охрану методов ведения бизнеса и способов обработки информации, определенная система подачи информации

[1] Лунц Л.А., Марышева Н.И. Международный гражданский процесс. М., 1976. С. 58, 60.

на сайте или способ совершения действий[2] может противоречить патенту, действующему на территории такой страны.

При осуществлении коммерческой деятельности в Интернете круг подобных ситуаций еще шире: наряду с разрешением споров, связанных с заключением и исполнением договоров, могут возникнуть вопросы о нарушении в данной стране законодательства о защите прав потребителей, о необходимости иметь специальное разрешение и лицензию для осуществления какого-то вида деятельности (например, банковских услуг) в стране проживания потенциальных клиентов, о правилах проведения рекламной кампании и др.

Безусловно, нельзя забывать и о возможности признания определенных действий в Интернете уголовным преступлением: вполне легальная в одной стране деятельность может оказаться запрещенной в другой. Так, в штате Юта (США) было возбуждено уголовное дело против лица, продававшего через Интернет алкогольные напитки, в том числе и резидентам этого штата[3].

Важным может оказаться признание судебными органами какого-либо государства отсутствия своей юрисдикции в отношении рассматриваемого спора. В этом случае лицо, хотя и может не бояться судебного преследования, в то же время не вправе рассчитывать на защиту своих интересов в такой стране.

Установление юрисдикции будет влиять определяющим образом и на выбор применимого права. Подходы к решению одинаковых правовых проблем могут настолько различаться в разных странах, что необходимость учитывать требования законодательства определенной страны может совершенно изменить представление лица о перспективах его деятельности.

Но в отличие от ситуации с выбором применимого права вопрос о «выборе» юрисдикции обычно не встает. Судебные органы, как правило, не оценивают возможность другого государства регулировать те же отношения и не определяют, суды какого государства могут рассматривать эти вопросы, а исходят исключительно из внутреннего законодательства, устанавливая пределы своей компетенции, а также возможность привлечения к ответственности иностранных лиц.

Таким образом, при любом использовании Интернета одним из основных вопросов является определение государств, которые по тем или иным причинам могут претендовать на право давать юридическую квалификацию действиям лиц, так или иначе обращающихся к возможностям всемирной сети. Чтобы соответствующий вопрос был поставлен в компетентном органе какой-то страны, необходимо, во-первых, чтобы он в принципе мог рассматриваться этим органом, во-вторых, чтобы данное государство распространяло действие решений своих органов на участников спора. Если первый аспект обычно достаточно четко определен законодательством каждой страны, то в отношении второго ситуация сложнее.

Обычно государство включает в рамки своей юрисдикции помимо своих граждан также лиц, находящихся на его территории. Государство может запретить своим резидентам открытие определенных сайтов в Интернете или осуществление определенных действий через Интернет и, соответственно, привлекать их к ответственности в случае нарушения этих правил независимо от того, на территорию какой страны в реальности были направлены эти действия.

Однако во многих случаях интересы государства легко могут быть затронуты и действиями лиц, находящимися за его пределами. В связи с этим за рубежом достаточно часто встречается разграничение *общей юрисдикции* (юрисдикции над лицами, находящимися на соответствующей территории или осуществляющими на ней систематическую и продолжительную деятельность, независимо от наличия связи рассматриваемой в суде деятельности с территорией) и *специальной юрисдикции* (она применяется, когда деятельность лица, являющаяся предметом спора, прямо направлена на данную территорию; в последнем случае также требуется наличие хотя бы минимальных контактов с такой страной).

В отношении деятельности с использованием Интернета наиболее сложные вопросы связаны с установлением специаль-

[2] Например, способ введения информации о потребителе: так, известный интернет-портал *Amazon.com* обвинил книготорговую фирму *Barnesandnoble.com* в нарушении принадлежащего ему патента на технологию 1-Click (эта технология дает возможность потребителю не вводить данные о своем адресе, номере кредитной карточки и т. п. при последующих покупках).

[3] State of Utah v. Amoroso, 1999 Utah App. Lexis 23.

ной юрисдикции, поскольку в этих случаях речь идет о признании юрисдикции государства над иностранными лицами, не находящимися на территории страны[4]. Оценить наличие связи лица с конкретным государством весьма трудно, поскольку любой материал, размещенный в Интернете, становится одинаково доступным для лиц, находящихся в любой точке земного шара. Применить критерий предвидения (т. е. лицо должно было знать о возможности привлечения к ответственности под определенной юрисдикцией в отношении деятельности в Интернете) не всегда удается, поскольку, с одной стороны, можно предвидеть возможность привлечения к ответственности в любой стране, где есть доступ к Интернету, с другой – реально оценить такой риск лицо не имеет возможности (для этого требуется знать законодательство каждой страны).

Интернет охватывает практически весь мир, а это означает, что определение юрисдикции – не только частная проблема отдельных государств, это общая для всех стран проблема, и решения, принимаемые на территории одной из них, в большинстве случаев способны затронуть интересы других. В таких условиях очень важно иметь представление обо всех многообразных подходах, применяемых в мире. По понятным причинам количество судебных споров, в которых ставилась рассматриваемая проблема, в разных странах неодинаково, поэтому в данной статье судебной практике разных стран уделено различное внимание[5].

В силу специфики передачи информации через Интернет отправитель и получатель взаимодействуют не напрямую, а через ряд посредников, осуществляющих передачу информации на различных участках сети. Возникает вопрос: будет ли передаваемая информация находиться в юрисдикции стран, через территорию которых она передается? Очевидно, что, отвечая на него, необходимо учитывать существенные особенности функционирования Интернета и организации передачи информации *через эту информационную сеть, а именно:* а) соответствующий объем информации передается не единым блоком, а фрагментированно, в виде особым образом сформированных *пакетов*, снабженных данными, позволяющими определить место назначения пересылаемого пакета; б) при передаче информации могут использоваться ресурсы любого фрагмента Интернета в зависимости от работоспособности и загруженности тех или иных соединений; в) конкретный маршрут каждого отдельного пакета заранее неизвестен. Таким образом, каждый пакет может передаваться по различным сетям, минуя те или иные страны, до тех пор, пока не достигнет адресата.

Представляется, что на этапе пересылки нельзя говорить о юрисдикции какого-то государства над движущейся информацией. Ее передача в пределах страны фактически сводится к мгновенному прохождению серии электрических импульсов по определенной линии связи в общем потоке передаваемых сигналов. И если соответствующее звено Интернета просто пересылает «транзитом» соответствующий пакет далее, деятельность упомянутого звена принципиально не отличается от передачи телефонного сигнала при международном звонке. Очевидно, что на отправителя не должна возлагаться ответственность, например, за содержание направленного им адресату документа в случае, если содержание по тем или иным причинам нарушает законодательство одной из стран, через территорию которых передается такая информация.

Нельзя не учитывать и того, что указанная специфика передачи информации присуща Интернету в силу технических особенностей организации этой сети, и попытки устанавливать юрисдикцию на каждом этапе прохождения соответствующего пакета информации способны просто заблокировать работу сети. Поскольку свободное использование средств коммуникации при передаче информации через Интернет является одним из ключевых положений организации всемирной сети, целесообразно было бы разрешить этот вопрос в рамках

[4] Например, согласно п. 3 ст. 12 УК РФ, иностранные граждане и лица без гражданства, не проживающие постоянно в Российской Федерации, совершившие преступление вне пределов Российской Федерации, подлежат уголовной ответственности по настоящему Кодексу в случаях, если преступление направлено против интересов Российской Федерации, и в случаях, предусмотренных международным договором Российской Федерации, если они не были осуждены в иностранном государстве и привлекаются к уголовной ответственности на территории Российской Федерации.

[5] При проверке содержания судебных решений использовались правовая система «Lexis-Nexis», справочные материалы, подготовленные фирмой Perkins Coie LLP., публикации отдельных решений.

международного соглашения об использовании Интернета.

В то же время отсутствие юрисдикции государства над информацией, идущей через его территорию, отлично от юрисдикции государства над соответствующими техническими средствами передачи. Так, в июле 2000 г. в Великобритании был принят закон, прямо разрешающий соответствующим ведомствам этой страны при определенных условиях запрашивать у провайдеров журналы сетевого трафика и перехватывать пересылаемые сообщения[6]. Каждая страна может регулировать передачу сигналов по линиям связи, но содержание пересылаемой информации будет находиться вне ее правового поля.

Теперь обратимся к анализу самих коммуникаций в сфере Интернета. Следует различать два их вида: пересылку определенного объема информации адресату средствами Интернета и открытие доступа к определенной информации в Интернете. Первый вид коммуникаций можно условно назвать активным (поскольку в этом случае отправитель[7] должен совершить некоторые активные действия для того, чтобы адресат получил сообщение), а второй – пассивным (ибо в этом случае отправитель пассивно ожидает, пока потенциальный адресат совершит определенные действия для копирования информации, к которой отправитель открыл доступ). К активным коммуникациям в этом случае можно отнести, например, отправку электронного письма, к пассивным – помещение информации на сайте.

Несмотря на распространенность коммуникаций **активного типа** (так, по данным компании International Data Corp., только электронных писем пользователи Интернета ежедневно отправляют около 10 млрд штук[8]), специфических проблем, связанных с определением юрисдикции, они обычно не вызывают, поскольку такие отношения, осуществляемые через Интернет, по своему характеру близки к традиционным (телефонным переговорам, почтовым отправлениям и т. д.), а для их участников обычно очевидны как личность другой стороны, так и направленность их собственных сообщений. В большинстве случаев определить применимые юрисдикцию и право в таких ситуациях, как правило, довольно легко. Даже когда письмо направляется одновременно большому количеству адресатов, сложностей при определении юрисдикции не возникает, поскольку принципиально эта ситуация не отличается от случая рассылки по почте большого количества бумажных копий письма.

Если лицо занимается продажей товаров или оказанием услуг через Интернет, его клиентами могут оказаться представители разных стран. Поэтому для такого лица важно иметь представление о законодательстве этих стран – всех, где находятся его клиенты, ведь возможные споры будут рассматриваться в местных судах. Конечно, это обстоятельство осложнит деятельность небольшой торговой фирмы, однако проблема вполне разрешима: можно обратиться к помощи специализированных организаций либо просто ограничить список стран, в которые будут поставляться соответствующие товары или где будут оказываться услуги.

Существует определенная область, где риск возникновения сложностей с определением юрисдикции может быть весьма высок и при коммуникациях активного типа. Это случаи, когда отношения предпринимателя и клиента строятся исключительно в пространстве Интернета, не выражаясь в поставках товаров или оказании услуг в «реальном» мире. Так, в виртуальной сфере можно переслать текст запрошенной программы, фильма или аудиозаписи, оказать различного вида консультационные услуги и др. В этих случаях предприниматель может и не знать, из какой страны происходит его клиент. Даже если требовать, чтобы клиент указывал страну своего проживания, проверить эту информацию невозможно. Не сработает в большинстве случаев в отношениях с потребителями (не являющимися предпринимателями) и определение в договоре юрисдикции и применимого права.

Несмотря на то что в данном случае сложности вызваны не столько трудностью *определения применимой юрисдикции*, сколько *риском предоставления клиентом ложной информации* (в результате чего во-

---

6 Regulation of Investigatory Powers Act (2000) (с текстом документа можно ознакомиться на сайте Правительства Великобритании: www.legislation.hmso.gov.uk).

7 Конечно, это лицо можно назвать отправителем лишь условно. Однако для упрощения терминологии в статье будут использоваться термины «отправитель» и «адресат».

8 См., напр.: http://itware.com.ua/news/2000/10/16/email.html.

прос может оказаться в юрисдикции компетентных органов страны, отличной от той, которую предполагал предприниматель), эта проблема будет общей для коммуникаций как активного, так и пассивного типа.

Если электронное письмо выступает лишь как средство пересылки определенной информации в рамках других отношений, существующих за пределами Интернета, то отправителю письма можно посоветовать тщательнее выбирать партнеров или просто избегать этого проблематичного средства общения. Но если бизнес лица базируется на использовании Интернета как средства коммуникации, ситуация сложнее. Проблема предоставления клиентом недостоверной информации о себе присуща всем отношениям в глобальной сети, и эффективных решений пока нет. Видимо, этот вопрос должен быть регламентирован на уровне международных соглашений. Полагаю, справедливым было бы введение правила о действии юрисдикции страны продавца (подрядчика, исполнителя) в том случае, если клиент сообщил продавцу ложную информацию о своем местонахождении и своем гражданстве (при отсутствии умысла или неосторожности со стороны продавца). Национальное законодательство в свою очередь может предусматривать определенные меры ответственности для клиента, сообщившего о себе ложную информацию.

Наибольшие сложности в отношении определения применимой юрисдикции возникают в связи с коммуникациями **пассивного типа**. В таких случаях информация, по сути, адресуется всему миру в целом и никому по отдельности. Такая неопределенность создает возможность для существования самых разных подходов к определению юрисдикции.

Как уже отмечалось, государства устанавливают свою юрисдикцию над лицом, если существует определенная связь между этим лицом и территорией такого государства. Наиболее очевидна связь с территорией при размещении информации на определенном сервере, делающем доступным эту информацию для пользователей Интернета. Понятно, что государство при желании всегда может установить свою юрисдикцию над лицами, хранящими свою информацию на его территории, и будет крайне неразумным для лица, осуществляющего деятельность в Интернете, не учитывать законодательство страны размещения информации. Сказанное вовсе не означает, что другие государства должны отказываться от своей юрисдикции в пользу юрисдикции государства размещения сервера.

Отсылка к юрисдикции *страны размещения сервера* была бы, безусловно, удобна лицу, размещающему соответствующий объект в Интернете, поскольку давала бы возможность не думать о законодательстве «принимающих» стран. Но здесь содержится и существенная проблема: лицо, открывающее доступ к документу, может выбрать наиболее удобную для себя юрисдикцию с минимальным уровнем охраны исключительных прав и отсутствием специального законодательства об Интернете. Так, по аналогичным причинам подверглось критике установление правила о применении «закона государства-участника, из которого происходит услуга» в директиве Совета Европейского Сообщества от 27 сентября 1993 г. № 93/83 о спутниковом вещании и кабельных передачах[9]. Представляется, что в отношении Интернета этот вариант еще более опасен, нежели в отношении спутникового вещания, поскольку, как правило, заинтересованное лицо не всегда в состоянии установить страну размещения сервера, на котором находится соответствующая информация. При этом важно помнить, что страна размещения сервера может не совпадать со страной регистрации доменного имени, причем для владельца доменного имени не составит особого труда заменить один компьютер, использующий в Интернете это доменное имя, другим, находящимся за тысячи километров от первого. Хотя известны случаи, когда суды в своих решениях ссылались на то, что юрисдикция может быть установлена только по месту создания сайта или его нахождения на компьютере провайдера[10], но на практике этот подход используется редко. Более того, в ряде случаев судебные органы прямо признавали, что нахож-

[9] «The act if communication to the public by satellite occurs solely in the Member State where, under the control and responsibility of the broadcasting organization, the programme-carrying signals are introduced into uninterrupted chain of communication leading to the satellite and down to the earth» (Official Journal of the European Communities. No. L. 248/15, 6 October 1993. Art. 1 (2 (b))).

[10] Copperfield v. Cogedipresse, 26 Med. L. Rptr. 1185; (C.D. Cal. 1997).

дения информации на сервере недостаточно для признания юрисдикции по месту нахождения сервера[11].

В литературе предлагался подход, основанный на принципе *национальной принадлежности* (включая «национальную принадлежность» страницы в Интернете)[12]. Так, лицо, создавшее отсылку (link) к странице в Интернете, будет находиться под юрисдикцией своей страны. Юрисдикция над лицом, помещающим данные в Интернете, будет определяться местом нахождения этих данных, а над получающим данные из Интернета – местом нахождения этого лица и т. д. Однако предлагаемый вариант создает много проблем, поскольку реален только при унификации законодательства. Разумеется, каждое государство может устанавливать юрисдикцию над своими резидентами. В то же время, если этот критерий будет воспринят как принцип исключения других юрисдикций, возникнут все уже рассмотренные ранее возможности для злоупотреблений – находясь под удобной для себя юрисдикцией, недобросовестные лица смогут безбоязненно нарушать чужие права. Критерий же *юрисдикции местонахождения данных* аналогичен критерию *юрисдикции страны размещения сервера*, уже рассмотренному нами.

Не всегда действенны в отношении Интернета и традиционные подходы к определению связи лица с территорией. Поскольку помещение материала (в том числе рекламы) в Интернете открывает доступ к нему для потребителей во всем мире, то применение критерия *места деятельности* в чистом виде практически не ограничивает «всемирную юрисдикцию».

Аналогичные проблемы возникают и с применением критерия *места нарушения*. В большинстве случаев «место реального нарушения» совпадает с местом проживания истца, так как обычно проще всего доказать, что именно он в первую очередь испытывает негативные последствия нарушения (особенно в делах об оскорблении, клевете и т. п.). В отношении сферы гражданского права это означает, что любое лицо, нарушающее своими действиями права резидентов данного государства, находится под его юрисдикцией[13]. Этот вариант является очень привлекательным для «принимающих» стран, поскольку позволяет им максимально защитить права своих резидентов. В частности, во Франции суды обычно признают свою юрисдикцию в отношении ответчика, даже находящегося за пределами территории Европейского Сообщества, если истец является французским резидентом. В США даже единственного акта, направленного на территорию штата (в случае, если этот акт и стал причиной подачи иска), бывает достаточно для признания соответствующей юрисдикции.

Однако в этом случае серьезные проблемы возникают уже у лица, распространяющего информацию в Интернете. Здесь речь идет не об установлении критерия, позволяющего заранее определить юрисдикцию, применимую в связи с планируемыми действиями, а об установлении юрисдикции *по результатам* совершенных действий. Нарушит ли определенное действие чьи-то права, можно будет установить заранее только в одном случае – если рассмотреть законодательство всего мира, что явно невозможно.

Еще очевиднее ситуация с применением, например, уголовного или административного законодательства. Вместо того чтобы вначале установить, совершено ли соответствующее действие в пределах юрисдикции страны, и затем уже определять, является ли это действие преступлением или иным правонарушением по законодательству этой страны, приходится рассуждать иначе: если какое-то абстрактное действие может рассматриваться как преступление или правонарушение, находясь в юрисдикции некой страны, то оно и находится в юрисдикции этой страны. Так, была признана юрисдикция Великобритании в отношении действий лица, размещавшего порнографические материалы на сайте в США, на том основании, что он

[11] В одном из дел истец (Steven Rambam) обвинил организацию JDO в распространении в Интернете клеветы о нем. Иск был предъявлен в суд Калифорнии на том основании, что ответчик использовал услуги двух калифорнийских организаций для размещения своего сайта. Было признано, что этого недостаточно для установления юрисдикции (Jewish Defence Organisation v. Superior Court of Los Angeles County, No. B129319, Cal. App. 2d Dist., 1999).

[12] Menthe D.C. Jurisdiction in cyberspace: a theory of international Spaces // Michigan Telecommunication and Technology Law Review. 1997/1998. № 4.

[13] Безусловно, определенные ограничения этого правила так или иначе будут признаваться (например, установление юрисдикции не должно входить в конфликт с принципами справедливости, разумности и т. д., эффект действий лица на данной территории должен быть значительным и т. п.).

передавал материалы на сайт из Великобритании, а также в связи с тем, что полиция смогла загрузить эти материалы, находясь в Великобритании[14].

Этот же подход в ряде случаев использовался в спорах о регистрации доменных имен, совпадающих с товарными знаками иных лиц. Так, в одном из дел ответчик приобрел право на доменное имя, аналогичное товарному знаку истца (INTERNET WORLD), зарегистрированному в Великобритании. Английский суд пришел к выводу о том, что, хотя сайт ответчика размещен в Германии, *юрисдикция над спором может быть установлена в любой стране, где это доменное имя нарушает права на товарные знаки*[15]. Однако территориальная ограниченность действия прав на товарные знаки означает возможность одновременного существования идентичных или схожих товарных знаков в разных странах. Признание нарушением права на товарный знак простого использования схожего наименования в Интернете означало бы искусственное распространение действия прав на этот товарный знак на все страны.

В связи с этим суды, как правило, пытаются установить направленность действий лица, применяющего такое обозначение в Интернете, на использование этого обозначения именно в определенной стране. Так, в одном случае истцу принадлежало право на товарный знак COLORWORKS, зарегистрированный в США, а ответчику – на товарный знак ColorWorks, зарегистрированный в Канаде, причем ответчик зарегистрировал на себя доменное имя *colorworks.com*. Истец полагал, что регистрация такого доменного имени нарушает его права на товарный знак, однако суд признал имеющиеся обстоятельства недостаточными для установления своей юрисдикции над ответчиком – канадской компанией. По мнению суда, для установления юрисдикции над иностранным ответчиком необходимо, чтобы ответчик осуществлял бизнес в Интернете, вступал в контакты с резидентами соответствующей юрисдикции и неоднократно сознательно пересылал этим резидентам соответствующие файлы[16].

Определенной разновидностью рассмотренного подхода является использование критерия доступа к интернет-сайту. Он часто применяется в Германии. Так, в случае, когда немецкая компания обвинила американскую фирму MCN в том, что зарегистрированное MCN доменное имя *concertconcept.com* нарушает права на принадлежащий ей товарный знак, немецкий суд пришел к выводу о том, что условием для признания его юрисдикции может быть доступность интернет-сайта с территории Германии. Ответчику было запрещено использование указанного доменного имени, а также его вариаций[17]. Указанный критерий иногда применяется и в странах англосаксонской системы. Так, в одном из дел[18] юрисдикция суда штата была признана на том основании, что реклама ответчика была постоянно доступна пользователям в каждом штате. О распространении юрисдикции штата на лицо, знающее, что информация, помещенная в Интернете, будет доступна и в этом штате, как об общем правиле заявил в своем меморандуме в 1995 г. Генеральный прокурор штата Миннесота Х. Хамфри.

Данный подход значительно усложняет эффективное использование Интернета. Помимо того что лицо, осуществляющее деятельность в сети, должно учитывать нормы законодательства всех стран, в которых имеется доступ к помещенному в Интернете объекту, заинтересованное лицо получает возможность выбора наиболее удобного для себя суда и правопорядка, что вряд ли можно счесть справедливым.

Риск для лица, осуществляющего деятельность в Интернете при использовании критериев *места нарушения* и *доступа к сайту*, очень велик, и трудно найти способ для его снижения. Малоэффективно, например, требовать от посетителей сайта ответить на вопрос о месте их проживания, с тем чтобы отфильтровывать определенные «нежелательные» страны. Приведем недавний пример. Компания, зарегистрированная на острове Антигуа, организовала сайт с азартными играми «on-line». Все посетители сайта должны были вводить свой адрес, чтобы представителей тех стран, где азартные игры запрещены,

[14] R v. Vaddon; Court of Appeal (Criminal Division), 2000.

[15] Mecklermedia Corp. v. D.C. Congress GmbH, High Court TLR, 1997.

[16] DesktopTechnologies, Inc. v. ColorWorks Reproduction & Design, Inc, 1999 U.S. Dist LEXIS 1934.

[17] 5U 659/97, 97 O 193/96, Landgericht Berlin, 26.05.1997.

[18] Inset Systems, Inc. v. Instruction Set., Inc. 937 F. Supp.161.

не допускать к игре на сайте. Однако один из клиентов, проживая в штате Нью-Йорк (где азартные игры запрещены), указал в качестве места проживания штат Невада и смог получить доступ к игре. Тот факт, что информация, связанная с участием в игре, в реальности передавалась из штата Нью-Йорк, был признан достаточным для установления юрисдикции штата над действиями ответчика[19].

Проблематичность использования указанных критериев становится все более очевидной, в связи с чем суды все чаще уделяют внимание установлению направленности действий лица на определенную территорию. Нужно установить, что нарушение направлено на территорию определенного государства, иначе любая деятельность в Интернете окажется слишком рискованной.

Особое значение установление такой направленности имеет при осуществлении «электронной торговли». Здесь также немало различных подходов. Однако, как правило, в случае признания деятельности с использованием Интернета *бизнесом* риск установления юрисдикции над лицом будет выше, чем при других видах деятельности.

В частности, при установлении специальной юрисдикции суды США обычно пытаются определить выполнение трех условий: а) ответчик должен сознательно направить осуществление бизнеса на соответствующую территорию (при наличии минимальных контактов); б) основание иска должно быть связано с деятельностью ответчика в штате; в) установление юрисдикции должно быть достаточно справедливо. Однако эти ориентиры не всегда помогают на практике. Понятия «осуществление бизнеса», «минимальные контакты», «справедливость установления юрисдикции» и т. п. очень расплывчаты и в каждом конкретном случае трактуются по-своему.

По делу Schweers v. Hovaten суд признал, что интернет-сайт, содержащий общую информацию, не направлен именно на резидентов штата Нью-Мексико и не указывает на намерение ответчика заниматься бизнесом в этом штате. При рассмотрении других дел указывалось, что одной лишь рекламы, не предназначенной непосредственно для жителей определенной территории, недостаточно для установления юрисдикции суда[20]. В отношении спора Pres-Kap, Inc. v. System One, Direct Access, Inc.[21] суд заявил, что наличия двух клиентов на территории штата Флорида недостаточно для признания юрисдикции штата над ответчиком. Но 22 случая продажи товаров ответчика резидентам штата уже стали основанием для установления юрисдикции[22]. В другом случае решающими фактами послужили концентрация рекламы на штате Коннектикут, а также соглашение ответчика с одним из агентств путешествий этого штата об оказании услуг клиентам ответчика, проживающим в этом штате[23].

Достаточным уровнем контактов сторон может быть признано наличие электронных коммуникаций между ними. В споре Plus system, Inc. v. New England Network, Inc.[24] стороны договорились проводить электронные расчеты через специальную платежную систему, управляемую истцом. Юрисдикция суда была признана по местонахождению центрального компьютера этой платежной системы (штат Колорадо, США). В качестве достаточных оснований для признания юрисдикции рассматриваются рассылка потенциальным клиентам рекламных материалов, образцов товаров и т. п., поддержание контактов с посетителями сайта (включая заключение с ними договоров), указание на сайте списка событий, специально отобранных, чтобы заинтересовать посетителей, живущих на определенной территории, и др.

Естественно, что в случае комбинации нескольких факторов вероятность признания соответствующей юрисдикции значительно возрастает.

Общий подход, используемый в США, был продемонстрирован в деле Zippo Manufacturing Co. v. Zippo Dot Com Inc.[25] Исходя из критериев интерактивности и направленности действий лица, можно выделить три ключевых варианта: а) в случае активного бизнеса в Интернете юрисдикция суда, в который обратился истец, скорее

[19] State of New York v. World Interactive Gaming Corp., 1999 N.Y. Misc LEXIS 425, Sup. Ct. N.Y. Cty.

[20] Например, Cybersell, Inc. v. Cybersell, Inc. 1997 U.S. App. LEXIS 33871 (130 F.3d 414).

[21] 636 So. 2d 1351, 1994 Fla. App. LEXIS 3364.

[22] International Star Registry of Illinois v Bowman-Haight Ventures, Inc, 1999 U.S. Dist. LEXIS 7009.

[23] Nancy Gates v. Royal Palace Hotel et al., 1998 Conn. Super. LEXIS 3740, Rockville Super.

[24] 804 F. Supp. 111, 1992 U.S. Dist. LEXIS 15768.

[25] 952 F Supp. 1119, 1997 U.S. Dist. LEXIS 1701.

всего будет признана; б) в случае создания интерактивного сайта, способного обмениваться информацией с посетителями сайта, юрисдикция суда зависит от уровня интерактивности и коммерческой (или некоммерческой) природы сайта; в) в случае, если сайт просто используется для пассивной информации потенциальных клиентов, юрисдикция такого суда скорее всего не будет признана.

Можно отметить, что, с одной стороны, такой подход создает серьезные затруднения для развития «электронной коммерции» (поскольку опять возвращает всех лиц, участвующих в электронной коммерции, к принципу «всемирной юрисдикции»), а с другой – так и не решает вопрос о том, как установить надлежащую для разрешения спора юрисдикцию.

В некоторых случаях при осуществлении «электронной коммерции» может использоваться договорное определение вопросов юрисдикции, применимой к возможным спорам сторон, в виде соглашений о выборе конкретной юрисдикции (прерогационные соглашения) или об исключении какой-либо юрисдикции (дерогационные соглашения). Однако такие соглашения зачастую не признаются; в любом случае положения в договоре о выборе юрисдикции скорее всего будут признаны не подлежащими применению в отношениях с потребителями.

Более того, одной из серьезнейших проблем, возникающих при осуществлении «электронной торговли», стало право потребителей подавать иски в странах своего проживания. Такая возможность, в частности, существует для резидентов стран – членов Брюссельской конвенции по вопросам юрисдикции и принудительного исполнения судебных решений в отношении гражданских и коммерческих споров 1968 г. Статья 13 данной конвенции предоставляет потребителям выбор между юрисдикциями своей страны и страны продавца. Но сложность осуществления «электронной коммерции» при возможности применения критерия *места проживания потребителя* стала очевидной, в результате чего вероятность использования этого критерия будет постоянно снижаться.

Особая ситуация с определением юрисдикции существует в отношении споров по поводу доменных имен. Помимо рассмотренных к таким спорам может применяться и критерий *национальной принадлежности домена*. Учитывая стремление различных государств установить свой контроль над регистрацией доменных имен в соответствующем национальном домене, такой подход представляется вполне логичным. Известны и судебные решения, при принятии которых был применен этот критерий. Так, в споре о «захвате» доменного имени epson.de лицом, единственной целью которого была перепродажа этого доменного имени одноименной корпорации, немецкий суд признал, что юрисдикция в отношении споров о доменных именах, входящих в домен *.de*, существует «повсюду в Германии»[26]. В отношении доменов верхнего уровня (*com.*, *org.*, *edu.* и др.) заметно стремление США установить свою юрисдикцию.

Таким образом, существует множество критериев, применяемых при выборе юрисдикции. Для лица, использующего Интернет, такая ситуация оборачивается существенным риском, поскольку трудно заранее определить правопорядок, который может затронуть деятельность в сети. Однако оценка вероятности установления определенных юрисдикций все же должна производиться. В некоторых случаях стоит подумать о прямом ограничении ведения бизнеса с определенными странами, включая помещение соответствующего предупреждения на сайте.

В любом случае наиболее опасным представляется отношение к Интернету как к средству обхода какого-то правопорядка. Характерный пример: с целью избежать конфликта с российским законодательством (поскольку деятельность, связанная с разработкой, производством, реализацией и эксплуатацией шифровальных средств на территории России, должна быть лицензирована ФАПСИ[27]) Microsoft начал поставку в Россию операционной системы Windows 2000 с удаленными возможностями шифрования передаваемой через Интернет информации. В то же время глава российского представительства этой фирмы О. Дергунова успокоила всех потенциальных пользова-

[26] См.: www.online-recht.de.

[27] См., напр., ст. 17 Федерального закона № 158-ФЗ «О лицензировании отдельных видов деятельности», п. 4 Указа Президента РФ от 3 апреля 1995 г. «О мерах по соблюдению законности в области разработки, производства, реализации и эксплуатации шифровальных средств, а также предоставления услуг в области шифрования информации».

телей этой программы: с сайта Microsoft можно загрузить специальное дополнение, которое восстановит в купленной программе удаленный фрагмент[28]. Естественно, что такой вариант правомерен только в том случае, если предоставление программы через Интернет будет находиться вне российской юрисдикции.

Очевидно, что решение проблемы определения применимой юрисдикции к деятельности, связанной с использованием Интернета, может быть достигнуто только при согласовании различными странами применяемых критериев. Представляются возможными следующие пути.

Во-первых, заключение международного соглашения об определении вопросов юрисдикции в отношении деятельности с использованием сети Интернет (подобного Брюссельской или Луганской конвенциям о выборе юрисдикции[29]). Такое соглашение может закрепить выбор определенной юрисдикции для каждого из наиболее распространенных типов отношений (отношений с потребителями, отношений в области предпринимательской деятельности, отношений, связанных с использованием различных объектов исключительных прав, и т. д.).

Во-вторых, частичное устранение проблем возможно путем унификации материального законодательства (например, с помощью международных соглашений). Действительно, если, например, произведения науки, литературы и искусства гражданина страны, присоединившейся к Бернской конвенции об охране литературных и художественных произведений, на относительно приемлемом уровне охраняются во всех странах – членах этой конвенции, то вопрос выбора юрисдикции будет уже значительно менее принципиальным для автора. Однако такой подход способен лишь смягчить, но не полностью устранить проблему, поскольку в связи с неизбежными различиями в законодательстве разных стран неопределенность в правовой оценке соответствующих действий сохранится.

В-третьих, способом смягчения проблемы выбора юрисдикции может стать заключение международного соглашения, определяющего применимое право к различным ситуациям, возникающим в связи с использованием Интернета. Если суд должен применить, например, право страны нахождения сервера, поддерживающего определенный сайт, то проблема определения суда, компетентного применить это право, станет менее важной. В то же время эффективная реализация данного варианта возможна только при унификации законодательства разных стран, иначе недобросовестное лицо всегда сможет заранее подобрать для себя наиболее удобное право.

Наконец, четвертое предложение, в определенном смысле объединяющее некоторые черты указанных ранее подходов, состоит в создании специального международного правового режима для Интернета. Данный способ представляется достаточно сложным, однако некоторый опыт уже имеется: достаточно вспомнить специальные правовые режимы мирового океана, Антарктики, космического пространства. В частности, широко распространено мнение о том, что, чем, например, изменять Брюссельскую конвенцию о юрисдикции, приспосабливая ее к нуждам электронной коммерции, проще, дешевле и эффективнее будет создать альтернативный механизм для разрешения споров. Возможно установление постоянно действующего арбитража с централизованной юрисдикцией[30].

Во всех перечисленных случаях решить проблему определения юрисдикции в отношении деятельности в Интернете невозможно без определенных согласованных действий разных стран. Очевидно, что достичь консенсуса на международном уровне всегда непросто, однако ясное осознание проблемы и ее верная постановка –

[28] Нефедов П. Windows 2000 – в продаже // Ведомости. 2000. 18 февраля.

[29] Эти конвенции, к сожалению, малоэффективны в отношении деятельности в Интернете.

[30] См., напр.: Martyr C. The European Commission's Public Hearing on E-Commerce // World Internet Law Report. 1999–2000. No. 12-1. P. 30.

Л.В. Терентьева
Преподаватель кафедры международного частного права МГЮА им. О.Е. Кутафина, кандидат юридических наук

Сетевое пространство и государственные границы: вопросы юрисдикции в сети Интернет

Сложности определения международной юрисдикции в сети Интернет обусловлены трансграничным характером сети и ограниченной территориальной компетенцией государств. Анализ российского законодательства показывает, что за рамками юрисдикции — главного атрибута суверенитета государства, осталось сетевое пространство. Вседоступность информации, размещенной в сети Интернет, объективно приводит к необходимости расширения оснований юрисдикции судов РФ. Критерии подсудности должны быть сформулированы таким образом, чтобы исключалась возможность установления юрисдикции, базируясь только на основании доступности размещенной информации в сети Интернет. Желаемым вариантом разрешения юрисдикционного вопроса в отношении споров в сети Интернет могли бы стать региональные конвенции в области гражданского процесса государств, национальное законодательство которых не отличается друг от друга коренным образом.

Ключевые слова: международная юрисдикция; суверенитет; территория государства; Конституция Российской Федерации; сеть Интернет; сетевые границы; доменные имена; критерии подсудности; тесная связь спорного правоотношения с территорией РФ; персональная юрисдикция

Рост общественных отношений, складывающихся в сети Интернет, и необходимость их правовой регламентации повлекли за собой объективную необходимость критического анализа адекватности правового инструментария, которым располагают на сегодняшний день различные отрасли права.

В подавляющем большинстве работы специалистов сконцентрированы на проблемах интеллектуальной собственности в Сети, ведения коммерческой деятельности, киберсквотерства, диффамации. Вопрос установления юрисдикции в сети Интернет в основном не подвергался детальному исследованию, за исключением ряда работ[1]. В литературе были озвучены предложения о необходимости

[1] *Наумов В.Б.* Проблема юрисдикции сети Интернет // Информационная безопасность регионов России. Т. I. СПб., 1999; *Калятин В.О.* Право в сфере Интернета. М., 2004; *Кемрадж А.С.* Правовые аспекты использования интернет-технологий. М., 2002.

заключения международных договоров, определяющих статус международного информационного пространства и фиксирующих соответствующие коллизионные нормы определения применимого права[2]. Кроме того, представлены позиции о необходимости скорейшей разработки и принятии международной конвенции, которая установила бы зоны национальной юрисдикции в Интернете по аналогии, например, с Арктикой, космическим пространством, Луной и другими небесными телами[3]. Возможность интернет-ресурса затрагивать интересы любых лиц в любой точке земного шара, трансграничный характер Сети и ограниченная территориальная компетенция государств ставит законодателя перед необходимостью решать вопросы определения юрисдикции государства вообще и определения судебной юрисдикции в частности.

В Конституции РФ суверенитет, предполагающий верховенство, независимость и самостоятельность государственной власти распространяются на территории Российской Федерации. Реализация отношений в Сети вне связи с определенной территорией и территориальный суверенитет государства, провозглашенный в Конституции РФ, обнаруживает, что за рамками юрисдикции, главного атрибута суверенитета государства, осталось сетевое пространство. Учеными обозначено, что проблема юрисдикции отношений в сети Интернет обусловлена деятельностью провайдеров (информационных посредников) и потребителей информации, осуществляемой вне территории Российской Федерации[4].

Конституция РФ в ст. 67 включает в территорию Российской Федерации территорию ее субъектов, внутренних вод, территориальных морей и воздушного пространства над ними. В теории международного права под территорией понимают пространственную сферу действия государственного суверенитета, сферу территориальной юрисдикции государства, часть географической среды, материальную основу существования общества[5]. Интернет не имеет каких-либо материальных и физических границ. В связи с этим представляется важным, чтобы сфера и пределы суверенной власти государства в отношении сетевого пространства были также отражены в Основном законе РФ.

На сегодняшний день наиболее адекватным решением юрисдикционной проблемы в сети Интернет представляется ограничение компетенции государства национальными доменными именами. Данное положение некоторым образом реализовано в п. 1 ст. 247 АПК РФ, указывающего, что арбитражные суды рассматривают дела с участием иностранных лиц, если спор возник из отношений, связанных с государственной регистрацией имен и других объектов и оказанием услуг в международной ассоциации сетей Интернет на территории РФ. В литературе отмечались неточности этого положения: государственная регистрация имен

[2] *Наумов В.Б.* Право и Интернет. М., 2003.

[3] *Федотов М.А.* Конституция как символ доцифровой эпохи. http://www.unescochair.ru/content/view/237/8/ (последнее посещение — 25 ноября 2008 г.); *Дашян М.С.* Право информационных магистралей (Law of information highways): вопросы правового регулирования в сфере Интернет. М., 2007.

[4] *Ловцов Д.А., Верхоглядов А.А.* Информационная безопасность судебных автоматизированных систем: правовое регулирование и юрисдикция // Информационное право: Сборник научных трудов. М., 2007.

[5] *Лукашук И.И.* Международное право. Особенная часть. М., 2005; *Тункин Г.И.* Международное право. М., 1994; *Бекяшев К.А.* Международное публичное право. М., 1998.

в России и большинстве других стран не осуществляется, так как данная функция преимущественно реализуется негосударственными организациями[6]. Кроме того, неоднозначен термин «международная ассоциация сетей Интернет», который не определен ни в одном законодательном акте.

В зарубежной литературе также рассматривалась возможность отнесения спора, вытекающего из отношений в сети Интернет, к юрисдикции того государства, в котором зарегистрировано доменное имя[7]. Например, российский сегмент (сектор) сети Интернет в национальном домене «.ru» должен соответственно подпадать под российское законодательство[8]. Здесь стоит отметить, что в Российской Федерации домен «.ру» является открытым и регистрация доменных имен осуществляется в заявительном порядке как резидентами, так и нерезидентами. На данный момент в российском домене зарегистрировано около 1,4 млн имен. 97% доменов второго уровня в «.ru» зарегистрировано российскими организациями и гражданами; и только 3% имен принадлежат нерезидентам, которые, впрочем, используют их для ресурсов, ориентированных на рынок России[9]. Как представляется, на использование нерезидентами доменов второго уровня в зоне «.ru» должна также распространяться юрисдикция РФ.

Что касается функциональных доменов (к ним относятся такие имена, как «.com», «.org», «.int»), то здесь целесообразно использовать привязку национальной принадлежности органа, который сертифицирует домен.

Помимо определения юрисдикции государства, представленного в широком смысле как вытекающая из суверенитета государства законодательная, судебная, административная власть, существует термин «судебная юрисдикция». В каждой стране своя судебная система и установление государством юрисдикции своих судов — вопрос суверенитета. Термин «судебная юрисдикция» является логическим продолжением понятия юрисдикция и означает полномочие государства распространять на определенных лиц действие национальной судебной системы. В статье 47 Конституции РФ сформулировано субъективное право каждого об определении подсудности дел законом. В законе должны быть закреплены критерии, которые в нормативной форме (в виде общего правила) заранее, т.е. до возникновения спора или иного правового конфликта, предопределяли бы, в каком суде подлежит рассмотрению то или иное дело[10]. В международном частном праве проблемы выбора надлежащего суда и определения судебной компетенции в отношении дел с участием иностранных лиц приобретают особую значимость.

Вопросы международной юрисдикции разрабатываются преимущественно на национальном уровне. Правила, по которым решаются вопросы международной юрисдикции во внутренних законах различных государств, индивидуальны, но они

---

[6] *Петровский С.В.* Проблемы судебного правоприменения в сфере сети Интернет // Информационное право; *Калятин В.О.* Право в сфере Интернета. М., 2004.

[7] *David R. Johnson.* Law And Borders — The Rise of Law in Cyberspace // Stanford Law Review. 1996. P. 34.

[8] Первым доменом отечественного Интернета по первым буквам названия страны стал «.su» еще в 1990 г. В 1994 г. России был присвоен домен «.ru».

[9] http://www.flomaster.ua/blog/rubrics/4?page=4 (последнее посещение — 5 декабря 2008 г.).

[10] Постановление Конституционного Суда РФ от 25 февраля 2004 г. № 4-П // СЗ РФ. 2004. № 9. Ст. 831.

могут быть сведены к некоторым типовым системам международной юрисдикции: по признаку гражданства сторон или стороны в деле (Франция, Бельгия, Италия, Алжир); по признаку места жительства ответчика или места нахождения юридического лица (Германия, Россия); по признаку личного присутствия ответчика или принадлежащего ему имущества на территории данного государства (Англия). Все указанные основные критерии установления юрисдикции базируются на физической связи с территорией.

По мнению Т.Н. Нешатаевой, критерии подсудности споров по месту нахождения или месту жительства ответчика, предусмотренные в ст. 35 АПК РФ и 28 ГПК РФ, достаточно широко определяют компетенцию российских судов и являются достоинством российского закона[11]. Автор полагает, что законы иностранных государств содержат более узкие критерии: закон гражданства ответчика (Франция, Италия), фактическая возможность вручения ответчику приказа о вызове в суд (Англия), волеизъявления судьи о приемлемости спора (США). Т.Н. Нешатаева также указывает, что не всегда можно определенно установить критерий места жительства ответчика, закрепленный в Брюссельской конвенции 1968 г. о юрисдикции и принудительном исполнении иностранных судебных решений по гражданским и коммерческим делам.

Указанные критерии вызывают дополнительные трудности при разрешении споров, вытекающих из отношений в сети Интернет. Фактор физического присутствия или физической досягаемости ответчика теряет для суда свою значимость, поскольку нарушение законов государства может происходить без проникновения на территорию самого государства. Определение подсудности по критерию гражданства и места жительства или по критерию места нахождения может обнаружить отсутствие связи государства с правоотношением, локализованным в сети Интернет.

В то же время сложно согласиться с точкой зрения, что основания компетенции российских судов, перечисленные в ГПК РФ, определены достаточно широко. Суды в РФ вправе рассматривать дела с участием иностранных лиц в случае, если:

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

2) ответчик имеет имущество, находящееся на территории РФ;

3) по делу о взыскании алиментов и об установлении отцовства истец имеет место жительства в РФ;

4) по делу о возмещении вреда, причиненного увечьем, иным повреждением здоровья или смертью кормильца, вред причинен на территории РФ или истец имеет место жительства в РФ;

5) по делу о возмещении вреда, причиненного имуществу, действие или иное обстоятельство, послужившие основанием для предъявления требования о возмещении вреда, имело место на территории РФ;

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

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

[11] *Нешатаева Т.Н.* Международное частное право и международный гражданский процесс. М., 2004.

8) по делу о расторжении брака истец имеет место жительства в РФ или хотя бы один из супругов является российским гражданином;

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

Как представляется, перечисленные основания компетенции суда, основанные на критериях «место нахождения», «место причинения вреда», «место исполнения», также неоднозначно будут решать проблемы юрисдикции в сети. Местом причинения вреда путем размещения информации на интернет-сайте может быть любое государство, с территории которого осуществлен доступ на соответствующий сайт. Также сложно определить место исполнения договора, заключенного и реализованного в сети Интернет. Традиционные принципы не являются адекватными для установления международной юрисдикции применительно к правоотношениям в сети Интернет, и, соответственно, необходимо расширять основания международной юрисдикции в отношении данной категории дел.

Более широко представлен перечень оснований юрисдикции арбитражных судов в ст. 247 АПК. Перечень критериев подсудности арбитражных судов наряду с такими традиционными основаниями, как «место нахождения ответчика», «место исполнение договора», «место причинения вреда», дополнен таким критерием, как наличие тесной связи спорного правоотношения с территорией РФ. Данный критерий дает возможность установления судебной компетенции в отношении лиц, находящихся вне территории государства суда, и некоторым образом перекликается с правилами подсудности дел американским судам.

Так, для того чтобы суды штатов могли рассматривать споры с участием иностранных лиц, в том числе, когда истец предъявляет иск иностранному ответчику, он должен обладать судебной юрисдикцией (judicial jurisdiction), или, как ее еще называют, персональной юрисдикцией (personal jurisdiction)[12]. Под судебной, или персональной, юрисдикцией понимают полномочия соответствующего суда рассматривать и разрешать исковые требования против иностранных лиц (foreign persons) или их собственности. Персональная юрисдикция представляет собой географическое ограничение, налагаемое на право суда вызывать ответчиков в суд для защиты своих прав. Для осуществления персональной юрисдикции необходимо соблюдение правила «длинной руки» (long-arm statutes). В соответствии с данным правилом суды могут осуществлять юрисдикцию, основанием которой являются специфические («минимальные») контакты, т.е. правоотношения, установленные между ответчиком и штатом, в котором предъявлен иск[13].

В законодательстве США не дается определение общего понятия «статут длинной руки». Впервые указанные принципы были сформулированы в решении Верховного суда США по делу International Shoe v. Washington, в котором Верховный суд расширил персональную юрисдикцию за физические границы своей территории. Правило минимальных контактов может быть проиллюстрировано на примере судебного дела американской компании Adobe Systems против российской компании «Элкомсофт». Компания «Элкомсофт» реализовывала программу Advanced

[12] Федеральные правила гражданского процесса (Federal Rules of civil Procedure) от 1935 г. с послед. изменениями и дополнениями 1989 г.

[13] *Белов А.П.* Разрешение внешнеэкономических споров в судебном порядке // Право и экономика. 2001. № 4. С. 32.

eBook Processor (AEBPR), позволяющую снимать защиту с электронных книг, что нарушало действующий в США Digital Millennium Copyright Act (DMCA), название которого переводится как «Авторское право в цифровом тысячелетии». Соответствующая программа, не нарушавшая законодательство РФ, была выложена на сайте, что послужило основанием обращения американской компании в суд штата Калифорния, который принял иск к рассмотрению.

Как представляется, столь широкое толкование юрисдикции на основании критериев «правила минимальных контактов» и «наличия тесной связи» в отношении споров в сети Интернет может вылиться в проблему мультиюрисдикции, когда в отношении одного дела будут признавать себя компетентными несколько судов. Суд может установить свою компетенцию в отношении любого субъекта, разместившего информацию в сети Интернет, к которой имеется доступ. Здесь показательно дело Британской ассоциации звукозаписывающей индустрии (BRI) против компании «Медиа Сервисиз» — владельца российского сайта Allofmp3.com. Основанием компетенции английского суда послужил довод, что пользователи в Соединенном Королевстве, скачивающие музыку с российского сайта allofmp3.com, нарушают британские законы об авторских правах, так как у этого сайта нет лицензии на продажу записей. При этом сайт содержит информацию, призывающую пользователей удостовериться в том, что они не нарушают законы своей страны, загружая или скачивая те или иные файлы в формате mp3. Содержащиеся на сайте материалы доступны для распространения по Интернету в соответствии с лицензией Российского общества по мультимедиа и цифровым сетям (РОМС). Таким образом, несмотря на то, что ответчик и информационный ресурс находятся вне Великобритании, а юрисдикция английских судов определяется посещаемостью сайта гражданами соответствующего государства. Кроме того, французская фонографическая ассоциация также обратилась в суд парижского пригорода Нантерр с иском против компании «Медиа Сервисиз» — владельца соответствующего информационного ресурса.

Как показывает зарубежная судебная практика, вседоступность информации, размещенной в сети Интернет, объективно приводит к необходимости расширения оснований юрисдикции судов РФ не только в АПК, в котором сформулирован критерий тесной связи, но и судов общей юрисдикции. В то же время критерии подсудности должны быть сформулированы таким образом, чтобы исключалась возможность установления юрисдикции, базируясь только на основании доступности размещенной информации в сети Интернет. Идеальным вариантом разрешения юрисдикционного вопроса в отношении споров в сети Интернет мог бы стать международный договор, унифицирующий соответствующие правила подсудности. Но, учитывая сложности заключения универсальных международных договоров в области гражданского процесса, решением проблемы могли бы стать региональные конвенции государств, национальное законодательство которых не отличается друг от друга коренным образом.

Контактные данные автора: 8-929-618-83-26
terentevamila@mail.ru

УДК 347:681.324 + 342.951:681.324
ББК 67.401 + 67.404 + 67.99(2)3
Н 34

Научный редактор
д. ю. н., проф. В. Б. Исаков

Рецензенты:
д. ю. н., проф. С. В. Запольский,
к. ю. н., проф. В. Н. Монахов

Наумов В. Б.
Н34 Право и Интернет: Очерки теории и практики. — М.: Книжный дом «Университет», 2002. — 432 с.: ил.

ISBN 5-8013-0155-0

Книга представляет собой отдельные очерки, в которых затрагиваются теоретические и практические аспекты проблем правового регулирования сети Интернет в России. В качестве предмета для анализа выбраны проблемы юрисдикции сети Интернет и ответственности информационных провайдеров, распространения массовой информации и спама, защиты персональных данных при работе в сети Интернет; исследованы вопросы защиты авторских прав и проанализирован статус доменного имени. В книге дан обзор инициатив, связанных с регулированием сети Интернет в России, и рассмотрены предметная российская судебная практика и статус доказательств в спорах, связанных с использованием сети Интернет.

Книга предназначена для практикующих юристов, журналистов, студентов юридических факультетов и факультетов журналистики, руководителей организаций всех форм собственности, аналитиков в сфере информационных технологий и государственных служащих, интересующихся или по долгу службы занимающихся вопросами развития сети Интернет в России и за рубежом.

УДК 347:681.324 + 342.951:681.324
ББК 67.401 + 67.404 + 67.99(2)3

ISBN 5-8013-0155-0

© Наумов В. Б., 2002



Краткая характеристика ключевых проблем регулирования сети Интернет

К ключевым проблемам правового регулирования общественных отношений, возникающих в связи с использованием сети Интернет, можно отнести три:

— проблему юрисдикции отношений в сети Интернет;
— проблему ответственности информационных провайдеров (посредников);
— проблему разработки и реализации инициатив в сфере саморегуляции отношений в сети Интернет.

Они являются теми критериями, которые определяют состояние решения любой проблемы в сфере правового регулирования информационного пространства и сервисов сети Интернет.

Неслучайно по сути в первом международном соглашении, посвященном регулированию отношений в сети Интернет — в Convention on Cybercrime (ETS n: 185)[1], подписанной 23 ноября 2001 года в Будапеште большинством стран-членов Совета Европы, а также США и Японией[2], определению юрисдикции посвящена отдельная статья[3], а термин «провайдер»[4] встречается в тексте Convention on Cybercrime повсеместно.

---

[1] См. текст Конвенции по адресу http://conventions.coe.int/.

[2] На начало февраля 2002 года Конвенция не была ратифицирована ни одним из подписавших государств.

[3] Art. 22.

[4] Точнее, «service provider», которого Конвенция определяет как «any public or private entity that provides to users of its service the ability to communicate by means of a computer system, and any other entity that processes or stores computer data on behalf of such communication service or users of such service» (Art.1c).

В настоящем разделе будет дана краткая характеристика названных проблем. В последующих же разделах книги будут приводиться всевозможные конкретные решения, определяющие регулирование отношений с иностранными элементами, характер и степень ответственности лиц, оказывающих услуги по распространению, доступу и размещению информации в сети Интернет, а также будут рассматриваться предметные инициативы общественных и коммерческих организаций, стремящихся в рамках механизмов саморегулирования упорядочить использование сети Интернет.

Любое государство и любой человек хочет быть хозяином в своем доме. Для государств это естественное желание обеспечивается принципами международного права, принципом государственного суверенитета, заключающимся в верховенстве, самостоятельности и независимости государственной власти, и принципом невмешательства во внутренние дела других государств. Для личности — международным и национальным законодательством, гарантирующим всем известные права человека и гражданина.

Последнее десятилетие глобальное информационное пространство, существующее, в первую очередь, в виде сети Интернет и возникшее в результате интернационализации общественных отношений и научно-технического прогресса, заставляет пересматривать границы дома и объем прав и обязанностей хозяина. Кроме того, часть пользователей, проповедуя «экстерриториальность» Сети, декларирует свою независимость от государств и закона и борется за свою «суверенную Сеть».

Как же выглядят информационные общественные отношения, возникающие при использовании Интернета (в терминах отечественного законодательства в сфере информатизации[1])?

Упрощенно цепочку информационных общественных отношений в терминах можно представить следующим образом: пользователь (потребитель) — информационный ресурс — собственник (владелец ресурса)[2]. При этом в существующей общественно-правовой ситуации

---

[1] Обзор такового законодательства приводится в Приложениях.

[2] Федеральный Закон Российской Федерации от 20 февраля 1995 года № 24-ФЗ «Об информации, информатизации и защите информации» определяет данные понятия следующим образом:

каждый из элементов находится в сфере юрисдикции определенной страны мира. Понимая, что для каждого элемента цепочки отношения существует свой собственный правовой режим, имеем в общем случае три варианта правового регулирования: регулирование отношений по законодательству страны проживания пользователя, страны местонахождения ресурса и по законодательству страны собственника.

На самом же деле приведенная схема весьма условна и не учитывает тот факт, что цепочка информационных общественных отношений, выстраивающаяся в процессе использования Сети, имеет не *три*, а *минимум пять элементов* (см. рис. 1), в число которых входят лица, оказывающие услуги по доступу, размещению и распространению информации в сети Интернет и называемые информационными провайдерами (посредниками)[1].

Рассмотренная многомерность информационных общественных отношений вполне закономерно представляет собой источник растущего клубка общественно-правовых противоречий. Регулировать эти противоречия и конфликты в связи с эксплуатацией Сети пользователями, собственниками и хозяевами серверов хостинга из разных стран мира пытаются уже сейчас.

Основными источниками права, регулирующего общественные отношения, являются международные договора, национальное законодательство, судебная практика и обычаи, формирующиеся в процессе реализации тех или иных общественных отношений.

«собственник информационных ресурсов, информационных систем, технологий и средств их обеспечения — субъект, в полном объеме реализующий полномочия владения, пользования, распоряжения указанными объектами;

владелец информационных ресурсов, информационных систем, технологий и средств их обеспечения — субъект, осуществляющий владение и пользование указанными объектами и реализующий полномочия распоряжения в пределах, установленных Законом;

пользователь (потребитель) информации — субъект, обращающийся к информационной системе или посреднику за получением необходимой ему информации и пользующийся ею» (ст. 2 закона).

[1] Следует обратить внимание на одну любопытную деталь: в определении понятия пользователя в ст. 2 закона «Об информации, информатизации и защите информации» упоминается термин «посредник», но далее ни в этом акте, ни в других предметных законах сферы информатизации не приводится ни определений, ни прав и обязанностей данного субъекта информационных отношений.

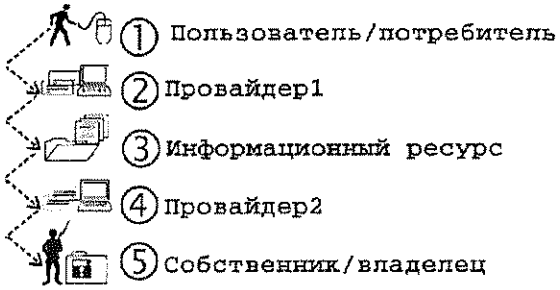


Рис. 1. Схема общественных отношений, возникающих в связи с использованием сети Интернет

В настоящее же время несколько десятков стран имеют зачатки национального законодательства, касающегося использования глобального информационного пространства. Международные соглашения по этому вопросу отсутствуют, обычаи использования Сети весьма противоречивы — а значит, спорных ситуаций становится все больше, и постепенно формируется судебная практика по данным общественным отношениям. Нельзя сбрасывать со счетов и геополитические интересы различных стран. Одни из этих стран еще не осознали значения всемирного информационного пространства, другие стремятся распространить на него свое влияние, в частности, пытаясь использовать свою систему права и свое законодательство для разрешения конфликтов в Сети.

Для РФ ни один из перечисленных источников нельзя назвать даже формирующимся. У нас масса пробелов и противоречий, связанных с правовым регулированием Сети. Конечно, ряд норм содержится в гражданском законодательстве[1], в уголовном законодательстве существует территориальный принцип, распространяющий действие законов на всю территорию РФ, и принцип гражданства, устанавливающий, в частности, уголовную ответственность граждан РФ, совершивших преступное деяние за пределами РФ[2]. Тем не менее,

[1] См. нормы вступившего в силу 1 марта 2002 года Раздела VI Части 3 Гражданского Кодекса Российской Федерации.

[2] Соответственно, ч. 1 ст. 11 и ч. 1. ст. 12 Уголовного Кодекса Российской Федерации.

этих норм и принципов явно недостаточно для регулирования информационных процессов в Интернете.

В спорных ситуациях сталкиваются различные интересы и правовые системы, и возникает коллизия: какое право применять, в чьем ведении находится тот или иной информационной процесс, юрисдикция какого государства распространяется на те или иные информационные общественные отношения?

В международном праве для ответа на эти вопросы существуют так называемые коллизионные нормы. Они не разрешают вопрос сами по себе, а лишь указывают на те нормы, которые должны быть использованы в данной конкретной ситуации (например, lex loci contractus — закон места совершения сделки, lex loci actus — закон места совершения акта, lex patrie — закон гражданства, lex domicilii — закон местожительства, lex rei sitae — закон местонахождения вещи и т. д.).

В настоящее же время таковые нормы для Интернета отсутствуют, и международное информационное пространство пытаются «осваивать», используя подручные средства и национальные правовые концепции. Можно заметить, что аналогичные процессы имели место в первые десятилетия нашего века в сфере освоения воздушного пространства, но, несомненно, темпы освоения, масштабы и потенциальные возможности Сети на фоне общего потенциала развития планеты выглядят значительнее.

Судебная практика, трактующая и разрешающая проблему юрисдикции Сети, сейчас относится главным образом к наиболее доходным отраслям бизнеса в Сети — игорному и торговле информацией «для взрослых» — и формируется в тех странах, которые уже встали на путь правого регулирования Интернета, в первую очередь, в США.

В 1996 году в деле «Штат Миннесота против Granite Gate Resorts, Inc.» было вынесено решение о том, что ответчик, фирма из Невады, незаконно рекламировала жителям Миннесоты возможность интерактивно делать ставки на сайте WagerNet, зарегистрированном за пределами штата. На сайте утверждалось, что предлагаемые посетителю действия разрешены законом. И суд решил, что сайт, доступный всему миру, а значит, и жителям Миннесоты, вводил пользователей из этого штата в заблуждение.

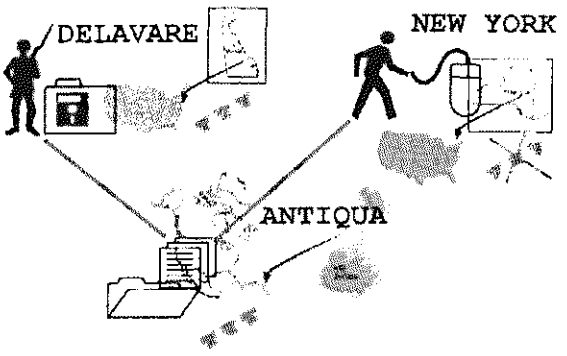


Рис. 2. Дело World Interactive Gaming Corp., 1999

В том же году бизнесмен Таттило Эдириче (Tattilo Edirice) организовал на итальянских серверах два сайта, Playmen Pro и Playmen Lite, предлагающих фотографии для взрослых, в том числе и из журнала «Playboy». Названия обоих сайтов оказались сходны с зарегистрированным в США Playboy Enterprises, Inc. товарным знаком «Playmen». Окружной суд штата Нью-Йорк постановил закрыть сайты или закрыть доступ на них американским пользователям.

В июле 1997 года в штате Миссури были признаны виновными в нарушении законов об азартных играх и о защите прав потребителей компания Interactive Gaming and Communications Corp. (штат Делавэр) и ее сотрудники, которые на сайте www.gamblenet.com организовали игры в блэк-джек и рулетку и выдавали входной пароль лишь после предварительной оплаты. Суд обязал прекратить запрещенный в Миссури вид деятельности.

Верховный суд штата Нью-Йорк, где игорный бизнес запрещен, в конце июля 1999 года вынес решение по делу «Народ против World Interactive Gaming Corp.». Ответчик, зарегистрированный в качестве юридического лица в штате Делавэр, организовал Интернет-казино на серверах, расположенных в Антигуа, и там же лицензировал свою деятельность в сфере игорного бизнеса (см. рис. 2). Тем не менее, решение было вынесено в интересах истца.

Суд в своем решении указал на следующее: для дела не имеет значения, что в Антигуа известный род деятельности разрешен, а

значит, ответчик не нарушал местных законов; важно то, что акт участия пользователя в игре происходил в штате Нью-Йорк и работа с серверами в Антигуа осуществлялась с суверенной территории штата. Таким образом, были нарушены и закон штата, и федеральное законодательство об азартных играх. В ходе следствия по делу было выяснено, что World Interactive Gaming Corp. получила в результате своей деятельности 1,8 млн. долларов от 114 инвесторов, в том числе от 14 граждан штата Нью-Йорк.

Указанный прецедент, провозглашающий верховенство законодательства штата Нью-Йорк (пока лишь для американских компаний) над законами любой другой страны, очень важен. Тем не менее, в США начинают понимать, что потенциальный доступ к сайту посредством Интернета не порождает автоматически ответственности владельца сайта за несоблюдение закона какого-либо штата. Об этом свидетельствуют решения суда по делам «Molnlycke Health Care против Dumex Medical Surgical Products» и «Hurley против Cancun Playa Oasis International Hotels», вынесенные соответственно в конце августа и начале сентября 1999 года. Для наступления ответственности необходим непосредственный информационный контакт, порождающий прямые фактические коммерческие отношения, существование которых необходимо доказать.

Так, в деле «International Star Registry of Illinois против Bowman Haight Ventures» суд признал факт 22 доказанных продаж через сайт в сети Интернет достаточным для установления юрисдикции штата Иллинойс для иностранной компании.

В Великобритании предприниматель Грэм Уоддон (Graham Waddon) за организацию порносайта на сервере, расположенном в США, получил 18 месяцев тюрьмы (см. рис. 3). Таким образом, возник национальный прецедент для регулирования отношений, связанных с открытием информационных ресурсов за рубежом.

В деле компании Braintech Inc. (Ванкувер, Канада), которая осуществляла свою деятельность в штате Техас, против Джона Костюка (John Kostiuk) столкнулись правовые системы США и Канады. Канадская апелляционная инстанция суда весной 1999 года отказалась признать решение суда штата Техас по делу о диффамации и провозгласила, что юрисдикция США не распространяется на информационное пространство Канады, где был организован ресурс ответчика.

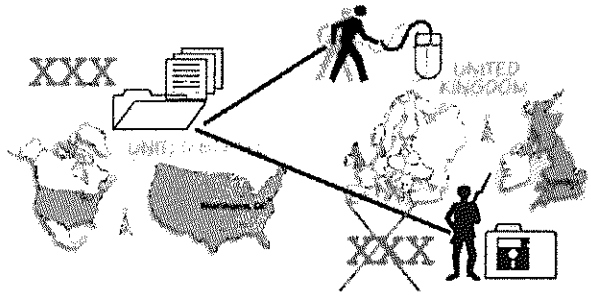


Рис. 3. Дело Грэма Уоддона, 1999

На рис. 4 и 5 приведены две схемы, характеризующие еще два судебных прецедента, имевших место ранее, в 1997 году: дело Atlanta's Georgia Institute of Technology[1] и известное всем исследователям юридической практики в области Интернет дело немецкого отделения провайдера CompuServe Inc.

Каковы же возможные пути решения проблемы юрисдикции использования сети Интернет?

В первую очередь, это международные договора, определяющие статус международного информационного пространства и фиксирующие соответствующие коллизионные нормы использования законодательства различных государств. Не панацеей, но временным выходом могут служить региональные многосторонние соглашения, а также двусторонние договора о правовой помощи. Именно в них нужно вкраплять коллизионные нормы, помогающие стабилизировать международные информационные отношения. В идеале, необходима

[1] Так называемое дело французского студенческого лагеря. Ресурс был создан в Интернете студентами указанного института. Относился он к истории образования во Франции и находился непосредственно на территории французского государства. Пользователями его были французы, американцы и, естественно, граждане других стран. Суд в Париже в 1997 году принял решение, что несмотря на то, что собственниками ресурса являются американские граждане и американское юридическое лицо, так как он расположен на территории Французской республики, указанное дело находится в юрисдикции Франции. Поэтому владельцев сайта вынудили в силу особенностей французского законодательства об использовании национального языка перевести информацию о Франции на французский язык.

унификация норм национальных законодательств относительно использования Сети (не во всех странах есть нормы, подобные ч. 4 ст. 15 Конституции РФ о верховенстве международных договоров).

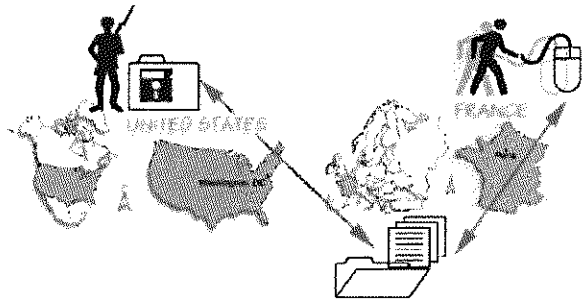


Рис. 4. Дело Atlanta's Georgia Institute of Technology, 1997

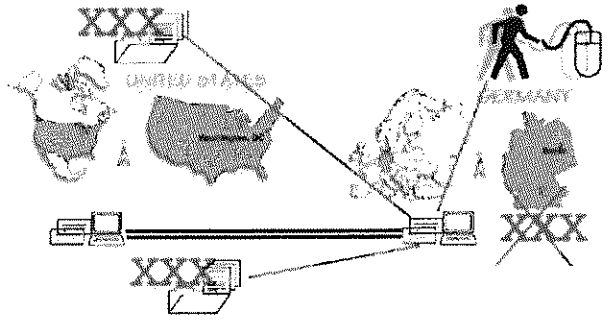


Рис. 5. Дело CompuServe Inc., 1997

Требуется соответствующее национальное информационное законодательство, чтобы не быть ни «открытыми на фоне всеобщей закрытости», ни отгораживаться от всех железным занавесом. Конечно, предварительно необходимо на государственном уровне решить, какова в принципе идеология использования информационного пространства и в рамках данного решения принять соответствующие нормы.

Пока же, на фоне отсутствия соответствующих норм в российском законодательстве владельцам ресурсов в сети Интернет, провайдерам, другим лицам следует самостоятельно включать в соглашения по использованию ресурсов и систем в сети Интернет соответствующие нормы о применяемом праве.

Вернемся к схеме многомерных информационных отношений, изображенной на рис. 1.

Регулирование этих отношений, помимо проблемы юрисдикции, определяется специальным институтом ответственности информационных провайдеров.

Последних называют по-разному: ISP, ASP, владельцы служб информационных объявлений (от досок объявлений до Интернет-аукционов), в европейском законодательстве в ходу термин «intermediary service providers», в американской практике — on-line service provider, provider of access, provider of the informational content.

В российских законопроектах употребляют термин «информационный посредник». Например, определяя его как «лицо, которое от имени другого лица отправляет, получает или хранит электронные документы или предоставляет другие услуги в отношении данных документов»[1].

Действия информационных провайдеров по оказанию услуг обладают следующими свойствами. Провайдер не инициирует информационные отношения, не выбирает содержание передаваемой информации и ее получателя, не влияет на содержание информации и хранит таковую только в пределах времени, определяемого техническими стандартами и протоколами для нужд передачи информации.

Ответственность провайдеров базируется на том, что они имеют организационно-техническую возможность в любой момент времени воздействовать на информационные общественные отношения своих пользователей. Форма воздействия может быть довольно разнообразной: от блокирования информационного обмена до информирования третьих лиц о содержании передаваемой информации.

---

[1] Соответствующие определения понятия «информационный посредник» приведены в разделе « Обзор инициатив по регулированию сети Интернет в России».

В каком случае провайдер — владелец информационного ресурса и/или информационной системы — несет ответственность за действия лиц, которые воспользовались указанными ресурсами и/или системами?

На этот счет существуют три основных подхода:

— провайдер несет ответственность за все действия пользователей, вне зависимости от наличия у него, как у субъекта права, знания о совершаемых действиях;

— провайдер не несет ответственности за действия пользователей в том случае, если выполняет определенные условия, связанные с характером предоставления услуг и взаимодействием с субъектами информационного обмена и лицами, чьи права нарушаются действиями пользователей;

— провайдер не отвечает за действия пользователей.

Законодательства разных стран предлагают решение проблемы ответственности провайдеров сообразно трем приведенным схемам (для наглядности см. рис. 6). Если, например, в Китае и странах Ближнего Востока принят первый подход, в США — третий (в подавляющем большинстве случаев провайдеры обладают иммунитетом и не несут ответственности за действия своих пользователей), то в Европе придерживаются второго подхода: наиболее детально решение проблемы ответственности проработано в европейской директиве по электронной коммерции[1].

Директива устанавливает, что провайдер не несет ответственности за передаваемую информацию в случае, если он не инициирует ее передачу, не выбирает получателя информации и не влияет на целостность передаваемой информации.

При этом допускается временное хранение передаваемой информации для осуществления необходимых технических действий по ее передаче. Также детализируются условия кэширования (ст. 13) и утверждается, в частности, что провайдер не несет ответственности за действия пользователей при предоставлении услуг хостинга, если он не был осведомлен об их противозаконной деятельности и после получения информации прекратил размещение или доступ к информации пользователей.

---

[1] Directive on electronic commerce. Council of European Union. Brussels, 2000, 28 February. Раздел 4, статьи 12–15.

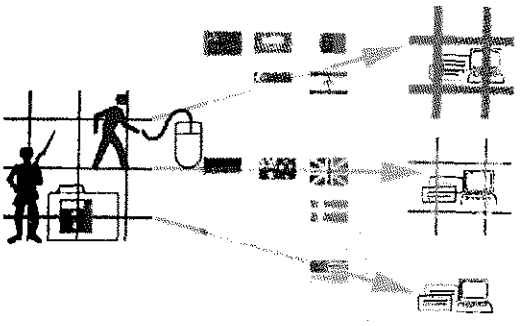


Рис. 6. Схема ответственности провайдера в разных странах

В настоящий момент в ряде стран мира приняты предметные законы, касающиеся института ответственности провайдеров. Так, в шведском законе, регулирующем ответственность владельцев досок объявлений[1], устанавливается, что таковые обязаны удалять сообщения третьих лиц в том случае, если содержащаяся в сообщениях информация нарушает ряд норм уголовного законодательства и гражданского законодательства (в части авторского права).

При анализе иностранных судебных прецедентов (в первую очередь, имевших место в США), можно заключить, что при отсутствии предметной нормы в законе суд действует по-разному, но всегда обращает внимание на характер волеизъявления провайдера при получении информации о нарушении прав третьих лиц посредством функционирования его информационных ресурсов и систем.

Так в деле Religious Technology Center v. Netcom (США, 1995), когда посредством службы телеконференций и доски объявления, поддерживаемых ответчиком, в Сети пользователями последнего были распространены материалы, авторские права на которые принадлежали истцу, и ответчик по требованию истца отказался удалить данные материалы, суд не квалифицировал действия ответчика как лица, непосредственно распространяющего чужие объекты авторского права. При этом аргумент истца о том, что аппаратно-программное обеспечение ответчика действовало автоматически, также

[1] Act (1998:112) on Responsibility for Electronic Bulletin Boards.

не был воспринят судом, подчеркнувшим, что ответчик не получал от указанного режима функционирования какой-либо выгоды. Тем не менее, суд указал, что отказ ответчика от прекращения распространения материалов при достаточном объеме представленных в претензии ответчику доказательств принадлежности авторских прав истцу может быть квалифицирован как нарушение прав истца (к сожалению для науки, было заключено мировое соглашение).

В другом известном деле Playboy Enterprises v. Frena (США), ответчик, владелец BBS, чья доска объявлений содержала размещенные третьими лицами фотоматериалы истца и функционировала в режиме открытого доступа, был признан виновным в нарушении авторских прав.

В России проблема ответственности информационного провайдера за действия пользователей решалась главным образом в спорах, связанных с регистрацией доменных имен (в делах kodak.ru, coca-cola.ru, ntv.ru)[1].

В споре ООО «Кодак» против РосНИИРОС (третье лицо — А. Грундул) истец указывал на нарушение своих прав на фирменное наименование при использовании доменного имени kodak.ru. Истец заявлял, что ответчик препятствовал реализации прав на фирменное наименование после того, как был поставлен в известность об имеющемся, по мнению истца, факте нарушения прав путем использования информационных услуг ответчика.

Но так как при третьем по счету рассмотрении дела в первой инстанции в октябре 1999 года место ответчика заняло третье лицо, квалификации судом действий первого ответчика получено не было.

Резюмируя вышесказанное, можно утверждать, что проблема ответственности провайдеров — это актуальный вопрос государственной политики по использованию сети Интернет. В зависимости от того, как будет определена и регламентирована роль провайдеров в информационных общественных отношениях в сети Интернет, возможны разные пути развития сети Интернет.

Поэтому необходимо законодательное разрешение проблемы ответственности информационных провайдеров. Предлагаемые в на-

---

[1] См. раздел «Доменное имя и средство индивидуализации: антагонизм и конвергенция».

стоящий момент нормы касаются только обмена информационными сообщениями и не затрагивают всех видов сетевых информационных услуг. При этом можно использовать схему и формулировки ст. 18 «Рекомендаций по организации деятельности лиц в сфере Интернет-коммерции в Российской Федерации», разработанные рабочей группой по электронной коммерции Комитета по экономической политике и предпринимательству Государственной Думы Федерального Собрания РФ:

«Информационный провайдер не несет ответственности за незаконные действия лиц, использующих его услуги, в случае отсутствия информации об указанных действиях или отсутствия возможности своевременно и достоверно выявить и/или квалифицировать указанные действия.

Информационный провайдер не несет ответственности за действия лиц, использующих его услуги и нарушивших обычаи делового оборота в сфере использования сети Интернет, если иное не предусмотрено законом или договором.

Информационный провайдер несет ответственность за модификацию и задержку передачи информации, если иное не предусмотрено законом или договором.

Информационный провайдер несет ответственность за неполное или недостоверное ознакомление пользователей сети Интернет об условиях использовании и существенных особенностях функционирования его информационных ресурсов».

Представляется целесообразным, чтобы сами информационные провайдеры обратили внимание на детальные ограничительные (с исчерпывающим перечнем возможностей) описания собственных услуг по использованию информационных ресурсов и систем.

Кроме этого, при взаимодействии с клиентами провайдеры с целью добросовестного описания своих услуг должны предлагать пользователям схемы регулирования вопросов, касающихся конфиденциальности действий пользователей, времени и условий хранения промежуточной (служебной) информации, условий доступа к лог-файлам и механизмов обеспечения доказательств при спорах провайдера и/или пользователя с третьими лицами.

Последняя ключевая проблема регулирования сети Интернет относится к разработке и реализации инициатив в сфере саморегуляции. Не анализируя подробно данную проблему, а адресуя читателя к последующим разделам книги, нужно заметить, что в связи с объективной сложностью и «хрупкостью» отношений, связанных с использованием информационных технологий, а также в связи с инерцией государственного регулирования, в ряде случаев с задачей защиты интересов субъектов информационных отношений в сети Интернет лучше всего справляются именно посредством инициатив в сфере саморегулирования, что будет показано далее.

А. В. Банковский

КОЛЛИЗИОННЫЕ ВОПРОСЫ РЕГУЛИРОВАНИЯ ДЕЛИКТНЫХ ОБЯЗАТЕЛЬСТВ, ОСЛОЖНЕННЫХ ИНОСТРАННЫМ ЭЛЕМЕНТОМ, В СФЕРЕ ИНТЕРНЕТ

В настоящее время развитие новых видов технологий, в том числе информационных, ставит перед юристом-международником ряд непростых вопросов, в том числе в отношении определения права, применимого к правоотношениям сторон, возникшим и развивающимся в сфере глобальной информационно-коммуникационной сети Интернет. Темпы роста количества пользователей этого средства быстрой и эффективной передачи информации постоянно увеличиваются[1], и в этой связи неуклонно возрастает важность правового регулирования отношений участников информационного обмена как на национальном, так и на международном уровне.

При этом виды неправомерных действий, совершаемых в сфере виртуального пространства, весьма многообразны. Вот лишь некоторые из них: нарушение авторских прав, нарушение прав на товарные знаки и фирменные наименования, недобросовестная конкуренция, диффамация. Помимо перечисленных видов деликтов, типичных также и для отношений "реальной" жизни, существуют правонарушения, присущие именно глобальной компьютерной сети. Это прежде всего "хакинг", целенаправленная передача компьютерных вирусов в базы данных или компьютерные системы, несанкционированный перехват корреспонденции, поступающей на адрес электронной почты другого лица. Ряд зарубежных исследователей[2] выделяют также в качестве неправомерных действий намеренное направление нежелательной корреспонденции ("спама") по электронной почте какому-либо лицу.

Представляется, что, несмотря на явную специфику Интернета, к вышеуказанным видам деликтов возможно применение по аналогии правовых норм, первоначально предназначенных для регулирования более или менее сходных отношений вне сферы всемирной виртуальной сети. Не вызывает, однако, сомнения, что более желательным является создание комплекса специальных материально-правовых норм, призванных упорядочить правоотношения участников всемирного информационного обмена в сети Интернет. При этом необходимо изучить и учесть богатый предшествующий опыт в этой области зарубежных государств и региональных объединений, прежде всего США и ЕС[3].

По мнению ряда исследователей, к числу "нерешенных проблем" глобальной сети следует отнести комплекс вопросов, связанных с трансграничностью Интернета. "В частности, законы какой страны следует применять, в суд какой страны следует обращаться и в соответствии с процессуальными нормами какой страны суд будет рассматривать соответствующее дело о нарушении ... прав в Интернете"[4]. Что касается выбора "процессуальных норм", следует отметить, что суд того или иного государства практически всегда применяет собственное процессуальное право[5]. Вопрос о выборе суда решается истцом с учетом всей совокупности обстоятельств, в том числе учитывается процессуальное и материальное право страны суда, в первую очередь вопросы подсудности[6], а также последствия принятия судом решения (при этом исследуется вопрос о возможности последующего признания и исполнения судебного решения на территории другого государства). В случае

[1] По данным службы Cerveillance в 2000 году пользователями Интернета являлось около 300 млн. человек, в два раза больше, чем в предыдущем году, а рост числа web-страниц происходил со скоростью более 7 млн. в день. См. Петрова О.М. Защита авторства в Интернет. Материалы Третьей всероссийской конференции "Право и Интернет". М. 2000; в России в настоящее время более 3 млн. компьютеров подключено к сети Интернет – см. Ананьева Е.В. Интернет и вопросы авторского права // Современное право. №5. 2000. С. 10

[2] См. напр.: *Mankowski P.; Zeitschrift R.*, 63 (1999), Internet im Internationalen Vertrags- und Deliktsrecht, S. 284.

[3] См. напр. текст проекта:European Parliament and Council Directive on the harmonisation of certain aspects of copyright and related rights in the Information Society // Official Journal of the European Communities. 2000. December 1. C. 344/1.

[4] *Подшибихин Л.И.* Некоторые проблемы правовой охраны объектов авторского права и смежных прав в Интернете. Материалы Третьей всероссийской конференции "Право и Интернет". М., 2000. С. 93

[5] Иногда судом могут применяться те или иные нормы иностранного права, которые рассматриваются иностранным правоприменительным органом в качестве процессуальных, но в целом вопрос о "выборе процессуального права" не стоит.

[6] См. напр. о критериях подсудности в отношении споров, связанных с сетью Интернет, в судебной практике США — Christopher Wolf, Internet Jurisdiction, http://profs.lp.findlaw.com/netjuris/index.html.

наличия иностранного элемента право, применимое к правоотношениям, определяется судом в соответствии с нормами международного частного права. При отсутствии материально-правовых норм, напрямую регулирующих соответствующие правоотношения на международном уровне, суд для определения применимого права использует коллизионные нормы международного частного права.

Принимая во внимание специфику отношений, складывающихся в сфере глобальной информационной сети, важным представляется следующий вопрос: требует ли появление и развитие Интернета создания специальных коллизионных норм или же использование ныне действующих коллизионных норм с учетом соответствующего толкования со стороны доктрины и правоприменительной практики является достаточным?

Представляется, что на вопрос о необходимости создания комплекса специальных коллизионных норм для регулирования деликтных правоотношений, возникающих в информационной сети, может быть дан отрицательный ответ. Путь толкования существующих коллизионных норм позволяет подойти к проблеме Интернета, как, впрочем, и к другим подобным проблемам, "с точки зрения права, а не с точки зрения уровня развития техники"[7]. Несмотря на то, что Интернет является существенно новым техническим средством информационного обмена, вопросы, с ним связанные, представляют для юриста, занимающегося коллизионными проблемами, скорее "количественную", но не "качественную" сложность.

Как известно, в настоящее время в Российской Федерации основным коллизионным началом в сфере деликтных обязательств, осложненных иностранным элементом, остается привязка lex loci delicti commissi, то есть закон места совершения противоправного действия. Так, в соответствии с ныне действующей нормой, которая содержится в ст. 167 Основ гражданского законодательства, "права и обязанности сторон по обязательствам, возникающим вследствие причинения вреда, определяются по праву страны, где имело место действие или иное обстоятельство, послужившее основанием для требования о возмещении вреда". Норма п. 1 ст. 1343 проекта раздела VII части III Гражданского кодекса Российской Федерации конкретизирует: "В случае, когда в результате такого действия или иного обстоятельства вред наступил в другой стране, может быть применено право этой страны, если причинитель вреда предвидел или должен был предвидеть наступление вреда в этой стране".

Очевидно, что для правонарушений, совершенных в сфере сети Интернет, местом, где произошло "действие..., послужившее основанием для требования о возмещении вреда", является место ввода информации, имеющей деликтное содержание, в сеть. С точки зрения субъекта, это место, в котором находится делинквент при совершении неправомерного действия. С учетом технических особенностей передачи информации в Интернет важно отметить, что местом совершения подобных действий является именно место ввода информации в сеть, а не место нахождения сервера, через который производится передача информации и который эксплуатируется, как правило, информационным посредником (т.е. провайдером интернет-услуг).

В этой связи часто возникает проблема технического обнаружения места ввода информации в сеть. Такое место далеко не всегда удается установить с высокой степенью достоверности. При этом необходимо учесть, что делинквент, заинтересованный в том, чтобы не быть обнаруженным, может использовать все имеющиеся в его распоряжении возможности для того, чтобы "замести следы" и усложнить процесс такого обнаружения. В итоге результат зависит от уровня развития техники "шифровки-дешифровки" места передачи информации, а также от технических возможностей делинквента и пострадавшего.

Избежанию технической проблемы обнаружения с большим или меньшим успехом может служить поворот бремени доказывания факта передачи информации в том или ином месте. В соответствии с общим правилом бремя доказывания тех или иных фактических обстоятельств несет лицо, ссылающееся на эти обстоятельства как на основания своих требований. Представим, что потерпевшему предоставляется право указать место, которое будет a priori считаться местом передачи информации в сеть. При этом потерпевший, бесспорно, будет стараться выбрать место, материальный закон которого предоставил бы ему наибольшие права требования. С другой стороны, лицо, передающее информацию в Интернет, то есть потенциальный делинквент, фактически будет вынуждено предпринимать усилия для того, чтобы достоверно зафиксировать факт передачи информации именно в месте ее ввода в сеть. Ценность такого подхода к решению проблемы, однако, снижается возможным обходом критериев "достоверности фиксации" места передачи информации опять-таки с технической точки зрения.

Помимо вышесказанного, следует учесть и то, что, кроме технических проблем, присущих сети Интернет, существует и общая с другими средствами передачи данных возможность преднамеренного выбора

[7] Mark Gould. Review of Thomas J. Smeddinghoff's Online Law (1996) http://jilt.law.strath.ac.uk/jilt/BookRev/97_2goul/default.htm.

места такой передачи. К примеру, письмо оскорбительного содержания может быть составлено на территории государства, право которого предусматривает ответственность для написавшего, а отправлено через почтовое отделение в стране, закон которой не рассматривает данное действие как противоправное или предоставляет потерпевшему значительно меньший объем прав требования.

Возможным решением проблемы правильной локализации места совершения противоправного действия, вероятно, была бы правовая презумпция о совпадении обычного местонахождения административного центра организации-нарушителя (обычного места жительства физического лица-делинквента) с местом ввода данных в сеть. Такой подход воспринят, в частности, законодательством Швейцарии. В соответствии со ст. 139 Закона Швейцарии о международном частном праве 1987 г. ответственность за вред, нанесенный правам личности с помощью средств массовой информации, определяется по праву государства, в котором находится обычное местопребывание автора такой информации. В случае, если для передачи данных использовались услуги различного рода рекламных или маркетинговых агентств, следует, видимо, установить место расположения подразделения, принявшего решение об использовании таких услуг.

В любом случае следует признать, что полностью исключить возможность преднамеренного выбора делинквентом места действия с целью последующего применения к возникшим правоотношениям выгодного для него права и минимизации риска в случае с деликтами, совершенными в сети Интернет, не удастся.

Представляется, что места транзита информации по пути от делинквента к потерпевшему в принципе не могут приниматься во внимание при выборе применимого права. В каждом данном случае поток информации избирает наиболее удобный (свободный) маршрут прохождения, который не может определяться ни лицом, передающим эту информацию, ни лицом, принимающим ее.

Думается, что для целей определения применимого права в случае с деликтами, совершенными в сети Интернет, основное внимание следует уделить месту востребования информации, имеющей деликтное содержание, то есть месту наступления вреда. При этом надо признать, что лицо, передающее информацию в сеть, должно, по возможности, учитывать тот эффект, который будет иметь такая передача во всех странах, где может быть установлен доступ к этой информации, по крайней мере с учетом языка, сегмента рынка, в котором действует это лицо и иных конкретных обстоятельств. Это обременение является платой за ту или иную выгоду, которую извлекает лицо, передавая информацию в Интернет. Тот, кто выражает себя в глобальной коммуникационной сети, должен отдавать себе отчет в том, что потенциально он делает это для населения многих стран. Полагаем, что такой подход не может в настоящее время стать серьезным тормозом для развития интернет-технологий, бурному и плохо контролируемому росту которых может быть даже нужен некоторый противовес. Добавим также, что тенденция применения права места наступления вреда в случаях совершения деликтов в сети Интернет является в последнее время господствующей в правоприменительной практике зарубежных стран[8].

Рассмотрим некоторые наиболее типичные виды деликтов в сфере Интернет и те вопросы, которые могут возникнуть в таких случаях при выборе применимого права.

Один из них — несанкционированное использование средств индивидуализации в сети. Для целей коллизионно-правового регулирования представляется необходимой правильная локализация нарушенного права. Наиболее остро в настоящее время стоит вопрос о захвате доменных имен, совпадающих с зарегистрированным товарным знаком или известным фирменным наименованием (Domain-Grabbing). В этом смысле определенный оптимизм в деле признания за такими действиями признаков противоправности внушает позиция российского правосудия в так называемом деле www.quelle.ru[9].

Несанкционированный захват доменного имени, в соответствии с преобладающей точкой зрения, может быть квалифицирован по российскому праву как "нарушение прав на товарный знак, нарушение прав на фирменное наименование и недобросовестная конкуренция"[10]. Соответственно, при нарушении прав на товарный знак или фирменное наименование наиболее целесообразным представляется применение права места регистрации товарного знака[11] или фирмен-

[8] См., например, о применении итальянским судом права места наступления вреда в деле о трансграничной диффамации в сети Интернет – Italian court rules foreign websites can be closed// International Internet Law Review. 2001. February. P. 3.

[9] См. подробнее: *Табастаева Ю.Г.* Доменные имена, фирменные наименования, товарные знаки: правовая защита. Судебная практика в России (на примере Квелле.Ру). Материалы Третьей всероссийской конференции "Право и Интернет". М., 2000. С. 113-116.

[10] *Вацковский Ю.* Проблемы защиты средств индивидуализации в Рунете. Материалы Третьей всероссийской конференции "Право и Интернет". М., 2000. С. 39.

[11] Такой подход воспринят законодательством и судебной практикой США, Великобритании, Нидерландов и Швейцарии — см.: Mankowski P., Op. cit., S. 287. Суды ФРГ применяют в случаях с domain grabbing нормы Закона о товарных знаках,

ного наименования[12]; а в случае недобросовестной конкуренции — права страны, рынок которой затронут такой конкуренцией. Последнее, кстати, отражает суть нормы, содержащейся в ст. 1346 проекта части III Гражданского кодекса РФ, в соответствии с которой к обязательствам, возникающим вследствие недобросовестной конкуренции, применяется право страны, рынок которой затронут такой конкуренцией, если иное не вытекает из закона или существа обязательства.

Не менее остро в настоящее время воспринимается проблема целенаправленного несанкционированного проникновения в базы данных с целью изменения, уничтожения и иного неправомерного использования содержащейся там информации (хакинг). В данном случае применимым правом, видимо, следует считать право места обычного расположения владельца данных, в отношении которых действует хакер. В частности, такой подход был воспринят создателями Директивы ЕС о защите баз данных 1995 г.[13].

Заражение вирусами представляет собой сегодня весьма распространенный вид правонарушений в сети Интернет. С точки зрения коллизионно-правового регулирования, права и обязанности сторон при заражении вирусами, видимо, должны определяться по месту нахождения поврежденных баз данных и программного обеспечения. При этом, принимая во внимание возможность самостоятельного последующего распространения вирусов, представляется целесообразным отвергнуть доводы нарушителя о невозможности предвидения наступления последствий на территории той или иной страны.

Как и обычная корреспонденция, электронная почта может при некоторых обстоятельствах несанкционированно перехватываться третьими лицами с целью ознакомления с содержимым, искажения или уничтожения содержащейся информации. В этом случае, по-видимому, также наиболее целесообразно применение к правоотношениям сторон права места наступления вреда. Поскольку вред причиняется правам того или иного лица (отправителя или получателя), подлежит применению право страны этого лица.

Некоторые действия, которые еще не были квалифицированы в российском правовом поле как противоправные, хотя неоднократно осуждались на страницах Интернет-изданий[14], по мнению ряда авторов, все же могут рассматриваться в качестве таковых. К примеру, размещение в компьютере пользователя виртуальных модулей cookies[15], которые помогают лицу, владеющему информационным ресурсом и использующему cookies, получать информацию о том, какие именно страницы посещаются пользователем и насколько часто. Информация, полученная таким образом, может быть использована в самых разных целях. Представляется, что такие действия могут быть признаны в будущем одним из видов нарушения прав человека на неприкосновенность его частной жизни.

В этом случае коллизионный вопрос может быть разрешен следующим образом. Местом действия является как место нахождения веб-сервера, который способствует размещению cookies на жестком диске пользователя, так и место нахождения самого жесткого диска. Местом наступления результата в данном случае, видимо, следует признать обычное место нахождения владельца жесткого диска, на котором размещается cookie, поскольку основной ущерб причиняется личным правам этого лица.

Несанкционированная рассылка большого количества сообщений, не запрошенных пользователями (т.е. "спама"), представляет собой фактическое использование чужого сетевого ресурса. Такого рода действия приводят к материальным потерям как для оператора связи, так и для пользователя, который в любом случае вынужден оплачивать доступ к Интернету. В случае, если "спама" "приобретает характер навязчивости, злостности или когда рассылается информация оскорбительного характера"[16], такие действия могут быть квалифицированы как хулиганство.

При этом местом действия является, по-видимому, место ввода "спама" в сеть. Вероятно, целесообразно использовать презумпцию о совпадении этого места с обычным местонахождением делинквента. Местом наступления результата следует считать место подключения пострадавшего к сети.

В настоящее время в литературе широко обсуж-

предусматривающие за нарушение прав на товарный знак санкцию в виде лишения свободы сроком до пяти лет — см. например: Rainer V. Court punishes domain grabbing // International Internet Law Review. 2001. February. P. 48; См. также: Калятин В.О. Особенности использования объектов исключительных прав в Интернет // Современное право. 2000. Ноябрь. С. 39.

[12] Защита доменного имени с точки зрения фирменного наименования практикуется в ФРГ и Австрии — см.: Mankowski P., Op. cit., S. 287.

[13] Richtlinie 95/46/EG des Europeischen Parlaments und des Rates vom 24.12.1995 zum Schutz naturlicher Personen bei der Verarbeitung personalbezogener Daten und zum freien Warenverkehr.

[14] См., например: *Леонов Д.* Анонимности Net, Internet. 2001. Апрель. №30. С. 26.

[15] Cookies определяются как некоторые строки символов, сохраняемые веб-сервером на жёстком диске пользователя с помощью его броузера, которые могут быть прочтены веб-сервером при последующих заходах на сайт.

[16] *Шевченко Н.Л.* Третейский суд по информационным спорам в Интернет // Современное право. 2000. Декабрь. С. 26.

дается проблема ответственности информационных провайдеров[17]. Законодательство и правоприменительная практика разных стран предлагают различные решения проблемы. Наиболее четко этот вопрос проработан в европейской директиве по электронной коммерции ("Directive on electronic commerce". Council of European Union. Brussels, 2000. 28 February). В Российской Федерации вопросы ответственности информационных провайдеров в настоящее время законодательно не урегулированы. Определенный подход к такому регулированию намечен в "Рекомендациях по организации деятельности лиц в сфере Интернет-коммерции в Российской Федерации", разработанных Комитетом по экономической политике и предпринимательству Государственной Думы Федерального Собрания РФ[18].

Особенно остро вопрос об ответственности провайдера встает в случае, если лицо, передающее информацию в сеть, не выявлено, предъявление к нему требований экономически неэффективно или связано с большими трудностями.

В случае, если судом или иным правоприменительным органом учитываются доли ответственности лица, передающего информационный ресурс в Интернет (собственника информационного ресурса) и информационного провайдера, может возникнуть вопрос о выборе права, применимого к ответственности провайдера, иного, чем право, применимое к ответственности владельца информационного ресурса. Видимо, в этом случае может применяться право места расположения сервера, через который информационный ресурс, имеющий "деликтное" содержание, передается в сеть. При этом требуется, однако, заметить, что информационный провайдер, как правило, имеет больше технических возможностей, чем "обычный" делинквент, по манипулированию данными, а также по размещению места своей деятельности в государствах, законодательство которых предусматривает минимальную ответственность информационных посредников или не предусматривает ее вовсе.

Суть альтернативного подхода заключается в том, чтобы использовать для определения ответственности информационного провайдера акцессорную привязку к праву, регулирующему ответственность собственника информационного ресурса, имеющего вредоносное содержание. В данном случае информационный посредник рассматривается как лицо, способствующее осуществлению деликта. Такой подход имеет ряд преимуществ. Во-первых, он помогает избежать двойного выявления и доказывания фактических обстоятельств, существенных для определения применимого права (место нахождения провайдера и т.д.). Кроме того, он способствует определению владельца информационного ресурса как основного делинквента.

Развитие института ответственности провайдера может придать определенный стимул для создания самими информационными посредниками систем контроля с целью эффективного выявления владельцев информационных ресурсов, размещающих эти ресурсы в Интернете. Тогда в случае предъявления иска непосредственно к провайдеру последний мог бы воспользоваться правом регрессного требования к основному делинквенту, которым является владелец информационного ресурса.

В связи с вышеизложенным необходимо подчеркнуть, что речь идет об информационном посреднике (провайдере), услугами которого пользуется основной делинквент. Вышесказанное в отношении акцессорной привязки к праву, регулирующему ответственность владельца информационного ресурса, вряд ли применимо к провайдеру, который предоставляет услуги потерпевшему на основании договора с ним.

Достаточно спорным является вопрос о том, должно ли нести ответственность (и если да, то в какой степени) лицо, размещающее в Интернете гиперссылку на сайт, который содержит вредоносную информацию. При этом особо следует обратить внимание на то обстоятельство, что даже если при размещении гиперссылки информационный ресурс, к которому она отсылает, был проверен и в нем не было найдено ничего предосудительного, то с течением времени содержимое сайта может измениться. С другой стороны, размещение ссылки на сайт с "деликтным" содержанием явно способствует распространению вредоносной информации. Выходом из сложившейся ситуации, вероятно, могла бы стать разработка правил более или менее регулярного контроля за информацией, к которой отсылает электронная ссылка со стороны ее владельца. В случае нарушения этих правил и распространения в результате этого "деликтного" информационного ресурса ответственность владельца гиперссылки могла бы регулироваться, как и в случае с иформационным провайдером, правом, определяемым на основе акцессорной привязки к "основному" деликтному статуту.

Одним из видов деликтной ответственности в отношении рассматриваемой нами темы является ответственность за вред, причиненный вследствие не-

[17] *Bovenzi G.* Liabilities of System Operators on the Internet: Berkeley Technology L.J. 11 http://www.law.berkeley.edu/btlj/articles/11-1/Bovenzi.html; *Flechsig N.R.* Haftung von Online-Diensteanbietern im Internet. 1996; См. также: *Наумов В.* Проблема ответственности информационных провайдеров. Материалы Третьей всероссийской конференции "Право и Интернет". С. 77.

[18] Там же. С. 78.

достатков программного обеспечения, распространяемого с помощью сети Интернет. В данном случае для определения применимого права (конечно же, в случае наличия в правоотношении иностранного элемента) подлежат использованию коллизионные нормы о праве, подлежащем применению к ответственности за вред, причиненный вследствие недостатков товара, работы или услуги. В частности, ст. 1345 раздела VII "Международное частное право" *проекта предоставляет потерпевшему* право выбора между правом страны, где имеет место жительства или основное место деятельности продавец или изготовитель товара или иной причинитель вреда, правом страны, где имеет место жительства или основное место деятельности потерпевший, и правом страны, где была выполнена работа, оказана услуга, или правом, где был приобретен товар. В случае, если потерпевший не использует предоставленное ему право выбора, применимое право определяется в соответствии с общими *нормами, подлежащими применению к обязательствам* вследствие причинения вреда.

На правах рукописи

НЕЗНАМОВ
Андрей Владимирович

ОСОБЕННОСТИ КОМПЕТЕНЦИИ ПО РАССМОТРЕНИЮ ИНТЕРНЕТ-СПОРОВ: НАЦИОНАЛЬНЫЙ И МЕЖДУНАРОДНЫЙ АСПЕКТЫ

Специальность 12.00.15 – Гражданский процесс;
арбитражный процесс

Автореферат
диссертации на соискание ученой степени
кандидата юридических наук

Екатеринбург 2010

ИЗДАТЕЛЬСКИЙ ДОМ
«Уральская государственная юридическая академия»

Работа выполнена на кафедре гражданского процесса государственного образовательного учреждения высшего профессионального образования «Уральская государственная юридическая академия»

Научный руководитель: доктор юридических наук, профессор ***Ярков Владимир Владимирович***

Официальные оппоненты: доктор юридических наук, профессор ***Скворцов Олег Юрьевич***, кандидат юридических наук, доцент ***Фетюхин Марат Владимирович***

Ведущая организация: ***Российская академия правосудия***

Защита состоится 24 июня 2010 г. в 11.00 ч на заседании диссертационного совета Д.212.282.01 при Уральской государственной юридической академии по адресу: 620066, г. Екатеринбург, ул. Комсомольская, д. 21, зал заседаний совета

С диссертацией можно ознакомиться в библиотеке Уральской государственной юридической академии

Автореферат разослан « 20 » мая 2010 г.

Ученый секретарь
диссертационного совета
доктор юридических наук,
профессор В. И. Леушин

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Актуальность темы диссертационного исследования. Современные общественные отношения складываются под влиянием научно-технических достижений, многие из которых являются результатом разработок ученых XX века. Среди таких достижений важное место занимает сеть Интернет. В России сфера пользователей Интернетом расширяется огромными темпами, что влечет за собой различные последствия социально-экономического и правового характера.

Деятельность современного общества все больше ориентируется на использование Сети как средства межкультурной коммуникации и социального общения. В то же время возможности, которые предоставляет Интернет, привели к его быстрой коммерциализации, и Сеть крайне широко используется для ведения предпринимательской деятельности. Однако многие проблемы, существующие в социальной и экономической сфере, также получили свое преломление в виртуальном пространстве.

Являясь, по сути, принципиально новым институтом общественной жизни, Интернет поставил перед правовой наукой целый комплекс проблем. Возникла необходимость переосмыслить правовую доктрину с учетом последствий функционирования Сети, которые вызывают массу вопросов юридического характера. Среди них – проблема определения понятия «Интернет», пределы правового регулирования Сети, вопросы юрисдикции по спорам, возникающим из сетевых отношений, вопросы квалификации сделок и правонарушений, совершенных в Интернете, используемых доказательств и множество других.

Это обусловило потребность в разработке соответствующих решений на законодательном уровне. Фактически каждая отрасль российского права так или иначе сталкивается с проблемами, связанными с функционированием сети Интернет: уголовное право – в преступлениях против чести и достоинства личности (клевета, оскорбление), а также в «компьютерных» преступлениях; гражданское право – в сделках, совершаемых с использованием сети Интернет; административное право будет решать вопрос о том, в какой степени Интернет подлежит регулированию. Международное частное право и коллизионное право призваны решить вопрос о юрисдикции

государств и их органов в этой сфере; налоговое право – вопрос о налогообложении деятельности в Интернете. Отдельно стоит выделить авторское право, поскольку большинство споров, связанных с Интернет-отношениями, возникают именно из отношений по охране авторских и смежных прав.

Значительные проблемы существуют и в сфере процессуального права. Вопросы подсудности и подведомственности, доказывания и обеспечения доказательств сегодня из-за отсутствия соответствующих законодательных положений призваны решать на практике юристы и суды.

В настоящее время возникают споры уникальных, специфичных категорий (например, споры о доменных именах, споры, возникающие из деятельности Интернет-магазинов и Интернет-провайдеров). Новые нюансы появляются в делах традиционных категорий, в том числе в делах по защите авторских прав, деловой репутации, в спорах, связанных с дистанционным оказанием услуг. Решение таких споров осуществляется на основе не адаптированных для этих целей правовых норм, и поэтому позиция правоприменительных органов сегодня как никогда сильно зависит от деятельности ученых-юристов.

Указанными обстоятельствами и определяется актуальность темы диссертационного исследования.

Степень научной разработанности темы. Подавляющее большинство исследователей справедливо считают, что развитие Интернета в России: а) сравнимо с ключевыми вехами его развития в других странах, б) происходит бурными темпами, в) ставит множество проблем в правовой плоскости.

В зарубежной юридической науке проблема компетенции по рассмотрению юридических дел, связанных с использованием сети Интернет, традиционно является неотъемлемой и одной из самых важных частей «Интернет-права» (Cyberlaw) как такового и в силу актуальности и популярности проблематики сети Интернет среди юристов существенно разработанной.

Среди зарубежных доктринальных источников следует отметить работы М. Гейста, одного из самых видных специалистов США в области «Интернет-права». Вопросы юрисдикции над Интернет-отношениями изучали также Д. Менте, который создал довольно известную теорию интернациональных пространств; Д. Зиттрэйн – один из самых видных зарубежных специалистов в области Интернет-права; Д. Пост и Д. Джонсон – авторы исследования, посвященного экстерриториальности Сети, и многие другие ученые – Ю. Коль, Л. Эдвардс, С. Уилски, Р. Майклс и т. д.

Представители российской правовой науки также начали изучать очень многие юридические аспекты и проблемы, связанные с функционированием сети Интернет. В фундаментальных работах многих ученых дается не только подробное техническое описание системы, принципов и методов работы Сети, истории ее появления и становления, но и глубокий анализ различных правовых аспектов ее действия.

Однако верно и то, что до сих пор в юридической науке отношения, связанные с использованием сети Интернет, изучаются либо с самых общих позиций информационного права, либо крайне фрагментарно.

Среди работ по общим вопросам функционирования сети Интернет можно отметить исследования И. Л. Бачило, В. О. Калятина, В. А. Копылова, А. В. Шамраева, А. А. Тедеева, М. А. Якушева, И. М. Рассолова, Б. В. Андреева и др.

Среди специальных трудов выделяются работы А. Г. Серго, П. В. Бабарыкина, С. А. Воропаева, П. Д. Барановского, С. А. Бабкина, В. И. Скиба, С. В. Коростелевой, О. П. Бойко, О. В. Мозолиной, В. Б. Наумова, Э. А. Казарян, К. Л. Брановицкого, Е. И. Кокотовой, С. Н. Мироновой, В. П. Талимончик, Е. В. Михайленко, А. В. Глушкова, С. В. Малахова, Н. А. Дмитрик, П. С. Симонович, А. В. Зажигалкина, С. В. Петровского и иных авторов. Каждый из этих ученых детально рассматривал отдельные проблемы, связанные с функционированием сети Интернет, как-то: охрана результатов интеллектуальной деятельности в сети Интернет, методы и средства публичного международно-правового регулирования Сети, возможности применения информационных технологий в деятельности судов, проблемы распространения информации в Сети, особенности Интернет-отношений и т. д.

Вопросы компетенции безотносительно сети Интернет изучали А. А. Мамаев, М. Ю. Лебедев, Т. П. Ерохина, М. А. Рожкова, И. М. Дивин, Е. В. Кузнецова, К. А. Чудиновских, И. В. Стрелкова, В. А. Филановский, И. Л. Бурова, Л. П. Ануфриева, М. М. Богуславский, И. В. Елисеев, Л. А. Лунц, Ю. К. Осипов, К. С. Юдельсон,

В. П. Воложанин, В. М. Жуйков, П. С. Дружков, Т. М. Нешатаева, В. К. Пучинский, В. В. Ярков, И. В. Решетникова, Г. Л. Осокина и др. Проблемы компетенции над спорами, как-либо связанными с использованием сети Интернет, рассматривали В. О. Калятин, Е. Б. Леонович и А. С. Кемрадж.

Самой, пожалуй, близкой к теме нашего исследования (отдельной его части) и своего рода единственным в этой области является диссертационная работа Л. В. Горшковой, посвященная проблемам регулирования частноправовых отношений международного характера в сети Интернет, в которой она рассмотрела, в том числе, вопросы международной подсудности и ряд используемых в практике судов США юрисдикционных критериев.

Однако комплексного исследования в науке гражданского и арбитражного процессуального права, касающегося компетенции по рассмотрению Интернет-споров и иных правовых вопросов, связанных с функционированием сети Интернет, до настоящего времени не проводилось.

Теоретическая, нормативная и эмпирическая основы работы. Теоретическую основу настоящего диссертационного исследования составили работы всех указанных, а также иных ученых.

Нормативная основа работы – нормы и институты российского законодательства (положения АПК и ГПК РФ, ГК РФ, различные федеральные законы и ведомственные нормативные акты), нормы международного права (в частности, положения Брюссельской конвенции по вопросам юрисдикции и принудительного исполнения судебных решений в отношении гражданских и коммерческих споров).

Эмпирической базой исследования послужила правоприменительная практика российских судов (как общей юрисдикции, так и арбитражных), а также практика зарубежных судов (в работе исследовано более двух десятков прецедентных дел судов США и решения Суда Европейских сообществ в Люксембурге).

Объект исследования. Объектом исследования являются общественные отношения, связанные с использованием сети Интернет, а также споры, возникающие на их основе и связанные с их развитием.

Предмет исследования. Предмет настоящего исследования составили действующие нормы законодательства России и международного права, а также ряда зарубежных стран, посредством которых осуществляется разграничение дел, связанных с использованием сети Интернет, между различными юрисдикционными органами, а также нормы, определяющие статус и полномочия таких органов; правоприменительная практика российских и зарубежных юрисдикционных органов по рассмотрению Интернет-споров; правовые средства и методы правового регулирования процессуальных вопросов компетенции, связанных с использованием сети Интернет, выработанные как в зарубежных, так и в российской правовых системах; научно-теоретические исследования вопросов юрисдикции над Интернет-спорами зарубежных и отечественных ученых.

Методология исследования. Для достижения поставленных задач использовались общенаучные методы познания (системный, описательный, анализа и синтеза, формально-логический), а также специальные методы: сравнительно-правовой, историко-правовой анализ, а также метод технико-юридического анализа.

Цель исследования – выявить теоретические и практические проблемы процессуального характера, связанные с компетенцией различных правоприменительных органов по разрешению споров, возникающих при использовании сети Интернет, провести их комплексный научный анализ, определить их правовую природу и специфику, сформулировать возможные варианты их решения, разработать предложения по совершенствованию правового регулирования институтов международной и национальной подсудности, подведомственности.

Названные цели обусловили постановку и решение следующих *задач*:

1) охарактеризовать юридически значимую специфику Интернет-отношений и определить причины, по которым споры, связанные с использованием сети Интернет, могут быть выделены в отдельную категорию, а также классифицировать эти Интернет-споры по различным основаниям;

2) определить понятийно-категориальный аппарат исследования, который позволяет на основе единых критериев без терминологических противоречий объединить категории «юрисдикция», «компетенция», «подведомственность», «международная подсудность»;

3) изучить и обобщить наиболее значимый зарубежный опыт развития юрисдикционных подходов при определении международной

компетенции Интернет-споров на законодательном, правоприменительном и доктринальном уровне, сформулировать предложения по совершенствованию российского законодательства в этой области;

4) выявить круг юрисдикционных органов, к компетенции которых в соответствии с действующим законодательством относится рассмотрение Интернет-споров, а также сформулировать предложения по дальнейшему развитию их полномочий, уточнению круга таких органов.

5) исследовать возможности применения и специфику традиционных правил национальной подведомственности в отношении Интернет-споров в соответствии с общепринятыми критериями подведомственности и наиболее распространенными видами дел, связанных с использованием сети Интернет, а также сформулировать предложения по совершенствованию института подведомственности для устранения выявленных проблем;

6) рассмотреть специфику института подсудности дел, связанных с использованием сети Интернет, российским судам, определить возможность применения общих традиционных правил территориальной подсудности к спорам рассматриваемой категории, сформулировать предложения по совершенствованию принципов территориальной подсудности Интернет-споров;

7) выявить сопутствующие частные и общие проблемы процессуального характера, обусловленные спецификой сети Интернет и связанные с вопросами компетенции по рассмотрению Интернет-споров.

Научная новизна исследования. Настоящая работа является одним из первых в области процессуального права исследований проблемы применения на национальном и международном уровне традиционных юрисдикционных правил к отношениям, возникающим при использовании компьютерной сети Интернет. Впервые на уровне диссертационного исследования в науке гражданского и арбитражного процессуального права детально, на общей методологической и единой понятийно-категориальной основе изучается специфика подведомственности, а также национальной и международной подсудности в отношении споров, связанных с использованием сети Интернет.

На защиту выносятся следующие положения.

1. Дается авторское понятие «Интернет-спора» как спора, связанного с использованием сети Интернет, при условии, что отношения, из которых возник такой спор, существенным образом обусловлены в своем возникновении или развитии использованием телекоммуникационной сети Интернет. Выявлены и обоснованы сущностные признаки Интернет-споров: спор является связанным с использованием сети Интернет, если его существенным элементом, непосредственно связанным с делом, является сеть Интернет. Предлагается классификация Интернет-споров по характеру дела на оригинальные и производные, а также в зависимости от соответствующей, ключевой для спора, особенности Интернет-отношений.

2. На основе анализа развития юрисдикционных правил в зарубежных странах доказывается, что при определении международной подсудности Интернет-споров целесообразно ориентироваться не только на объективные выражения действий ответчиков, как это имеет место в европейской практике, но и на субъективную составляющую таких действий для установления территории, на которую они фактически были «целенаправлены», как это имеет место в практике судов США.

В соответствии с обоснованной необходимостью более широкого внедрения в российское право принципа «целенаправленной деятельности» высказывается предложение о создании дополнительного правила территориальной подсудности Интернет-споров судам РФ, основанного на направленности действий ответчика на определенную территорию.

3. Анализ юрисдикционных критериев, используемых в разных правовых системах, позволил доказать, что существующие коллизии компетенции различных юрисдикционных органов в отношении Интернет-споров могут устраняться путем доработки существующих «территориальных» критериев подведомственности посредством внесения изменений в действующее процессуальное законодательство.

Вместе с тем обосновывается, что наиболее оптимальным и перспективным способом устранения названных коллизий является замена территориального принципа компетенции принципом так называемой «конвенциональной компетенции», основой которой выступает участие пользователя в каком-либо глобальном Интернет-сообществе.

4. Доказывается необходимость рассмотрения доменных споров как разновидности Интернет-споров по правилам специальной подведомственности, так как решение вопроса о подведомственности таких споров на основе традиционных критериев (характер спора и статус его участников) создает существенные и непреодолимые сложности как теоретического, так и практического характера.

5. Обосновывается, что компетенция негосударственных правоприменительных органов по рассмотрению Интернет-споров должна строиться на основании квазитретейских соглашений пользователей Сети, что станет частным проявлением принципа «конвенциональной компетенции».

Предлагается введение обязательного досудебного порядка урегулирования Интернет-споров отдельных категорий на основе соглашений пользователей Сети, что позволит разграничить компетенцию национальных судов и специализированных органов по рассмотрению различных Интернет-споров в соответствии с правилами императивной подведомственности.

6. Исследование специфики критерия спорности права как части института подведомственности позволило обосновать вывод о существовании конкурирующей компетенции у нескольких категорий юрисдикционных органов в отношении Интернет-споров. В качестве одного из возможных способов устранения коллизий подведомственности между судами и органами нотариата по вопросам охраны прав на результаты интеллектуальной деятельности предлагается расширить круг полномочий нотариусов по так называемому «депонированию» объектов авторского права.

7. Обосновывается, что дела, связанные с порядком признания информационных материалов экстремистскими, относятся к Интернет-спорам и в настоящий момент компетенция по их рассмотрению регламентируется в соответствии с правилами альтернативной подсудности. Доказывается необходимость рассмотрения Интернет-споров такой категории по правилам исключительной подсудности.

Теоретическая и практическая значимость работы. Результаты проведенного исследования могут быть использованы для дальнейшего совершенствования законодательства, регулирующего институты международной подсудности, подведомственности и национальной подсудности, а также в дальнейших научных исследованиях. В работе сделаны теоретико-правовые выводы относительно компетенции по рассмотрению отдельных категорий Интернет-споров, выявлены мировые тенденции развития институтов международной и национальной подсудности в аспекте Интернет-отношений и сформулированы рекомендации по их внедрению в российскую правовую систему. Сделанные автором выводы могут быть использованы при определении правового статуса и совершенствовании правомочий юрисдикционных органов, полномочных рассматривать Интернет-споры, в том числе в российском законодательстве.

В соответствии со сделанными выводами и выявленными перспективами развития отдельных процессуальных институтов сформулированы предложения по внесению изменений в некоторые законодательные акты. В частности, предлагается изменить редакцию п. 5 ч. 1 ст. 33 и п. 9 ч. 1 ст. 247 Арбитражного процессуального кодекса РФ, дополнить подраздел III раздела II Гражданского процессуального кодекса РФ главой «Производство по делам о признании информационных материалов экстремистскими», а проект Федерального закона «О нотариате и нотариальной деятельности в Российской Федерации» дополнить главой «Депонирование оригиналов авторских произведений».

С учетом обнаруженных проблем в области компетенции в делах, связанных с использованием сети Интернет, и отдельных негативных тенденций развития правоприменительной практики по вопросам подведомственности наиболее распространенных категорий Интернет-споров сформулированы рекомендации, которые могут быть учтены в практической деятельности как правоприменительных, так и законодательных органов. Результаты исследования могут также использоваться при рассмотрении конкретных дел, связанных с использованием сети Интернет, а также при преподавании общих курсов гражданского и арбитражного процессуального права, а также курса «Особенности судопроизводства по гражданским делам».

Апробация результатов исследования. Диссертация подготовлена и обсуждена на кафедре гражданского процесса Уральской государственной юридической академии. Основные ее положения освещены в научных публикациях автора и использовались при проведении практических занятий в Уральской государственной юридической академии.

Некоторые результаты исследования докладывались на Четвертой международной научно-практической конференции, посвящен-

ной памяти М. И. Ковалева «Уголовная политика в сфере информационной безопасности РФ» (Екатеринбург, февраль 2007 г.).

Автор принял участие в подготовке законопроекта «О нотариате и нотариальной деятельности в Российской Федерации», внеся ряд предложений на рассмотрение рабочей группы.

Отдельные положения диссертации и выработанные в ней подходы были успешно использованы автором при работе в составе экспертной группы по авторским и смежным правам Российско-Американской рабочей группы по межбиблиотечному сотрудничеству и информационному обмену между Национальной Президентской библиотекой имени Б. Н. Ельцина и Библиотекой Конгресса США, в частности при подготовке всех промежуточных и итогового доклада, посвященного специфике информационного обмена, в том числе посредством сети Интернет, в правовых системах России и США.

Структура исследования. Структура работы обусловлена целями и задачами исследования. Диссертация состоит из введения, трех глав, объединяющих семь параграфов, заключения, приложения и списка использованной литературы.

СОДЕРЖАНИЕ РАБОТЫ

Во **введении** обосновывается актуальность выбранной темы исследования, определяются его цель и задачи, отражены его научная новизна и положения, выносимые на защиту, а также научно-практическая значимость результатов.

В первой главе **«Понятие и юридическая природа Интернет-споров и компетенции в процессуальном праве»** в соответствии с поставленными задачами исследования даются определения понятий, используемых в настоящей работе, в их соотношении со смежными правовыми категориями.

В первом параграфе первой главы **«Признаки Интернет-отношений и специфика Интернет-споров»** рассматривается специфика Интернет-отношений для целей определения понятия Интернет-спора, используемого в контексте работы. Выделяются существенные признаки Интернет-отношений, которые в совокупности позволяют дать определение спорам, связанным с использованием сети Интернет (Интернет-спорам).

С точки зрения специфики видов и критериев подведомственности Интернет-споров существенными особенностями Интернет-отношений, из которых вытекают Интернет-споры, являются: 1) сложность идентификации участников отношений в сети и (или) неопределенность их местонахождения; 2) возникновение и развитие значительного числа отношений с использованием регулируемой системы доменных имен; 3) множественный субъектный состав этих отношений в большинстве споров; 4) необходимость использования субъектами специальных технических средств с определенным программным обеспечением для вхождения в сеть.

Указанные особенности позволяют выделить следующие признаки Интернет-спора:

спор возникает из правоотношений между его сторонами;

спор связан с использованием сторонами телекоммуникационной сети Интернет.

использование сторонами сети Интернет является существенным для развития спора: без такого использования данные отношения не сложились бы (не складывались соответствующим образом) либо развивались в значительной степени по-иному.

Спор, таким образом, считается связанным с использованием сети Интернет, если его существенным элементом, непосредственно

связанным с делом, является сеть Интернет. Существенность подразумевает, что без использования сети Интернет такого рода отношения не сложились бы (не складывались соответствующим образом) либо развивались бы в значительной степени по-иному.

На основе выделенных признаков дается следующее понятие: *Интернет-спор – это спор, связанный с использованием сети Интернет, при условии, что отношения, из которых возник такой спор, существенным образом обусловлены в своем возникновении или развитии использованием телекоммуникационной сети Интернет.*

В качестве примера рассматриваются некоторые категории отношений, в которых в зависимости от существенности использования сети Интернет основанный на таких отношениях спор может быть квалифицирован как Интернет-спор (договор займа, купля-продажа товара в магазине, использование объектов авторского права и т. д.).

Производится классификация Интернет-споров по нескольким основаниям. В частности, выделяются оригинальные Интернет-споры, возникшие в связи с функционированием сети (дела о доменных именах, споры, связанные с использованием различных электронных денег), и производные, имеющие под собой «реальные» категории дел (споры о защите авторских прав в сети Интернет, о защите прав потребителей в отношениях, когда заключение или исполнение договора между сторонами осуществлялось посредством сети Интернет).

Делается вывод о возможности классификации Интернет-споров в зависимости от того, какая из приведенных особенностей Интернет-отношений имеет наибольшее значение при рассмотрении дела. Например, возникновение и развитие определенных отношений с использованием регулируемой системы доменных имен практически всегда имеет определяющее значение в доменных спорах.

Множественный субъектный состав имеет важное значение, в частности, в спорах об использовании объектов авторских и смежных прав через систему так называемых торрент-трекеров; в спорах, связанных с участием Интернет-аукциона в совершении или исполнении сделки купли-продажи в сети Интернет; в делах о защите чести, достоинства и деловой репутации в сети Интернет и т. д.

Необходимость использования субъектами спора специальных технических средств с определенным программным обеспечением для доступа в Интернет принципиально важна в тех случаях, когда

исследуется возможность привлечения провайдера к ответственности за деятельность пользователя, которому тот предоставил доступ в Интернет, а также в спорах, связанных с использованием электронных денег, спорах, связанных с осуществлением Интернет-банкинга, и т. д.

Наконец, сложность идентификации участников отношений в сети и (или) неопределенность их местонахождения – проблема, которая возникает практически во всех делах, связанных с осуществлением Интернет-коммерции и распространением информации в сети Интернет.

Во втором параграфе первой главы **«Понятие компетенции и ее соотношение с основными категориями, используемыми для разграничения предметов ведения в сфере сети Интернет»** исследуется понятие «компетенция» в его соотношении с категориями юрисдикции, подведомственности и подсудности.

Рассматриваются высказанные в процессуальной науке точки зрения на понятия «компетенция», «юрисдикция, «подведомственность» и «подсудность», – как классические, так и авторов диссертационных исследований последних лет. Приводится обзор нормативных актов РФ и положений международных договоров РФ, в которых используется термин «компетенция», и контекстов его применения.

В работе понятие «компетенция» рассматривается в его традиционном понимании, обоснованном Ю. К. Осиповым: как определенный круг полномочий, властных функций любого органа – как государственного, так и негосударственного, как национального, так и международного. Кроме того, компетенция направлена не только на рассмотрение вопросов правоприменения, но и вообще на рассмотрение абсолютно любых вопросов, в том числе организационного характера.

Практика применения термина «компетенция» в российском праве, а также в правопорядках ряда других стран свидетельствует о том, что он обозначает наиболее общее понятие, которое в зависимости от контекста и особенностей правопорядка призвано охарактеризовать отношение определенного властного субъекта (органа) к объектам его правомочий на самых разных уровнях – от полномочий самого государства (его «юрисдикции»: на этом уровне данный термин более точен) до полномочий конкретного суда (в системе общего права они обозначаются тем же термином «юрисдикция»,

а в российском праве – термином «подсудность»). Кроме того, термин «компетенция» в наибольшей степени соответствует терминологии большинства международных соглашений.

По мнению автора, именно от понятия «компетенция» можно отталкиваться при исследовании как общих, так и частных вопросов рассмотрения определенных категорий дел соответствующим полномочным органом.

Вторая глава **«Международная подсудность Интернет-споров»** посвящена вопросам международной подсудности. В ней исследуются различные юрисдикционные принципы, применяемые для определения международной подсудности Интернет-споров, а также предлагаются варианты их адаптации к российской правовой системе.

В первом параграфе второй главы **«Юрисдикционные принципы, применяемые к Интернет-спорам в правовой системе США»** изучается эволюция юрисдикционных принципов в правовой системе США и рассматриваются отдельные наиболее значимые судебные прецеденты, а также разработанные в практике США юрисдикционные правила в отношении Интернет-споров, к которым, в частности, относятся следующие.

Тест минимальных контактов: для распространения юрисдикции на ответчика, который не находится в рамках соответствующей подсудной суду территории, необходимо, чтобы ответчик имел «минимальные контакты» с местом рассмотрения дела (дела International Shoe Co v. Washington, Helicopteros Nacionales de Colombia v. Hall).

Критерий целенаправленного подчинения: персональная юрисдикция над нерезидентом возникает, когда его действия были целевым образом и осознанно направлены на территорию, находящуюся в юрисдикции суда. Если нерезидент совершит действия, направленные на то, чтобы получить возможность пользоваться всеми преимуществами правовой защиты данной юрисдикции, то он тем самым подчинит себя ей. В дальнейшем к этим характеристикам добавилось предвидение ответчиком возможности судебного разбирательства в данном штате (дела Hanson v. Denckla, World-Wide Volkswagen Corp. v. Woodson, CompuServe v. Patterson).

Принцип скользящей шкалы (шкала Zippo): на одном конце шкалы («наличие юрисдикции») находятся случаи, когда ответчик очевидно осуществляет предпринимательскую деятельность в сети Интернет, совершая сделки с лицами, находящимися на территории

соответствующей юрисдикции, что влечет за собой постоянную и целенаправленную передачу данных в электронной форме. Осуществление такой активной деятельности через веб-сайт позволяет распространить юрисдикцию на ответчика. На другом конце шкалы («отсутствие юрисдикции») находятся ситуации, когда ответчик лишь выкладывает на веб-сайт информацию. Такая пассивная деятельность через веб-сайт не дает оснований для распространения юрисдикции на ответчика (дела Zippo Manufacturing Co. v. Zippo Dot Com, Inset Systems Inc. v. Instruction Set, Inc, Cybersell, Inc. v. Cybersell, Inc).

Критерий цели: суд будет обладать юрисдикцией на рассмотрение спора, если ответчик, не являющийся резидентом, очевидно и осознанно направил свои действия на территорию, находящуюся под юрисдикцией данного суда, зная при этом, что они причинят вред именно на этой территории. Суд будет обладать юрисдикцией на рассмотрение спора в тех случаях, когда место, где рассматривается спор, было явной целью деятельности ответчика (дела Calder v. Jones, Yahoo! Inc. v. La Ligue Contre Le Racisme et l'antisemitisme).

Автором также рассмотрены модификации этих критериев в различных судебных прецедентах (Asahi v. Superior Court, Toys «R» Us v. Step Two S. A.).

Во втором параграфе второй главы **«Юрисдикционные правила Интернет-споров в европейском континентальном праве и международная подсудность Интернет-споров в правовой системе РФ»** рассматриваются юрисдикционные правила в отношении Интернет-споров, действующие в европейских странах, а также установленные в РФ правила международной подсудности Интернет-споров и высказываются предложения по их дополнению.

Исследуется проблема применения доктрины forum non convenience в европейском праве, позволяющей суду, который обладает юрисдикцией на рассмотрение дела, не рассматривать его, если это не отвечает интересам сторон и если дело может быть передано другому, более подходящему суду.

Отказ от этой доктрины в европейском праве свидетельствует о том, что урегулирование всех возможных спорных ситуаций осуществляется путем создания целого комплекса достаточно подробных юрисдикционных правил.

В связи с этим анализируются юрисдикционные критерии, содержащиеся в Регламенте ЕС 44/2001 от 22 декабря 2000 г., в частнос-

ти критерий, в соответствии с которым юрисдикцией на рассмотрение спора будет обладать суд по месту исполнения обязательств, а также суд по месту действия, которым был причинен вред, или месту, где этот вред мог наступить. При этом указанные критерии исследуются с учетом позиции Европейского суда (дела G. J. Bier B. V. v. Mines de Potasse D'Alsace S.A и Shevill v. Presse Alliance).

Сравнивая европейский и американский подходы к решению этого вопроса, автор обосновывает следующий вывод: фундаментальная разница между ними заключается в том, что европейские суды в значительно меньшей степени используют критерий цели действий ответчика, вслед за Европейским судом ставя на первое место понятия вреда и места его причинения либо понятие места осуществления конкретного юридического действия. Таким образом, можно сказать, что европейская практика ориентирована, скорее, на объективные выражения действий ответчиков, в то время как суды США стремятся дополнительно установить цель, замысел, назначение таких действий.

В то же время развитие общеевропейских юрисдикционных правил свидетельствует, по мнению автора, о постепенном внедрении в них критериев, аналогичных разработанным судами США. Так, положения ст. 15 Регламента ЕС № 44/2001, учитывающие «направленность любыми способами» действий продавца на территорию страны, где потребитель имеет постоянное место жительства, является попыткой определить критерий «целенаправленной деятельности» на европейский манер. На это указывает, в частности, и совместная декларация Совета ЕС и Комиссии ЕС в отношении названной статьи.

Сопоставляя приведенные подходы с юрисдикционными правилами, действующими в российском праве, автор приходит к выводу о том, что критерий «целенаправленной деятельности», применяемый самостоятельно, без дополнительных, сопутствующих принципов, было бы целесообразно использовать и в правовой системе РФ.

Одновременно с этим подвергаются сомнению высказанные в научной литературе предложения о совершенствовании института международной подсудности, в том числе в пользу компетенции суда наиболее пострадавшей стороны, в пользу суда страны, в доменной зоне которой размещен спорный сайт, а также критерий места нахождения оборудования, содержащего информацию, которая привела к возникновению Интернет-спора.

Соглашаясь с мнением о необходимости внедрения в российскую правовую систему критерия целенаправленности, автор считает, что его применение возможно и без дополнительной ссылки на правила «скользящей шкалы» относительно степени интерактивности вебсайтов, как ранее предлагалось в науке.

Такой критерий уже заложен в норме п. 9 ч. 1 ст. 247 АПК РФ. Однако ее действие распространяется только на споры из оказания услуг в ассоциации сетей Интернет, а также государственной регистрации объектов (в том числе имен) на территории РФ; такое ограничение представляется некорректным.

Судам РФ должны быть подведомственны споры с участием иностранного элемента, если спорное правоотношение в целом направлено на территорию РФ. Высказываемое предложение учитывает главным образом деятельность ответчика, т. е. направленность его действий на территорию РФ, но при этом не ограничивает ее одним элементом правоотношения. Для внедрения такого правила формулируются предложения по внесению изменений в п. 9 ч. 1 ст. 247 АПК РФ.

Третий параграф второй главы **«К вопросу об общих путях решения проблемы международной подсудности Интернет-споров»** посвящен фундаментальным способам решения проблемы международной подсудности Интернет-споров.

Проблема компетенции Интернет-споров не исчерпывается технико-юридическими критериями разграничения юрисдикции. Причина, по которой суды разных стран вынуждены вырабатывать юрисдикционные критерии, заключается в том, что общее представление о компетенции формируется через понятие государственной территории.

В научной литературе предлагались разные пути развития отношений Интернета и права, но, по мнению автора, большинство из них не учитывает специфику функционирования сети Интернет и перспективы ее развития.

Эффективным способом регулирования сети Интернет может стать формирование некоторого сообщества или группы сообществ, соблюдающих, как и любое сообщество, определенные правила поведения, поддерживаемые на межгосударственном уровне. Речь, по существу, идет о создании группы пользователей Интернета, на добровольных началах принимающих на себя определенные обязательства и юрисдикцию своего сообщества.

Такое конвенциональное построение Интернет-сообществ содержит в себе предпосылки создания особых юрисдикционных правил, при которых пользователь подчиняется компетенции юрисдикционного органа такого сообщества на добровольных началах. Присоединяясь к правилам данного сообщества, он получает выгоды различного характера, обусловленные этим участием; в этом отношении его подчинение юрисдикции будет осознанным и сопряженным с получением преимуществ участника сообщества.

Компетенция юрисдикционного органа названного сообщества должна строиться исключительно по принципу членства пользователей, что позволяет говорить о возможности создания нового юрисдикционного правила в отношении Интернет-споров: если такой спор происходит между членами сообщества, он становится подсудным соответствующему юрисдикционному органу. Этот критерий компетенции юрисдикционного органа можно назвать критерием «конвенциональной компетенции».

Уже сегодня существуют реальные предпосылки для подобного регулирования отношений в сети Интернет на самых разных уровнях – от общения пользователей Интернет-форумов до деятельности Корпорации по распределению адресного пространства в сети (ICANN). Последняя давно создала и успешно использует собственные юрисдикционные правила в отношении доменных споров, которые распространяются на лиц не по территориальному принципу, а по принципу «участия» (наличия договора на «регистрацию» доменного имени).

В третьей главе **«Подведомственность и подсудность Интернет-споров»** изучаются вопросы распределения компетенции на национальном уровне.

В первом параграфе третьей главы **«Подведомственность Интернет-споров в правовой системе РФ»** исследуется специфика подведомственности наиболее показательных и распространенных категорий Интернет-споров, выявляется круг юрисдикционных органов, полномочных рассматривать Интернет-споры, обозначаются сложности и тенденции развития общих правил подведомственности, анализируются традиционные критерии подведомственности и возможность их использования в Интернет-спорах.

Исследуя в качестве критериев *характер спора* и *статус его участников*, автор обращается к проблеме разграничения подведомственности между судами общей юрисдикции и арбитражными судами на примере споров о доменных именах.

В работе доказывается, что с точки зрения действующего законодательства доменные споры с участием физических лиц должны относиться к подведомственности судов общей юрисдикции, причем независимо от того, имеет ли указанное лицо статус индивидуального предпринимателя или нет.

Однако в российской правоприменительной практике имеет место искусственное подчинение такого рода споров подведомственности арбитражных судов без четкого формулирования правил подведомственности того или иного вида. Это, по мнению автора, является одним из свидетельств локальных сбоев в применении традиционных правил подведомственности к Интернет-отношениям, что приводит к нарушению баланса между полномочиями разных юрисдикционных органов и правами участвующих в споре сторон.

При фактическом отсутствии одного из фундаментальных критериев подведомственности – критерия субъектного состава – правила разграничения подведомственности между судами общей юрисдикции и арбитражным судами становятся чересчур перегруженными. Суду на практике придется крайне глубоко вникать в природу спора (в частности, устанавливать экономический характер конкретного действия ответчика), что едва ли осуществимо и может привести к еще большим ошибкам.

Наиболее реальный путь решения этой проблемы, по мнению автора, заключается в том, чтобы характер спора не исследовался в качестве критерия подведомственности вообще. Это станет возможным, если дела данной категории будут рассматриваться по правилам специальной подведомственности.

В связи с этим обосновывается целесообразность отнесения споров о доменных именах к специальной подведомственности арбитражных судов на основе процессуального законодательства, а не судебной практики, как это имеет место сейчас, а также формулируются предложения по соответствующему изменению арбитражного процессуального законодательства.

При анализе специфики такого критерия подведомственности, как *спорность или бесспорность права*, исследуется проблема разграничения полномочий по рассмотрению Интернет-споров между органами исполнительной власти, нотариатом и судами. При этом делается вывод о том, что действующие нормы права, регламентиру-

ющие разграничение полномочий различных юрисдикционных органов на основе критерия спорности или бесспорности права, также не предназначены для урегулирования соответствующих вопросов в Интернет-спорах, вследствие чего появляются неоднозначность регулирования, а также дублирование полномочий юрисдикционных органов. Каждый такой случай должен рассматриваться отдельно и иметь самостоятельное решение.

В качестве одного из возможных способов устранения коллизий подведомственности между судами и органами нотариата по вопросам охраны прав на результаты интеллектуальной деятельности предлагается законодательно уточнить полномочия нотариусов по так называемому «депонированию» объектов авторского права.

Необходимость этого обусловлена тем, что споры о защите авторских прав при их использовании в сети Интернет являются одними из самых распространенных Интернет-споров. В связи с этим обосновывается, что нотариальная процедура имеет потенциал, чтобы считаться юрисдикционным органом, в компетенцию которого входят вопросы, связанные с «удостоверением» авторских прав лиц, размещающих свои произведения в сети Интернет. При этом подчеркивается, что процедура «депонирования» не является регистрацией авторства, а имеет целью закрепление авторской презумпции и носит, таким образом, удостоверительно-доказательственный характер.

Возможность «депонирования» объектов авторского права позволит предоставить дополнительную защиту авторам, чьи произведения публикуются или активно используются в сети Интернет. Предварительное (до размещения в сети) депонирование станет не только иметь доказательственное значение в том случае, если дело будет рассматриваться судом, но и носить превентивный характер, способствуя досудебному решению возможных споров относительно защиты авторских прав. По нашему мнению, в дальнейшем такую нотариальную процедуру целесообразно было бы распространить также на объекты, выраженные в цифровой форме.

В соответствии со сказанным формулируется предложение о внесении соответствующих дополнений (отдельной главы) в разрабатываемый закон «О нотариате и нотариальной деятельности в РФ».

При исследовании такого критерия подведомственности, как *наличие договора между сторонами*, автор приходит к выводу о том,

что он наиболее специфичным образом проявляется в отношении Интернет-споров.

Анализ правовой основы деятельности различных негосударственных специализированных центров по рассмотрению Интернет-споров и юридической природы их компетенции позволил автору прийти к выводу, что возможность рассмотрения Интернет-споров негосударственными специализированными центрами законодательством РФ не предусмотрена. Ни специализированные центры, ни какие-либо иные органы третейского характера не являются юрисдикционными с точки зрения действующего законодательства и соответственно не могут претендовать на возможность включения в традиционный институт подведомственности.

Проведенный анализ компетенции таких специализированных центров с точки зрения всех существующих в российском праве критериев подведомственности позволяет сделать вывод, что наиболее близким критерием подведомственности, связанным с разграничением полномочий этих органов и государственных судов, является критерий наличия договора между сторонами.

Однако компетенция международных центров, действующих, к примеру, под эгидой корпорации ICANN, по существу основывается на «квазитретейских» соглашениях пользователей, существование которых российским законодательством не предусмотрено.

Таким образом, для того чтобы система негосударственных органов по рассмотрению любых категорий Интернет-споров начала действовать, необходимо концептуально переосмыслить ряд существующих юрисдикционных правил с учетом специфики сети Интернет, так как компетенция этих органов является «конвенциональной», а не «территориальной».

Во-первых, требуется модифицировать такой критерий подведомственности, как наличие договора между сторонами, чтобы интегрировать компетенцию негосударственных правоприменительных органов в институт национальной подведомственности.

Во-вторых, необходимо разграничивать полномочия национальных судов и специализированных комиссий в соответствии с правилами императивной подведомственности, когда обращению в национальный суд должно обязательно предшествовать обращение в такой центр.

Применение соответствующего правила императивной подведомственности могло бы рассматриваться в порядке ч. 5 ст. 4 АПК

РФ как расширенная часть досудебного порядка разрешения споров, предусмотренного федеральным законом в отношении Интернет-споров, в частности споров о доменных именах.

Во втором параграфе третьей главы **«Подсудность Интернет-споров в правовой системе РФ»** исследуются практические проблемы подсудности отдельных категорий дел, связанных с использованием сети Интернет; обосновывается необходимость совершенствования правил территориальной подсудности Интернет-споров.

На сегодня действие традиционных, общих для всех категорий дел правил функциональной и родовой подсудности не вызывает, по крайней мере, пока, каких-либо существенных сложностей при рассмотрении дел, связанных с использованием сети Интернет. Однако сказанное не относится к подсудности территориальной – общие правила подсудности, установленные действующим законодательствам, не в полной мере отвечают специфике Интернет-отношений.

Так, одной из разновидностей Интернет-споров, подсудность которых является специфической, выступают дела, связанные с порядком формирования федерального списка экстремистских материалов в соответствии с Федеральным законом «О противодействии экстремистской деятельности». Вопрос о том, подлежат ли такие дела рассмотрению в порядке гражданского или административного судопроизводства, до сих пор остается открытым. Но несмотря на это, содержащиеся в данном Федеральном законе правила подсудности являются уникальным для российского права примером особых юрисдикционных правил рассмотрения Интернет-споров. По существу, это пример реализации принципа «летучей подсудности», действующего в праве Германии, так как данные правила позволяют органам прокуратуры фактически любого субъекта РФ обращаться с заявлениями о признании обнаруженных в Интернете материалов (а также целых web-сайтов) экстремистскими в суд по месту их обнаружения.

Вместе с тем хотя необходимость в создании такого рода правил подсудности обусловлена особым характером объекта правоотношений и необходимостью защиты публичных интересов, правила подсудности этих дел не являются совершенными и необоснованно нарушают баланс прав и законных интересов заинтересованных лиц и государства.

В связи с этим предлагается включить нормы, посвященные порядку признания информационных материалов экстремистскими,

в ГПК РФ, для чего формулируются соответствующие изменения в законодательство. В частности, высказывается предложение о включении норм, посвященных порядку признания информационных материалов экстремистскими, в раздел ГПК «Производство по делам, возникающим из публичных правоотношений» в виде отдельной главы. В ней предлагается сформулировать положение о том, что компетенция федеральных судов по рассмотрению споров, связанных с признанием экстремистскими информационных материалов в сети Интернет, должна определяться по правилам исключительной подсудности: по месту нахождения Генеральной прокуратуры Российской Федерации.

Изучение проблем территориальной подсудности Интернет-споров, в том числе выявленных в правоприменительной практике российских судов, позволило обосновать предложение о введении дополнительного правила территориальной подсудности.

По нашему мнению, наиболее перспективным является подход, согласно которому споры, связанные с использованием сети Интернет, по выбору истца могут также рассматриваться в месте, на которое были направлены действия ответчика. Целенаправленность подразумевает осознанную и умышленную направленность лицом своих действий либо сознательное допущение возможной их направленности.

Дела, связанные со спорами о доменных именах, согласно этому критерию будут рассматриваться по месту нахождения истца, если будет обосновано, что ответчик при регистрации доменного имени осознанно направлял свою деятельность на территорию, где расположен истец.

Сказанное относится и к спорам, связанным с нарушением авторских прав. Для подачи иска по месту нахождения истца необходимо представить доказательства того, что ответчик, совершая факт нарушения авторских прав, умышленно направлял свои действия против интересов истца, и тем самым целью его действий была территория, где истец зарегистрирован.

Такое правило могло бы стать дополнительным способом защиты обладателя прав на результаты интеллектуальной деятельности и приравненные к ним средства индивидуализации юридических лиц, товаров, работ, услуг.

И хотя принятие высказанных предложений об изменении правил территориальной подсудности в пользу критерия «целенаправленно-

сти» действий несколько усложнит институт подсудности и сделает это еще более существенным обстоятельством дела, такая мера является вынужденно необходимой.

В условиях «экстерриториальной эпохи» действующие правила подсудности следует адаптировать к существующей правовой реальности. Иначе адекватная защита прав участников Интернет-отношений будет невозможна.

В **заключении** изложены основные выводы диссертационного исследования.

В **приложении** даны сформулированные автором предложения о внесении изменений в действующее законодательство.

По теме диссертации опубликованы следующие работы

Статьи, опубликованные в ведущем рецензируемом научном издании, указанном в перечне ВАК

1. *Незнамов А. В.* Наличие договора между сторонами как критерий подведомственности доменных споров // Арбитражный и гражданский процесс. – 2010. – № 2 – С. 11–15 (0,55 п. л.).

2. *Незнамов А. В.* Наличие договора между сторонами как критерий подведомственности доменных споров // Арбитражный и гражданский процесс. – 2010. – № 3. – С. 2–5 (0,45 п. л.).

Статьи, опубликованные в иных изданиях

3. *Незнамов А. В.* Доказательства в Интернет-спорах // Арбитражное правосудие в России. – 2007. – № 8. – С. 77–93 (1 п. л.).

4. *Незнамова З. А., Незнамов А. В.* Клеветническая информация в сети Интернет: коллизии уголовно-правовой и гражданско-правовой юрисдикции // Уголовная политика в сфере информационной безопасности РФ: материалы конференции. – Екатеринбург, 2007. – С. 25–33 (0,45 п. л.).

Подписано в печать 19.05.10. Формат 60×84/16.
Бумага писчая. Печать офсетная.
Усл. печ. л. 1,63. Уч.-изд. л. 1,55.
Тираж 100 экз. Заказ № 45

Отдел дизайна и полиграфии
Издательского дома
«Уральская государственная юридическая академия».
620066, Екатеринбург, ул. Комсомольская, 23

Private International Law and the Internet

Dr. Dan Jerker B. Svantesson
B.A. (LTU, Sweden), M.A. (LTU, Sweden),
LL.M. (UNSW, Australia) Ph.D. (UNSW, Australia)

KLUWER LAW
INTERNATIONAL

I. THE IDEA IN FOCUS: THE 'BORDERLESS' INTERNET – FROM THE ILLUSION OF A 'NO MAN'S LAND' TO THE REALITY OF AN 'EVERY MAN'S LAND'

Different forms of Internet communication have different sets of characteristics. Some forms of Internet communication, such as communication via the World Wide Web, have a set of characteristics that make them fundamentally different to other forms of communication (*see further* Chapter 2). When existing rules of private international law are applied to, for example, World Wide Web communication, the effect is in some cases that these rules get an unprecedented wide application – acts done over the World Wide Web can, under certain circumstances, come under the jurisdiction of virtually each and every state where persons are connected to the Internet (*see further* Chapter 9). As national laws vary from state to state, this has serious implications. The Internet, or Cyberspace, has been transformed from what arguably was a no man's land, where no laws were seen to apply, to something that more realistically can be described as an 'every man's land', where the laws of all states apply at the same time.

The term 'every-man's land' can here be given two equally interesting and correct interpretations. First, the Internet has become an every-man's land, in that it is used by an enormous amount of people from a range of social and economical backgrounds (it should be remembered, however, that Internet access is very rare in the poorest regions in the world). Second, the Internet is now an 'every-man's land' as the total opposite of the international law term 'no-man's land' – instead of not being under the control of any country's jurisdiction, the Internet is within each and every country's jurisdiction at the same time. Indeed, already in 1997, it was observed that '[t]he Net is not an anarchic, unregulated dominion above and beyond individual state control, but rather a terrain policed by varied, numerous, and often contradictory national laws that create a variety of regulatory fiefdoms'.[4]

Many commentators, including me, have viewed this as a problem. However, perhaps that is inaccurate. Perhaps a line from the lyrics of John Lennon's classic *Watching the Wheels* more accurately describes the situation: 'there's no problem, only solutions'. These different solutions have different implications, and what we need to do is not to solve a problem, but to make a decision as to *which* solution out of a range of possible solutions, we want to employ to address the current situation.

There are at least three possible 'solutions' addressing the implications of the situation outlined above. First, all states' substantive laws could be harmonized, thereby creating a situation where it does not matter which state's law is used to determine a dispute. However, in relation to most legal areas, that is probably not a realistic option within a foreseeable future. Second, the Internet could be treated as a separate legal space with separate regulation and a separate judiciary (i.e. placing borders *around* the Internet). This alternative is interesting *de lege ferenda*, and, as I have illustrated elsewhere, there are several solid reasons justifying further research

4. V. Mayer-Schönberger and T.E. Foster, 'A Regulatory Web: Free Speech and the Global Information Infrastructure' (1997) 3 *Michigan Telecommunications and Technology Law Review*, 50.

into that alternative.[5] However, as I have also highlighted, such an approach is associated with serious difficulties.[6] Third, protective borders could be raised *on* the Internet. Private international law has the capacity to erect such borders, but perhaps so does the Internet architecture itself (*see further* Chapter 10). Although all these alternatives are interesting, it is the latter – the placing of borders *on* the Internet – which constitutes the focus of this book.

A sensible harmonization of private international law (i.e. making the jurisdictional claims fit with each other, as well as with the rules for recognition and enforcement)[7] could erect protective borders that would ensure that acts done over the Internet would not be exposed to the jurisdiction and laws of an overwhelmingly large number of states. However, such a harmonization will not be easily accomplished. Currently, states in general make much wider jurisdictional claims than they accept from other states when examining whether to recognize and enforce foreign judgments. This gap between what is regarded as reasonable grounds for jurisdictional claims and what is seen as reasonable grounds for the recognition and enforcement of foreign judgments has been considerably widened through, for example, the World Wide Web's set of characteristics. Although it is not necessary to close this gap entirely, it is necessary to bridge it in part. The best way to achieve the desired harmonization is through the creation of well-balanced international instruments (*see further*: Chapters 11 and 12).

II. THE SUBSTANTIVE FOCUS

The substantive focus of this book may be divided into two parts – issues and areas of law. The issues dealt with are jurisdiction, choice of law and recognition and enforcement of judgments. These three issues constitute private international law. The areas of law addressed are contracts (including consumer contracts) and the tort of defamation. Private international law could also be viewed as an area of law, but for the purpose of clarifying the substantive scope of this book, that would be unworkable. Instead private international law should be viewed as the mortar that surrounds the bricks (the bricks being areas of law, like contracts or defamation).

Either way, joining these two parts together the substantive focus can be summarized to be jurisdiction, choice of law and recognition and enforcement in contracts and defamation. However, as is hinted at by the book's title, further limitations are placed on the substantive focus: only 'Internet contracts' and 'Internet defamation' fall within the substantive scope. This is because what I wish to explore are the issues raised by the Internet as a medium for communication. This limitation makes

5. *See further*, D. Svantesson, 'Borders on, or border around – the future of the Internet' (2006) 16(2) *Albany Law Journal of Science & Technology*, 343.
6. *Ibid.*
7. The term 'harmonization' is used in different manners in different contexts. However, when the term is used in this book, in the sense it is used above, it refers to making the jurisdictional claims fit with each other as well as with the rules for recognition and enforcement.

it necessary to distinguish between, 'Internet contracts' and 'Internet defamation' on the one hand, and 'non-Internet contracts' and 'non-Internet defamations' on the other hand. 'Internet contracts' are contracts either formed or performed over the Internet, and 'Internet defamation' is the spreading of (allegedly) defamatory information over the Internet. If someone, for example, enters into a contract for the purchase of a book at www.amazon.com, that contract falls within the definition of 'Internet contract', although the physical book may not be delivered via the Internet. Similarly, if someone receives, prints out and then reads an e-mail containing defamatory material, the dissemination of that material will still fall within the category of 'Internet defamation', although the person did not read the material directly off the computer screen. In summary, the requirement for the contracts and defamations to be 'Internet contracts' and 'Internet defamations', should be given a rather wide interpretation, in relation to the substantive scope. A narrower approach would risk missing the 'bigger picture'.

Finally, it should also be noted that only international contracts and defamations fall within the substantive scope. There is one self-evident and one practical reason for this limitation. A totally domestic dispute in a non-federation simply does not give rise to any private international law issues, and as the conflict issues associated with a federal structure vary from federation to federation (such as the United States and Australia), addressing them is not practical in a study that takes account of seven different jurisdictions. Consequently, if a Swedish citizen, located in Sweden, defames another Swedish citizen, also located in Sweden, by posting something defamatory on a website located in Sweden, and only citizens of Sweden, located in Sweden, access the material so that no damage is suffered anywhere but in Sweden, the dispute would fall outside the scope. However, as it is likely that such a case would give some indication as to how a Swedish court would act in international Internet defamation cases, the case might very well be of interest anyhow. Similarly, this main delimitation excludes disputes between people located in two different states of a federation. However, perhaps even more than judgments in domestic disputes in non-federations, the judgments in such disputes are likely to provide important clues as to how the courts would view international disputes and can, thus, be used as examples. Against this background, it appears sensible to also view a dispute between one party in Hong Kong SAR and one party in the People's Republic of China (PRC) as a domestic dispute, and no particular effort has been made to discuss present or future special arrangements between Hong Kong and the PRC relating to, for example, recognition and enforcement.

A. Issues[8]

Together the three different components: jurisdiction, choice of law and recognition and enforcement make up what we somewhat inaccurately call private international

8. This part of the book draws upon D. Svantesson, 'Jurisdictional Issues and the Internet – A Brief Overview' (2003) *Cyberspace 2003: Normative Framework*, Brno Czech Rep. and D. Svantesson, 'An Introduction to Jurisdictional Issues in Cyberspace' (2006) 15 *Journal of Law and Information Science*, 50–74.

law (or conflict of laws).[9] While the three different components can be looked at separately without much problem, they are intricately interconnected. If a judgment cannot be recognized and enforced there is ordinarily little point in seeking a forum that will render a judgment. The corollary of this is that there is little comfort in knowing that a judgment could be recognized and enforced if one cannot find a forum that will render a judgment. The connection between jurisdiction on the one hand, and the recognition and enforcement on the other, is widely acknowledged. However, similar connections exist also in relation to choice of law. If the rules of a state, for example, provide that the applicable law always is the law of the forum (*lex fori*) that state's approach could be accused of being parochial and antiquated. Yet, if the same state's jurisdictional laws are very restrictive and only allow for jurisdiction where all connecting factors are pointing towards the courts of the state in question, the application of *lex fori* is perfectly understandable. Finally, one can observe the connection between the choice of law and recognition and enforcement. For example, in evaluating whether or not it is reasonable to recognize and enforce a foreign judgment it is suitable to take into consideration whether the judgment was rendered under a law that had a reasonable connection to the dispute.

The conclusion must be that one cannot make suggestions as to the structure of, for example, a state's jurisdictional rules without also considering the components of choice of law and recognition and enforcement. As this book aims at making concrete suggestions for the regulation of both Internet defamation and Internet contracts, it is necessary to approach private international law as a system (i.e. to take account of all three of the components of private international law).

1. Jurisdiction

> *The Internet is an international system as stated by the U.S. Supreme Court in the Reno-2 case. Therefore jurisdiction is a primary and basic question, which is essential in every case involving the Internet.*[10]

The term 'jurisdiction' carries more than one meaning. As is pointed out in the decision of the High Court of Australia in the *Gutnick* case,[11] jurisdiction refers both to 'the amenability of a defendant to process in such a way as will give a court authority to decide the controversy which that process seeks to agitate and, second, as referring to a particular territorial or law area or law district'.[12] The term 'jurisdiction' will be used for both these purposes in the book, but mainly in the former of the two meanings identified in the quote above.

Ordinarily, the first issue a court will consider in a cross-border dispute is whether or not it has jurisdiction to hear the dispute. A court must have both

9. *See further* F. Vischer, 'General Course on Private International Law' (1992-I) 232 *Recueil des cours*, 199–201.
10. H. Spang-Hanssen, *Cyberspace Jurisdiction in the U.S. – The International Dimension of Due Process* (Oslo, Norwegian Research Centre for Computers and Law, 2001), p. 1.
11. *Dow Jones & Company Inc. v. Gutnick* (2002) 210 CLR 575.
12. *Dow Jones & Company Inc. v. Gutnick* (2002) 210 CLR 575, 597.

subject-matter jurisdiction (i.e. jurisdiction over the type of dispute concerned) and personal jurisdiction (i.e. jurisdiction over the parties involved in the dispute). In practice, the subject-matter jurisdiction criterion simply means that a plaintiff cannot, for example, turn to the family court in relation to an intellectual property dispute. Another example would be that a party must initiate the proceedings at an appropriate court level; one cannot ordinarily turn to the highest court of a state at an initial stage of litigation. The criterion of personal jurisdiction or *in personam* jurisdiction, on the other hand, can give rise to more complex issues and is the focus for the discussion of jurisdiction.

The rules regulating jurisdictional claims are mainly location focused. For example, the court might query where the disputed contract was formed,[13] where the contract was broken,[14] where the contract was performed,[15] where the tort was committed,[16] where the damages were suffered,[17] where the server is located,[18] and where the defendant is located, domiciled or habitually residing.[19] While the jurisdictional grounds in contractual disputes often point to the court in one of the contractual parties' home state, the jurisdictional grounds relating to torts are extremely wide when applied in the Internet context. For example, damages stemming from the tort of defamation can occur virtually anywhere, which means that a defendant in a defamation proceeding might be subjected to a wide range of jurisdictional claims.

It is also common for the question of jurisdiction to be regulated in contracts (choice of forum clauses).[20] The issues associated with such practice are discussed below in relation to choice of law clauses (which are also very common). Here it is sufficient to note that restrictions may be placed on the validity of choice of forum

13. E.g., *General Rules of Procedure in Civil Proceedings* 1996 (Vic) 7.01 (1) (f) (i); *Law of Civil Procedure of the People's Republic of China* 1991, Article 243.
14. *Ibid.*
15. E.g., Council Regulation (EC) No. 44/2001 of 22 December 2000 on Jurisdiction and the Recognition and Enforcement of Judgments in Civil and Commercial Matters, OJ L12/1 2001. (Brussels Regulation 44/2001), Article 5(1); *Law of Civil Procedure of the People's Republic of China (1991)*, Article 243.
16. E.g., Brussels Regulation 44/2001, Article 5(3); *General Rules of Procedure in Civil Proceedings* 1996 (Vic) 7.01 (1) (i); *Law of Civil Procedure of the People's Republic of China (1991)*, Article 29.
17. *Ibid.*
18. E.g., *Interpretation of the Supreme People's Court on Application of Laws When Trying Dispute Cases Concerning Computer Network Copyright*, 22 November 2000, The Supreme People's Court, Article 1.
19. E.g., Brussels Regulation 44/2001, Article 2; *General Rules of Procedure in Civil Proceedings* 1996 (Vic) 7.01 (1) (c); *Law of Civil Procedure of the People's Republic of China (1991)*, Article 22.
20. For an example of Australian rules providing for such choices, *see General Rules of Procedure in Civil Proceedings* 1996 (Vic) 7.01 (1) (h); As far as the People's Republic of China is concerned, *see Law of Civil Procedure of the People's Republic of China (1991)*, Article 25 for domestic contracts and *Law of Civil Procedure of the People's Republic of China (1991)*, Article 244 for foreign-related contracts; *See also* Brussels Regulation 44/2001, Article 23 for the European position.

clauses. For example, Article 16 of the relevant European instrument, the *Brussels I Regulation* 44/2001, overrides choice of forum provisions and, a little simplified, provides protection for a consumer to the extent that the consumer may sue the seller in the consumer's home state while, at the same time, the business can only sue the consumer in the consumer's home state (*see further* Chapter 8.I.A).

For the parties, the question of jurisdiction is important for several reasons. Typically, a party may want the dispute to be heard in its home state for practical reasons; for example, due to confidence in, or familiarity with, the local court system, or to minimize that party's own expenses while increasing the other party's expenses. Often, however, a more important consideration is the fact that the choice of forum determines which court will adjudicate the matter, which in turn decides which choice of law rules will apply, which in turn determines the applicable law, and the substantive law being applied determines which party will win the dispute. Thus, when a party disputes a court's jurisdiction, it often does so with the question of applicable law in mind. Further, it must be noted that even where the court concludes that a foreign substantive law is applicable, it will nevertheless apply its own procedural law, and in some cases the procedural rules are determinative (e.g., rules regulating admissibility of evidence, trial by jury, etc.).

From a normative perspective, the jurisdictional dilemma is essentially that too wide jurisdictional claims are unjust towards the defendant, while too narrow jurisdictional claims might deprive the plaintiff of legal remedies.

Further, it should be noted that, the concept of jurisdiction is central in international law. Indeed, a state that cannot exercise any jurisdiction is arguably not a state at all:

> It is an essential attribute of the sovereignty of this realm, as of all sovereign independent states, that it should possess jurisdiction over all persons and things within its territorial limits and in a cases, civil and criminal, arising within these limits.[21]

The issue of jurisdiction should be viewed from at least two perspectives. For the parties, the question is: in which forum(s) can the matter at hand be heard? For the judge(s), the question is: can this forum exercise jurisdiction over the matter at hand? If the judge(s) conclude(s) that the forum can exercise jurisdiction over the matter at hand, two more questions may be asked: Does the court have the power to decline to exercise jurisdiction? And, if yes, should the court decline to exercise jurisdiction? While the rules regulating the courts' right to exercise jurisdiction are fairly similar from state to state, the courts' power and willingness to decline jurisdiction varies considerably from state to state, as is discussed below in the country-specific chapters (Chapters 4–8).

---

21. Statement made by Lord Macmillan in *The Christina* 1938 AC 485, 496–497 (As reproduced in T. Hiller, *Sourcebook on Public International Law* (London, Cavendish Publishing Ltd, 1998), p. 250)

2. Declining Jurisdiction

> *It seems to me [. . .] that that [the issue of forum non conveniens] is the place in which the Internet problem is going to be solved in the world. Countries are going to say, 'Of course we've got jurisdiction. The damage happened here or some other – we can serve here but it is much more convenient that this matter be litigated in another place'.*[22]

Generally speaking, the courts of states following the civil law tradition have less discretionary power to decline jurisdiction than do their common law counterparts.[23] Many civil law states are limited to declining jurisdiction based on the doctrine of *lis alibi pendens* (i.e. a suit pending elsewhere).

In common law countries, and to an extent in some civil law countries like Sweden, courts have the option of declining to exercise jurisdiction under the doctrine of *forum non conveniens*. The interpretation of this doctrine, however, varies greatly. For example, in most common law countries, a court will decline jurisdiction if there is another more appropriate forum, while under Australian law, a court will decline jurisdiction only if the court is a clearly inappropriate forum (*see further* Chapter 4.II.A).

Further, the quote introducing this section should make clear the important role that the doctrine of *forum non conveniens* plays in common law countries. Yet, at a first glance, the current trend of suing only in relation to local damages would appear to negate the value of the doctrine. For example, the courts in the *Gutnick*[24] case, the *Harrods*[25] case and the *Investasia*[26] case found no reason to decline jurisdiction since the plaintiffs' actions were related only to harm suffered within the respective states, and which court could be more suitable to determine a dispute relating exclusively to damages suffered within state X, than the court of state X? This line of reasoning certainly has a logical appeal, but at the same time it could perhaps be described as a simple trick by which the plaintiff circumvents the doctrine of *forum non conveniens*. However, the plaintiff does so at the expense of only being awarded damages for harm done within the state where the court is located. Consequently, even though the doctrine of *forum non conveniens* might not protect a foreign defendant from being sued in a certain forum, it might have the effect of preventing the plaintiff from seeking damages in relation to harm alleged to have occurred in multiple jurisdictions.

---

22. Transcript of High Court hearing of *Dow Jones & Company Inc. v. Gutnick*, 28 May 2002, points 1484–1487.
23. For further information on this, *refer to*: J. Fawcett (ed.), *Declining Jurisdiction in Private International Law* (Oxford, Clarendon Press, 1995).
24. *Dow Jones & Company Inc. v. Gutnick* (2002) 210 CLR 575.
25. *Harrods Ltd v. Dow Jones & Company Inc.* [2003] EWHC 1162 (QB).
26. *Investasia Ltd and Another v. Kodansha Co. Ltd and another* [1999] HKCFI 499.

3. Choice of Law

Few rules are so often sabotaged by the courts as the choice of law rules.[27]

While it has been described as 'the central topic of the law of conflict of laws',[28] the question of choice of law should, as highlighted above, not be discussed without the issue of jurisdiction also being addressed. If a court finds itself to have jurisdiction, it will turn to the question of which law should be applied. As the applicable law is the standard that ultimately will decide which party is successful, the choice of law question could, from a certain point of view, be said to be the most important question. Either way, also the choice of law rules focus primarily on locations as is exemplified in the widely spread choice of law rule in torts, *lex loci delicti* (i.e. the law of the place of wrong).[29] While the detailed manner in which the *lex loci delicti* rule is applied varies somewhat from state to state, a common feature is that it often favours the *lex fori* (i.e. the law of the forum). For example, under Australian law the *lex loci delicti* rule appears 'neutral' as it simply points to the place of wrong. However, the underlying rules of defamation law are biased towards the *lex fori*. Since the tort of defamation is deemed to have been committed where the defamatory material enters the mind of a third person, it is fairly easy to ensure that the *lex loci delicti* points to the *lex fori* – all you need to do is to show that somebody within Australia (or, more exactly, the desired Australian state) read or heard the defamatory material.[30]

A very important distinction between jurisdiction and applicable law is that it is widely considered that, while jurisdictional rules very well can point to more than one forum, the choice of law rules should identify one applicable law only. Current location-focused choice of law rules do not always do so, and indeed, in an Internet context it might be difficult to sensibly identify one single law. This is discussed in detail below (*see* Chapter 9.III.F).

More generally, the normative dilemma in relation to choice of law could be said to be that each state has a legitimate interest in applying its laws to acts done,

---

27. O. Lando, 'Lex Fori in Foro Proprio' (1995) 2(4) *Maastricht Journal of European and Comparative Law*, 371.
28. A.A. Ehrenzweig, *A Treatise on the Conflict of Laws* (St. Paul, Minn, West Publishing Co., 1962), p. 1.
29. The *lex loci delicti* rule is, for example, applied in Australia (*see Regie National des Usines Renault SA v. Zhang* (2002) 210 CLR 491), and is also suggested to be the main rule (Article 3) in the proposed European *ROME II Regulation on the Law Applicable to Non-contractual Obligations* (*see further* Proposal for a Regulation of the European Parliament and the Council on the law applicable to non-contractual obligations (ROME II) COM/2003/0427 final – COD 2003/0168). As far as the People's Republic of China is concerned, it can be noted that a form of the *lex loci delicti* rule is applied (*General Principles of the Civil Law of the People's Republic of China*, Article 146(1)), but the details around its application are somewhat unclear.
30. As was discussed in relation to the courts' option to decline jurisdiction, it is common for the plaintiff to limit the claim to damages suffered within the forum. In addition to the consequences this has in relation to the courts' option to decline jurisdiction, it also insures that the *lex fori* is applied to the entire dispute.

or having a real or potential effect, in their respective territory. As different states have different laws, actors on the Internet might have to consider and adjust their conduct to a confusing patchwork of laws.

4. Recognition and Enforcement of Judgments

> *Even before obtaining a judgment in his client's favor, counsel should plan how to enforce the judgment. When the judgment debtor has sufficient assets within the jurisdiction of the court rendering the decision, the problem should be one of merely complying with local procedures. However, enforcement becomes more complicated when there are no or insufficient assets within the judgment jurisdiction to satisfy the judgment debt.*[31]

While the focus of literature relating to jurisdictional issues and the Internet is often placed on the strongly connected, and often entwined, issues of jurisdiction and choice of law, the recognition and enforcement of judgments are vital and decisive components of private international law and must not be overlooked. After all, it is often of little use for a party to know that a court of a particular country can claim jurisdiction and will apply a particular country's law, if the subsequent judgment cannot be enforced in a forum where the other party has assets.[32] Getting a judgment recognized and enforced in a foreign forum is seldom easy and, in a sense, the general complexity of getting foreign judgments recognized and enforced in a forum in which the defendant has assets works as a protection for defendants in international litigation.

There are also other more basic reasons for studying recognition and enforcement. As noted above, it is necessary to bridge the gap between what can be regarded as reasonable grounds for jurisdictional claims and what can be seen as reasonable grounds for the recognition and enforcement of foreign judgments. This cannot be done without an in-depth examination of the rules for recognition and enforcement.

A few words should also be said about the distinction between 'recognition' and 'enforcement'. Recognition means basically that the foreign judgment is viewed as having the effect it has in its state of origin, while the enforcement of a foreign judgment means to 'compel compliance [. . .] through means such as attachment, committal, fine, sequestration, or execution'.[33] Thus, as noted in *Dicey and Morris on The Conflict of Laws*, 'while a court must recognize every foreign judgment which it enforces, it need not enforce every foreign judgment which it recognizes'.[34]

---

31. D. Campbell and D. Popat, 'Enforcing American Money Judgments in the United Kingdom and Germany' (1993–1994) 18 *Southern Illinois University Law Journal*, 517.
32. Of course, also a judgment that cannot be enforced can have a moral value. For example, a judgment in favour of a plaintiff in a defamation case might very well carry great value as 'evidence' that the defamatory material was untrue. However, this sort of moral value should be kept separate from the legal value discussed in the text above.
33. P. Nygh and P. Butt, *Butterworths Concise Australian Legal Dictionary* (2nd edn, Sydney, Butterworths, 1998).
34. L. Collins *et al.* (eds), *Dicey and Morris on The Conflict of Laws* (13th edn, London, Sweet & Maxwell, 2000), p. 468.

B. AREAS OF LAW

1. Contracts

The focal point of international trade is the contract.[35]

Contracts play a central role in all commerce, and have done so for many years. Consequently, electronic contracts are a novelty only in form and not substance. Although, historically the people of the states examined in this book have viewed contracts differently,[36] contracts are viewed as equally important in all jurisdictions today.

Certain types of contracts may generally not be concluded at all in electronic form; for example, contracts for the sale of immovable property. As consumer contracts constitute an important part of this book, it is reasonable to focus on the types of contracts that commonly are concluded by consumers via the Internet. Goods and services contracts are the most obvious choices. However, not all types of goods and not all types of services are discussed. Some types of goods and services contracted for over the Internet are governed by specific regulations, and are often geographically limited. For example, areas such as Internet banking, Internet gambling and the provision of medical services over the Internet are heavily regulated and associated with particular difficulties that are atypical for 'ordinary' Internet contracts. Others, like domain name contracts, are subjected to specific forms of dispute resolution. Such contracts are not discussed in this book.

Special complications arise when the product contracted for is a so-called 'digitized' product. These issues are discussed in Chapter 10.III.D.1.

The contractual situations dealt with can suitably be divided into two separate categories – contracts stipulating a forum and/or law, and contracts without forum and law selections. These two kinds of situations will obviously raise similar issues (i.e. which forum shall decide and which law shall be applied). However, very different considerations are of relevance. If the contract includes a forum and/or a law selection clause at least two questions needs to be examined:

- Is the selection exclusive?
- Are there any reasons to disregard the forum and/or law selection clause(s)?

In the absence of forum and/or law clauses the only question(s) to be raised is/are: which forum shall decide the dispute and/or which law shall be applied when deciding the dispute?

---

35. L. Marasinghe, *Principles of International Trade Law* (Singapore, Butterworth Asia, 1998), p. 1.
36. While contracts have a long history in western countries, it should be noted that up until recently in the PRC, contracts were seen more as an expression of 'a long-term cooperative and friendly relationship' than a legal instrument with attached ramifications (K H. Wang, *Chinese Commercial Law* (Melbourne, Oxford University Press, 2000), p. 37).

2. Consumer Contracts

To include consumer contracts is only natural since this type of contract is a large and growing part of e-commerce. It was recently estimated that consumer purchases constituted one third of the value of the world e-commerce.[37] Considering the fact that consumer purchases often involve relatively small values compared to business-to-business (B2B) contracts, it is reasonable to assume that consumer contracts represent considerably more than one third of the total number of contracts. Studying consumer contracts is also interesting as this is an area associated with particular problems, such as a low delivery rate. This type of problem is presumably rare in B2B contracts where large amounts of money are involved and the parties regularly know each other before hand.

The very fact that consumer contracts ordinarily involve small amounts of money gives rise to further complications. For the consumer, it is seldom economically feasible to initiate an international law suit against a foreign business. Indeed, the consumers may be left without effective remedies.

3. The Tort of Defamation

> *Clearly, the law of defamation represents the perfect lens through which to examine the adequacy of traditional choice-of-law regimes in cyberspace.*[38]

It is fruitful to place contracts in contrast to a tort. 'Tort' is here, and throughout the book, given a somewhat looser meaning than the common law term has in its purest form. The reason is obvious. Civil law states do not identify torts in the manner common law states do. Instead civil law systems often speak of non-contractual damages and the like.[39] Thus, the term tort is generally given the meaning of non-contractual damages.[40]

Defamation was a logical choice as the Internet already has given rise to a number of jurisdictional disputes relating to defamation worldwide. While the reasons for this are manifold, and may vary from state to state, one is that:

> The Internet is a highly effective instrument for bringing news and information rapidly to people. But the economic competitiveness and round-the-clock

37. N. Rosner, 'International Jurisdiction in European Union E-Commerce Contracts' <www.llrx.com/features/eu_ecom.htm>, Published 1 May 2002 (Last visited 25 April 2006).
38. P.A. Davis, 'The Defamation of Choice-of-Law in Cyberspace: Countering the View that the Restatement (Second) of Conflict of Laws is Inadequate to Navigate the Borderless Reaches of the Intangible Frontier' (2002) 54 *Federal Communications Law Journal*, 341.
39. *See*, e.g., X. Zeng, 'Can a Foreign Company Contract Out of a Chinese Court? A Comparison of the American and Chinese Legal Systems Regarding the Enforceability of the Arbitration Clause in a Commercial Contract' (1994–1999) 8 *China Law Reporter*, 97.
40. Note, however, that the term 'tort' obviously maintains its ordinary meaning in those country-specific chapters that deal with common law states.

> nature of Internet journalism also contribute to sensationalism and rumor-mongering, to a merging of news, advertizing, and entertainment, and to an apparent decline in serious reporting and commentary.[41]

With this in mind, there might be a greater rather than lower need for defamation regulation on the Internet than in 'real space'. Furthermore, a recent survey carried out by the American Bar Association and the International Chamber of Commerce states that:

> Of those sectors polled by the survey, the media sector was clearly the most affected by Internet jurisdiction. For example, more than half of media company respondents indicated that they have adjusted their business operations in response to Internet jurisdiction risk.[42]

Further, defamation is a very interesting area of law as regulation of defamation requires the balancing of two basic human rights; freedom of expression and the protection of reputation. Both these rights are protected as equally important under recognized international law, such as the *International Covenant on Civil and Political Rights*. It is also interesting to note that defamation law is an area where states often are rather protective. The citizens' right of freedom of expression and the protection of reputation go to the very core of the society, and are often said to be of fundamental importance in democratic societies. This might very well mean that states would be reluctant to enter into agreements relating to defamation law, or private international law rules regulating defamation.

Just as with contracts, it is necessary to examine the information tort of defamation in detail to understand the private international law implications. For example, it is not sufficient to know that the current choice of law rule in Australia is the so-called *lex loci delicti* – the law of the place of wrong. It is obviously vital to also understand which place is considered to be the 'place of wrong' under defamation law.

Furthermore, as jurisdiction and choice of law, as well as recognition and enforcement, in relation to criminal defamation fall outside the scope of private international law, only the civil aspects of defamation are covered. In this context it must, however, be noted that also criminal acts, such as criminal defamation, give rise to the same sort of issues as civil acts do. In fact, in some instances it may not be practical to draw a sharp distinction between a criminal act and its civil implications. It is, for example, not rare for the victim of a crime to be able to take civil action seeking compensation. In light of this, the reader must be aware that, while criminal defamation, as such, falls outside the scope, civil implications of criminal defamation necessarily fall within the scope.

---

41. 'Ethics in Internet, Pontifical Council for Social Communications' *Vatican City*, <www.vatican.va/roman_curia/pontifical_councils/pccs/documents/rc_pc_pccs_doc_20020228_ethics-internet_en.html> 22 February 2002 (Last visited 25 April 2006).
42. M. Geist *et al.*, *Global Internet Jurisdiction: The ABA/ICC Survey* (April 2004) (On file with author).

4. The Relationship between Contracts and Torts

One can picture situations where a plaintiff has a choice as to whether to bring an action in contract or in tort. Such situations seem to most commonly arise in actions brought in relation to employment contracts, and the normal procedure in many jurisdictions is for the plaintiff to plead his/her claim in the alternative,[43] provided that the jurisdictional ground relied upon allows for claims being made both in torts and contracts. In certain cases, such as where jurisdiction is founded on § 32 of the German Code of Civil Procedure (*Zivilprozeßordnung*), the plaintiff may not raise a claim for breach of contract, but must first obtain jurisdiction under a contract related ground.

As far as the tort of defamation is concerned, however, this issue would rarely arise. Even where a third person to whom publication is made has entered into an contractual agreement with the party accused of defamation, it would be highly unusual for the person alleged to have been defamed to be in any relevant contractual relation with the one making the defamatory publication. Nevertheless, the issue may arise, for example, in a situation where a defamatory remark is made in a discussion forum, and the rules of the forum to which any participant must contractually agree stipulate that defamatory remarks must not be made, and that where such remarks are made they constitute a breach of the contract of participation.

In such a situation, the plaintiff must be allowed to decide whether to bring an action under the contract or in tort. Further, as seems to be common practice, the plaintiff should be allowed to plead his/her claim in the alternative. That said, potential overlap between actions in contract and actions in tort are not dealt with further here.

III. THE JURISDICTIONAL FOCUS

> *Companies from North American [sic] responding to the survey were far more concerned with Internet jurisdiction issues than their counterparts in Europe and Asia. By a ratio of six to one, U.S. companies said that the Internet jurisdiction issues has [sic] become worse over the past two years and four of every five companies say they feel that matters will worsen by 2005. In contrast, responding Asian and European companies think that the risk associated with the issue has improved since 2001 and will improve further by 2005.*[44]

This book covers seven different jurisdictions or law areas, including Australia, England, Germany, Hong Kong SAR, the People's Republic of China, Sweden, and the United States of America. Although these seven law areas are referred to as states and countries, throughout the book, it is acknowledged that Hong Kong is neither a state nor a country.

---

43. *See*, e.g., L Collins *et al.* (eds), *Dicey and Morris on The Conflict of Laws*, (13th edn, London, Sweet & Maxwell, 2000), p. 1315.
44. M. Geist *et al.*, *Global Internet Jurisdiction: The ABA/ICC Survey* (April 2004) (On file with author).

A. AUSTRALIA

Being a federation, Australia has a certain degree of experience of dealing with cross-border issues. Partly, that is what makes Australia interesting for a study such as this. However, even more importantly, on 10 December 2002 the High Court of Australia handed down a judgment regarding jurisdiction and choice of law in an Internet defamation dispute. The judgment, being the first such judgment to be handed down by the highest court of a state, has gained worldwide attention and has been influential as a precedent within the common law world.[45]

Another interesting feature of studying Australia is that, while the law of Australia has its origins in the British common law just like for example the laws of Hong Kong do, Australian law has seemingly deviated much further from its origins than the law of most other traditional common law states.

As the laws and regulations of concern here vary little within Australia, the country-specific chapter dealing with Australia tries only to provide the reader with an overview of the rules of Australia as a nation state. However, references are provided to laws and regulations of all states and territories.

B. ENGLAND

While exceptions can be found, such as the doctrine of *forum non conveniens* being of Scottish origin, English law is the cradle for most of the concepts normally associated with the common law tradition. Interestingly, however, the current English law of relevance here is heavily influenced by European civil law. Indeed, through the *Private International Law (Miscellaneous Provisions) Act 1995* (UK), English law is even codified in aspects of its conflict of laws rules that are not yet codified in all European civil law jurisdictions.

Being a member of the European Union, English law is discussed both in the chapter dealing with the law of traditional common law jurisdictions (Chapter 4), and in the chapter dealing with relevant international instruments (Chapter 8).

C. GERMANY

German law has been very influential, and represents a logical choice when examining the European Civil Law tradition. Of the states considered here, the law of both Sweden and the People's Republic of China (through the influence of Japanese law, greatly influenced by German law) draws heavily upon German legal thinking.

Being a member of the European Union, German law is discussed both in the chapter dealing with the law of European civil law jurisdictions (Chapter 6), and in the chapter dealing with relevant international instruments (Chapter 8).

---

45. *Bangoura v. Washington Post* (27 January 2004), OSCJ 03-CV-247461CM1 (Subsequently changed on appeal); *Don King v. Lennox Lewis, Lion Promotions, L.L.C. and Judd Burstein* [2004] EWHC 168 (QB) *Harrods Ltd v. Dow Jones & Company Inc.* [2003] EWHC 1162 (QB).

Finally, while Germany is a federation, the areas of law relevant in this book are federal and not state law.

D. HONG KONG SAR

Hong Kong SAR represents an interesting mix of East and West. While Hong Kong has been under British rule for approximately 150 years, there is an ever-growing influence from the mainland since 1997 when Hong Kong became a Special Administrative Region (SAR) of the People's Republic of China. This influence is not only noticeable in the everyday life of the people of Hong Kong, but increasingly in the legal sphere.

As far as private international law is concerned, the Hong Kong rules are still very similar to those of the pre-EU England. Consequently, there are similarities between the Australian system and the Hong Kong approach. However, Hong Kong has maintained a very interesting common law tradition (recently abandoned in Australia) – the *double actionability* test. This peculiar choice of law rule is highly interesting in the online context.

E. SWEDEN

Sweden is of interest for several reasons. The first and perhaps most obvious reason is that Sweden is a Member State of the European Union since 1995, and thereby a study of Swedish law necessarily includes a study of European Community law. Due to its EU membership, Sweden has a dual private international law: one set of rules (the traditional Swedish rules) applies in relation to non-EU disputes, while cross-border disputes with parties from other EU Member States are exclusively regulated through EU instruments to the extent that relevant instruments are in place addressing the area of the dispute. This has been dealt with by discussing the European instruments separately in Chapter 8, while Chapter 6 focuses on domestic Swedish law.

Second, it is interesting to place the common law of the US, Hong Kong and Australia in contrast to a European civil law country like Sweden. Further, in relation to defamation, Sweden is interesting as it has a long tradition of free speech. Already in 1766 (i.e. 23 years before the US Constitution was adopted), Sweden introduced its first Freedom of the Press Act. Adding to the interest is also Sweden's peculiarly restrictive approach to foreign judgments, which puts it in contrast to the other states examined. Finally, it is also relevant that Sweden, like the other states studied, is a technologically advanced country with high levels of Internet usage.

F. THE PEOPLE'S REPUBLIC OF CHINA (PRC)

The People's Republic of China has more citizens than any other state in the world. That fact, in combination with the PRC Government's encouragement of Internet

use, make it reasonable to say that the PRC is emerging as a major participant in the use of the Internet. It is also relevant to note that since the late 1970s the PRC has taken huge steps to increase its participation in international arenas. This greater openness has, for example, lead to the recent accession to the World Trade Organization (WTO), the PRC's participation in the negotiations of the *Hague Convention on Choice of Court Agreements* and the fact that Beijing will be hosting the Olympic Games in 2008. Furthermore:

> In the year 2000, [the PRC] concluded some 330 state and governmental bilateral treaties and agreements (or other instruments with full features of treaties) with other countries, more important among which were 222 economic and trade treaties (and exchange of notes), 22 financial treaties, 26 political treaties, 10 consular treaties, 9 legal agreements and agreements covering the fields of culture, health, science and technology, communications and post and telecommunications; China also concluded 6 multilateral treaties with other countries.[46]

The PRC is starting to be noticed by the rest of the world in general and perhaps the western economies in particular. The potential of the PRC as a future market is augmented by the increasing strength of the PRC's economy. Currently the PRC is the fastest growing economy in Asia.[47] Indeed, the rapid development of the Chinese economy is unprecedented in modern history.[48]

Another reason to include the PRC in this study is the fact that there is currently a certain degree of fear about the impact that the PRC's restrictions on freedom of expression might have on the Internet. In that context, it is relevant to examine what steps the PRC has taken to regulate content on the Internet and how aggressive the jurisdictional claims provided for under the PRC's legislation are. Closely connected to this, it is of great interest that the PRC has chosen to use technical means to place borders around the 'Chinese part' of the Internet. Attention must also be given to the fact that the approach taken by the government of the PRC to a certain extent, defies some of the values that have been taken for granted by some theorists.

Since the mid-1980s,[49] serious discussions have been held aimed at a 'Private International Law of the People's Republic of China'. These discussions have led to the development of different draft legislations. Where applicable, reference is made to the provisions of the most recent (the third)[50] draft legislation. In doing so, I hope

---

46. Ministry of Foreign Affairs of the People's Republic of China, 'A General Survey of the Treaties Concluded between China and Other Countries' (2002).
47. C.D. Paglee, 'Contract Law in China: Drafting a Uniform Contract Law' (Chinalaw Web) (On file with author).
48. T. Carlén, *Observatorierapport 36/2001: Rapport om Internets påverkan på demokratin i Kina* (Stockholm, IT-kommissionen: Observatoriet för IT, demokrati och medborgarskap, 2001), p. 13.
49. The first nationwide academic conference on private international law was held in Guiyang, Guizhou Province in 1985.
50. *See* Wilde, *China's International Transactions* (Sydney, LBC Information Services, 2000), p. 223 *et seq.*

to supply an insight to a possible future development in relation to jurisdictional issues in the PRC's legislation. However, there are reasons to believe that any potential 'end-product' of the ongoing discussions on a 'Private International Law of the People's Republic of China' will be adjusted to the development on the international level.[51]

G. The United States of America (US)

Presently, no other state can match the enormous wealth of relevant case law that has evolved in the United States of America.[52] While the absolute majority of those cases relate to domestic disputes, this fact alone justifies the inclusion of the US in a study such as this. It is further important to remember that the Internet originates from a project sponsored by the US government, and that the US still exercises a huge influence over the Internet. It was also deemed necessary to include the US in this study for several other reasons, including the role that the US plays in international trade. Finally, it is interesting to note the apparently different mentality of US companies as compared to their Asian and European counterparts (*see* quote at start of Chapter 1.III). The fact that US companies appear to be more concerned about jurisdictional issues than their Asian and European counterparts is perhaps only natural bearing in mind that jurisdictional issues traditionally have gained much more attention in the US (due to its federal structure and relatively litigious culture), than in Europe and Asia.

The reason why there is such a large number of domestic US cases relating to the issues studied in this book, is found in the fact that the 50 US states are separate jurisdictions and have different laws. It should, however, be remembered that the issue of jurisdiction is regulated in the US Constitution. Thus, it could be said that on the most fundamental level all states share the same jurisdictional rules. In addition, it is common for state laws regulating jurisdiction, to simply adopt the limitations imposed by the Constitution. In light of this, I have chosen to focus on the limitations imposed on jurisdiction by the Constitution. While great similarities can be found also in relation to choice of law, the states' approaches in this regard are more varied than in relation to jurisdiction. As it is not practical for a book involving the study of no less than six other jurisdictions to examine each of the 50 States of America individually, focus is placed on the most dominant choice of law approach. Similarly, a general description is given in relation to the US approach to recognition and enforcement as describing each state's approach individually simply is not an option for a study such as this.

---

51. For example the PRC's participation in the discussion of the Hague Convention on Choice of Court Agreements, discussed further *below*.
52. Spang-Hansen notes that just '[t]he question of jurisdiction in relation to the Internet has been dealt within [sic] several hundred reported cases' in the US. H. Spang-Hanssen, *Cyberspace Jurisdiction in the U.S. – The International Dimension of Due Process* (Oslo, Norwegian Research Center for Computers and Law, 2001), p. 17.

H. The Chosen Mix of States

The most obvious way of looking at the chosen mix of States is perhaps in an East and West perspective. The PRC and Hong Kong are Asian states associated with an eastern culture, while Australia, England, Germany, Sweden and the US are western states associated with a western culture. However, looking further at the chosen states, other divisions become apparent. Australia, England, Hong Kong and the US are all common law states sharing origins in British law while Germany, the People's Republic of China and Sweden are civil law states. Yet another way of viewing the combination of states is from the perspective of 'openness' (i.e. the degree of freedom of expression). Australia, England, Germany, Hong Kong,[53] Sweden, and the US are all relatively 'open' States while the government of the People's Republic of China has, in practice if not theory, chosen a very restrictive approach to the question of freedom of expression. Closely connected to this, the same sort of distinction can be drawn in relation to the openness of the Internet. Australia, England, Germany, Hong Kong, Sweden, and the US have all chosen to structure their participation on the Internet in a very open manner, while the government of the People's Republic of China has chosen to separate the Chinese part of the Internet from the 'international Internet'.

It might also be relevant to observe that Germany, the United States of America and Australia are federations with varying degrees of different laws within their respective states. Also the People's Republic of China consists of several different areas with different laws. England is part of the United Kingdom and Hong Kong is in some regards affected by the law of the PRC. In contrast, Sweden has only one set of laws within its territory.

Finally the chosen mix of states could be divided according to their geographical locations. Taking such an approach we would find that Australia, Hong Kong, and the PRC are located in the Asia-Pacific region, England, Germany and Sweden are European states and the US represents North America. Consequently, no less than four continents are represented in the study.

IV. COMMENTS ON THE TERMINOLOGY

Although readers of this book are presumed to have a certain degree of prior knowledge of law in general and international law and Internet law more specifically, there are reasons to briefly comment on the terminology used. Starting with how the issues of jurisdiction, choice of law and recognition and enforcement are collectively referred to, there are at least three different terminological alternatives: private international law, conflict of laws and jurisdictional issues.

53. However, Hong Kong appears to be becoming increasingly similar to mainland China.

A. Private International Law, Conflict of Laws or Jurisdictional Issues?

The term private international law, or international private law, is commonly used, particularly in countries of the civil law tradition. However, it is not always suitable, and already in the mid-1930s, it was noted that: 'everybody agrees that the term International Private Law is very inadequate'.[54] The issues of jurisdiction, choice of law and recognition and enforcement frequently arise in a domestic context within federal states, such as Australia and the US. It would be wrong to refer to those situations as being determined by private *international* law.[55] In fact, the term private international law has been criticized for being misleading as the issues of jurisdiction, choice of law and recognition and enforcement are determined by national law, and thus have 'nothing to do with international law'.[56] This latter statement could be questioned for several reasons,[57] but highlights the reluctance found amongst, at least some, common law scholars to embrace the term private international law.[58] Furthermore, the term can be criticized for vainly attempting to draw a sharp line between private and public law.[59] It is perhaps illustrative to note that the only part of the term *private international law* which is not subject to dispute is the 'law' part. Despite this, I chose this term for the title of the book.

As this book is focused on international issues, the term is not a bad alternative. However, personally, I think the term 'jurisdictional issues' is preferable and I would have liked to use that term already in the title of the book. However, the potential harm of the title being misunderstood to merely include judicial jurisdiction was deemed to be too great. It can only be hoped that in the future the term 'jurisdictional issues' becomes the norm rather than the exception. So far, however, only few examples can be found of a general acceptance of the term.[60]

---

54. M. Rheinstein, 'Comparative Law and Conflict of Laws in Germany' (1934–1935) 232 *University of Chicago Law Review*, 257.
55. *See also* F. K. Juenger, *The Need for a Comparative Approach to Choice-of-law Problems, International Conflict of Laws for the Third Millennium: Essays in Honour of Friedrich K. Juenger* (New York, Transnational Publishers Inc., 2001), (Originally published: (1999) 73 *Tulane Law Review* 1309–1336, 181.) *See also* L. Collins *et al.* (eds), *Dicey and Morris on The Conflict of Laws* (13th edn, London, Sweet & Maxwell, 2000), p. 32.
56. R. Chisholm, and G. Nettheim, *Understanding law: an introduction to Australia's legal system* (6th edn, Sydney, Butterworths, 2002), p. 24
57. For example, one would have to question how the authors define 'international law'.
58. *See also* A.F. Lowenfeld, 'Editorial Comment: Forum Shopping, Antisuit Injunctions, Negative Declarations, and Related Tools of International Litigation' (1997) 91 *American Journal of International Law*.
59. The difficulties associated with such an exercise are well described in Rostam Josef Neuwirth's Master of Laws thesis (R.J. Neuwirth, *International Law and the Public/Private Law Distinction* (Montreal, MacGill University, 2000). Note too that private international law literature does discuss also public law situations (e.g., P. Nygh and M. Davies, *Conflict of Laws in Australia*, (7th edn, Sydney, Butterworths, 2002), pp. 66–68 discussing actions taken under the Australian *Trade Practices Act* 1974 (Cth.)).
60. One example is: J.R. Paul, 'Comity in International Law' (1991) 32(1) *Harvard International Law Journal*, 6, making the following statement: 'In this Article, I use the term "jurisdiction" to

Common law scholars predominantly refer to the area as 'conflict of laws'. This definition avoids the problem of excluding domestic 'conflicts of laws', but is instead flawed in another perspective. Taking the term literally, it seems that a situation where the applicable law is obvious and undisputed, but the forum selection is in dispute, would not be covered.[61] There is no conflict of laws, but rather a conflict of forums. Such a situation could, for example, arise if a contract includes an undisputed choice of law clause but does not identify the forum. Similarly the term 'jurisdictional issues' seems to be limited to the issue of jurisdiction, and thus excluding a situation where the forum question is settled but the applicable law is in dispute. However, that interpretation of the term 'jurisdictional issues' is very limited, and not the only possibility. The question of applicable law is also referred to as prescriptive, or legislative, jurisdiction, and the question of recognition and enforcement is also referred to as enforcement jurisdiction.[62] Thus, applying that terminology, all the three issues in this book are 'jurisdictional'. In addition, compared to the two other alternatives, this definition – jurisdictional issues – has the advantage of not being associated with one specific legal system (i.e. civil law and common law). Finally, the term 'jurisdictional issues' has the advantage of being able to include also the situations that are not strictly private, such as the jurisdictional scope of administrative law (e.g., Australian *Trade Practices Act 1974* (Cth)). Having concluded that all of these three terms are more or less flawed, they are all used as referring to the same thing (i.e. the issues of jurisdiction, choice of law and recognition and enforcement), throughout the book.

B. IT Law, Cyberspace Law or Internet Law

Turning to the question of how to define the area of law that relates to the recent technological developments, there are at least three different alternatives: information technology law (IT law), cyberspace law and Internet law.

Information technology law (IT law) is, as is obvious from the name itself, referring to the whole area of Information Technology. This area includes such diverse phenomena as the World Wide Web, EFTPOS and copyright for computer programs. On that very ground the name information technology law is deemed too inexact to be used here. One would simply not know what is being referred to.

---

refer collectively to prescriptive, adjudicative, and enforcement jurisdiction', thereby embracing the use of 'prescriptive jurisdiction' (as a reference to choice of law) and 'enforcement jurisdiction' (as a reference to recognition and enforcement of judgments). Another example is B. Fitzgerald *et al.*, *Jurisdiction and the Internet* (Sydney, Lawbook Co., 2004) which discussed jurisdiction, choice of law and recognition and enforcement. The reference to 'jurisdiction', in the tile, would seem to refer to all three forms of jurisdiction.

61. *See further* L. Collins *et al.* (eds), *Dicey and Morris on The Conflict of Laws* (13th edn, London, Sweet & Maxwell, 2000), p. 32.

62. *See*, e.g., J.R. Paul, 'Comity in International Law' (1991) 32(1) *Harvard International Law Journal*, 6.

This book concerns itself with issues related to the Internet and the Internet only. Therefore it would not be correct to use the term IT law.

Both the term Cyberspace law and Internet law are much more specific than IT law. The word 'Cyberspace' comes from the novel *Neuromancer* (1986), written by William Gibson. In that book the concept of Cyberspace includes a direct brain-to-computer link giving the user the illusion of moving around in a data 'matrix'.[63] Although the name Cyberspace law gives this field of law a bit of an exciting and mysterious character, 'Internet law' is preferred for the purpose of this book. The reason is that the Internet is a specific and defined instrument, while it is more likely that technological developments will create new and more advanced 'Cyberspaces'. Put simply, it is my view that the term Internet is more limited in its scope,[64] and might turn out to be more static than Cyberspace, and therefore better suited to describe the Internet of today.[65] Furthermore, Internet law seems to be more commonly used than Cyberspace law.[66] However, it cannot be said that the use of Cyberspace law is incorrect in any way.

C. The Relevant Actors

Further, a few words are necessary in relation to the definitions relating to the 'actors' on the Internet market. There are two types of actors on the Internet; Those who provide material, and those who access material. The former category of actors is referred to as content providers, website operators or similar terms. The latter category of actors is referred to as access seekers, web surfers, etc. Turning to the structure of the Internet, there are normally three tiers: Internet users (such as content providers and web surfers), Internet service providers (hereinafter, ISP) and Internet access providers (hereinafter, IAP). ISPs ordinarily operate in two capacities. They provide the Internet users with access to the Internet, and they 'host' (i.e. provide space for) websites. Australian law separates between these two functions and draws a distinction between Internet Service Providers and Internet Content Hosts.[67] Such a distinction is generally not drawn and is not drawn in this book either. ISPs connect to the Internet through IAPs – the owners of the actual infrastructure.

---

63. T. Hiller, *Sourcebook on Public International Law* (London, Cavendish Publishing Ltd, 1998), p. 256.
64. A view shared by other commentators, such as Darrel Menthe (D.C. Menthe, 'Jurisdiction in Cyberspace: A Theory of International Spaces' (1998) 4 *Michigan Telecommunications and Technology Law Review*, 69).
65. At the same time it must be acknowledged that the Internet has developed considerably since its inception.
66. A search via google.com for the term 'cyberspace law' gave the result of 267,000 pages found, while a search for 'Internet law' gave a result of 5,660,000 pages found. The search was conducted on the 19 April 2006.
67. *Broadcasting Services Amendment (Online Services) Act* 1999 (Cth.).

It is not uncommon for actors of one category to also match the description of another category. For example, ISPs frequently also operate their own website. This way, one and the same company/person can fit into more than one category. However, in such a situation one needs to focus on the relevant activity of the company/person in question. Regulations that apply to an ISP do so only in relation to activities carried out by a company/person operating as an ISP, in its capacity as an ISP. Section 91 of the Australian *Online Services Act*[68] can be used to illustrate this.

Section 91 limits the liability of Internet Content Hosts[69] and Internet Service Providers[70] if they operated without being aware of the nature of the material they hosted/carried. If, for example, the same company that operates as an Internet Content Host also operates a website with a 'guest-book', and defamatory material appears in that section of the website, the company cannot rely on Section 91 to protect them in their capacity as a website operator. This is no different to the fact that an off-duty police officer cannot enjoy the same privileges as he/she does in his/her capacity as a police officer.

D. SERVERS

Finally, so-called 'servers' play a variety of roles in Internet communication. Unless otherwise specified, when this book talks about 'servers', what is referred to are web servers performing the role of storing files related to one or several website(s) and performing all work necessary for hosting the website(s).

68. *Ibid.*
69. Defined as 'a person who hosts Internet content in Australia, or who proposes to host Internet content in Australia' (Section 3).
70. Defined as 'a person that supplies, or proposes to supply, an Internet carriage service to the public' (Section 8).

HEINONLINE

Citation: 54 Fed. Comm. L.J. 339 2001-2002

Content downloaded/printed from
HeinOnline (http://heinonline.org)
Wed Oct 12 09:18:01 2011

-- Your use of this HeinOnline PDF indicates your acceptance
of HeinOnline's Terms and Conditions of the license
agreement available at http://heinonline.org/HOL/License

-- The search text of this PDF is generated from
uncorrected OCR text.

-- To obtain permission to use this article beyond the scope
of your HeinOnline license, please use:

https://www.copyright.com/ccc/basicSearch.do?
&operation=go&searchType=0
&lastSearch=simple&all=on&titleOrStdNo=0163-7606

The Defamation of Choice-of-Law in Cyberspace: Countering the View that the Restatement (Second) of Conflict of Laws is Inadequate to Navigate the Borderless Reaches of the Intangible Frontier

Philip Adam Davis*

I. INTRODUCTION: THE DEFAMATION OF THE RESTATEMENT (SECOND) OF CONFLICT OF LAWS IN CYBERSPACE 340
II. BACKGROUND: THE LAW OF DEFAMATION AND THE RESTATEMENT (SECOND) OF CONFLICT OF LAWS 342
A. *The Law of Defamation* 343
B. *The Restatement (Second) of Conflict of Laws Approach for Defamation* 345
III. DEMYSTIFYING CYBERSPACE 348
IV. COUNTERING THE ARGUMENTS AGAINST TRADITIONAL CHOICE-OF-LAW DOCTRINES IN CYBERSPACE 349

* B.A., Indiana University—Bloomington, 1998. Candidate for J.D., Indiana University School of Law—Bloomington, December, 2001. Proud father of Addison Clark Davis, born October 28, 2000. The Author would like to thank *especially* Gene R. Shreve, Richard S. Melvin Professor of Law at Indiana University School of Law—Bloomington, for his guidance, debate, inspiration, and dedication toward the completion of this Note. In addition, the Author would like to thank Charles Gardner Geyh, Professor of Law at Indiana University School of Law—Bloomington, for his assistance in the completion of this Note. Further, the Author would like to thank fellow law student Jim Sarbinoff for his editorial aid. Finally, the Author would like to thank his wife, Angela Michaela Davis, for putting up with him throughout the note-writing process and law school.

A. *Criticisms Based on a Lack of Boundaries in Cyberspace*... 350
B. *Real-Space Traditional Choice-of-Law Criticisms Disguised*..... 356
C. *Problems with Proposed Alternative Approaches*..... 359
V. CONCLUSION..... 362

So she sat on, with closed eyes, and half believed herself in Wonderland, though she knew she had but to open them again and all would change to dull reality . . . .

—Lewis Carroll[1]

I. INTRODUCTION: THE DEFAMATION OF THE RESTATEMENT (SECOND) OF CONFLICT OF LAWS IN CYBERSPACE

The new information age has caused scholars to consider the adequacy of traditional jurisdictional regimes where interstate disputes arise in cyberspace. Personal jurisdiction has been one of the first of these regimes to undergo criticism and, for the most part, has come out relatively unscathed, despite its opponents' arguments that traditional notions of personal jurisdiction have no place in cyberspace.[2] While the assault on personal jurisdiction in cyberspace has lessened in recent years, in its wake has come yet another attack on conventional jurisdictional notions: a criticism of traditional choice-of-law regimes in cyber-disputes.

Much in the same vein as their assault on personal jurisdiction, many scholars argue that traditional choice-of-law doctrines are inadequate to determine which state law to apply in interstate cyber-disputes.[3] While these critics assert many arguments in support of their view that traditional

1. LEWIS CARROLL, ALICE'S ADVENTURES IN WONDERLAND 171 (The Heritage Reprints 2000) (1865).

2. Despite the continuous assault on usage of the minimum contacts and effects test analysis for determining personal jurisdiction when a dispute arises in cyberspace, courts tend to apply personal jurisdiction in cyberspace disputes the traditional way, rather choosing to better define concepts in cyberspace as opposed to redefining approaches to personal jurisdiction. *See generally* Allan R. Stein, *Symposium on Jurisdiction and the Internet: The Unexceptional Problem of Jurisdiction in Cyberspace*, 32 INT'L LAW. 1167 (1998) [hereinafter *The Unexceptional Problem*].

3. John D. Faucher, *Let the Chips Fall Where They May: Choice of Law in Computer Bulletin Board Defamation Cases*, 26 U.C. DAVIS L. REV. 1045, 1066 (1993) [hereinafter *Let the Chips Fall*].

choice-of-law approaches are inadequate for cyberspace,[4] the overwhelming criticism is that "old choice-of-law doctrines fail to provide any meaningful guidance in the virtual world because these doctrines depend on notions of physical location."[5] Essentially, the argument is that "because there is no 'there' in the virtual world, [traditional choice-of-law] doctrines are virtually useless."[6] In the same breath, many scholars are eager to propose offending alternative regimes to these perceived problems with choice of law in cyberspace,[7] most of which deal with choice of law by ignoring it.[8]

While many opponents criticize traditional choice-of-law regimes in cyber-disputes arising out of contracts, trademark infringement, and other areas of law, much of the criticism focuses on the law of defamation in cyberspace, or "cyber-defamation".[9] The brunt of this scholarly attack on traditional choice-of-law regimes almost certainly falls on cyber-defamation actions. This is because of the unique aspect the law of defamation brings to cyberspace: publishing on the Internet is publishing instantaneously all over the world. Thus, in a multistate cyber-defamation action, a defendant could conceivably collect for damages in any state where the defamatory material was published.[10] As one scholar notes, "[t]he Internet allows anyone connected to it to disseminate information, statements, gossip, and so on, to millions of people with a few strokes on a computer keyboard. Thus millions of people now have their own electronic printing presses—capable of inexpensively communicating with millions of others worldwide."[11] Clearly, the law of defamation represents the perfect lens through which to examine the adequacy of traditional choice-of-law regimes in cyberspace.

---

4. *See infra* Part IV.

5. Christopher P. Beall, *The Scientological Defenestration of Choice-of-Law Doctrines for Publication Torts on the Internet*, 15 J. MARSHALL J. COMPUTER & INFO. L. 361, 362 (1997) [hereinafter *The Scientological Defenestration*].

6. *Id.*

7. *Id.* at 368.

8. *See infra* Part IV.

9. *See The Scientological Defenestration*, *supra* note 5, at 362.

10. "Under the single publication rule, a [defamed] plaintiff can recover for all harm suffered within or without the forum in a single action." R. James George, Jr. & James A. Hemphill, *Defamation Liability and the Internet*, 507 PLI/PAT 691, 706 (1998).

11. R. Timothy Muth, *Old Doctrines on a New Frontier: Defamation and Jurisdiction in Cyberspace*, Sept. 1995, 68 WIS. LAW. 10, 11-12 (Sept. 1995) [hereinafter *Old Doctrines on a New Frontier*].

Despite the various choice-of-law doctrines available,[12] the focus of this Note is almost entirely on the Restatement (Second) of Conflict of Laws ("Restatement (Second)") for two reasons. First, the Restatement (Second) is an eclectic mix of dominant policies and principles taken from traditional choice-of-law doctrines.[13] Second, of those states turning away from the original Restatement of Conflicts of Laws, most are adopting the Restatement (Second).[14]

This Note examines the adequacy of the traditional choice-of-law rules, including the Restatement (Second), in interstate cyber-defamation disputes, and argues that there is nothing different or unique about cyberspace which warrants the modification or abandonment of traditional choice-of-law regimes for cyber-defamation disputes. A distinction must be made, however. This Note does not attempt to argue the adequacy of traditional choice-of-law approaches in and of themselves; the disparaging of traditional choice-of-law doctrines in the real world has been and continues to be a pastime among practitioners and scholars alike.[15] Further, this Note does not argue which choice-of-law approach would be most effective in dealing with cyber-defamation. The only goal of this Note is to demonstrate that traditional choice-of-law rules are not confounded by defamation disputes arising in cyberspace.

II. BACKGROUND: THE LAW OF DEFAMATION AND THE RESTATEMENT (SECOND) OF CONFLICT OF LAWS

Cyberspace is a breeding ground for defamation.[16] Several factors contribute to this. As one commentator suggests, "[T]he low cost of cyberspace communications makes wide-scale distribution of wrongful

12. In addition to the Restatement (Second) doctrines, other traditional choice-of-law doctrines include *lex loci delicti*, *lex fori*, the center of gravity approach, Currie's interest analysis, the Neumeier rules, comparative impairment, and Leflar's choice-influencing considerations. For detailed analysis of each of these approaches, *see generally* GENE R. SHREVE, A CONFLICT-OF-LAWS ANTHOLOGY (1997).

13. The Restatement (Second) "is a treatment that takes full account of the enormous change in dominant judicial thought respecting conflicts problems that has taken place" over the years. RESTATEMENT (SECOND) OF CONFLICT OF LAWS, at vii (1971) [hereinafter RESTATEMENT (SECOND)]. The Restatement (Second) acknowledges that the essence of "change has been the jettisoning of a multiplicity of rigid rules in favor of standards of greater flexibility, according sensitivity in judgment to important values that were formerly ignored." *Id.*

14. Hao-Nhien Q. Vu, *Choose or Lose: Choice-of-Law Issues in Cyberspace Cases Remain Unresolved*, L.A. DAILY J., May 22, 1997, at 7 [hereinafter *Choose or Lose*].

15. For a valuable critique of traditional choice-of-law approaches, *see generally* William L. Reynolds, *Symposium: The Silver Anniversary of the Second Conflicts Restatement: Legal Process and Choice of Law*, 56 MD. L. REV. 1371, 1371 (1997).

16. *Old Doctrines on a New Frontier*, *supra* note 11, at 12.

communications possible."[17] Therefore, "the caution ordinarily exercised in face-to-face real space tends to recede in the world of anonymity and solitude that one finds in front of computer terminals. The temptation to engage in otherwise reckless behavior increases the probability of [cyber-defamation]."[18] Further, messages in cyberspace "transmit few social cues, so people communicating electronically tend to talk more freely than they would in person."[19] Moreover, cyberspace provides numerous forms by which people can engage in cyber-defamation, whether via an e-mail message, a message posted to a newsgroup or bulletin board, or an available file via file transport protocol or database.[20] More than ever before, people are linked to one another across the country by engaging in various forms of communication. The more people communicate with one another, the greater the potential for defamation suits.

Due to the ease with which one can publish defamatory material via cyberspace, the potential for global publication of the material instantaneously[21], and the varying defamation laws among states[22], choice-of-law plays an even more crucial role in interstate defamation actions.

A. *The Law of Defamation*

In general, defamation refers to a "false written [or spoken] statement that exposes a person to public ridicule, hatred, or contempt, or injures [their] reputation."[23] The basic elements of a defamation action commonly include: (1) a statement of fact was published by showing or saying it to a third party; (2) the statement was false at the time it was made; (3) the statement was defamatory; (4) the statement reasonably refers to the plaintiff; (5) the statement was made with the requisite degree of fault; and

17. Matthew R. Burnstein, *Conflicts on the Net: Choice of Law in Transnational Cyberspace*, 29 VAND. J. TRANSNAT'L L. 75, 83 (1996) [hereinafter *Conflicts on the Net*].

18. *Id.*

19. *Let the Chips Fall*, *supra* note 3, at 1047.

20. *Conflicts on the Net*, *supra* note 17, at 83-84.

21. Not all publications of defamatory material in cyberspace are instantaneously published all over the world. In order to recover in a given state for the publication of defamatory material in that state, one must be able to prove that another person, other than the defamer, read the material. Therefore, an e-mail sent from person A in state A to person B in state A defaming person C in state C is only "published" in state A. Of course, person B could always show the defamatory material to another individual, as well as post the message in cyberspace for everyone to read.

22. Kimberly Richards, Comment, *Defamation Via Modern Communication: Can Countries Preserve Their Traditional Policies?*, 3 TRANSNAT'L LAW. 613, 615 (1990) [hereinafter *Defamation Via Modern Communication*].

23. *Let the Chips Fall*, *supra* note 3, at 1052.

(6) the statement caused actual injury.[24]

Despite the common elements of defamation shared among states, many key variations in defamation law exist. For example, state defamation laws may vary on the requisite degree of fault required in defamation cases,[25] the requirement of falsity,[26] distinctions between fact and opinion, the defamatory nature of the statement, the requisite reference to the plaintiff,[27] the availability of defenses and privileges,[28] and special procedural rules.[29] These differences among state defamation laws "reflect deliberate state policy choices, stemming from a balance of free speech values against interests in compensating injured plaintiffs."[30] Such state policy choices are what choice-of-law doctrines, like the Restatement (Second), serve to protect.

---

24. James R. Pielemeier, *Constitutional Limitations on Choice of Law: The Special Case of Multistate Defamation*, 133 U. PA. L. REV. 381, 384 (1985) [hereinafter *Constitutional Limitations on Choice of Law*].

25. *Id.* at 384-85. The requisite degree of fault is considered to be the most significant defamation element differing among states "because it prescribes the basic standard of conduct that publishers must meet." *Id.* at 384. *This requisite degree of fault turns on whether the plaintiff is classified as a public plaintiff or a private plaintiff.* The degree of fault that *public* plaintiffs must prove is the same in every state. New York Times Co. v. Sullivan, 376 U.S. 254, 283-84 (1964). Public plaintiffs may recover damages only by proving that the publisher of the defamatory material had knowledge of the falsity or reckless disregard for the truth. *Id.* at 283. However, the requisite degree of fault varies between states where a *private* plaintiff is defamed because the Supreme Court has delegated power to the states to define their own fault standards in those cases. Gertz v. Robert Welch, Inc., 418 U.S. 323, 347 (1974). The only limitation on a state's power to define its own standards for private plaintiffs is that a state may not impose liability without fault. *Id.* While some states have set the requisite degree of fault at simple negligence, some require actual malice, while others have variations of these standards. *Constitutional Limitations on Choice of Law*, *supra* note 24, at 384-85.

26. *Constitutional Limitations on Choice of Law*, *supra* note 24, at 385. For example, the burden of proving falsity varies from state to state. *Id.* Some states require the plaintiff to prove falsity, others place the burden on the defendant to prove the truth. *Id.*

27. *Id.* "Some jurisdictions have found words capable of a defamatory meaning that others have not." *Id.* One state employs the "innocent construction rule" to determine the defamatory meaning of a statement. Under this rule, a publication is not defamatory if the words may reasonably be given an innocent interpretation. Other states simply leave it to the trier of fact to determine a statement's defamatory meaning. *Id.*

28. *Constitutional Limitations on Choice of Law*, *supra* note 24, at 387. In some states, failure to demand a retraction can limit a plaintiff's damages, while in other states, a retraction demand may have no effect on damages. *Id.* Also, the existence of privilege defenses, such as the privilege of neutral reportage that protects the accurate reporting of defamatory statements on a matter of public interest, vary depending on the state. *Id.*

29. *Id.* at 387-88. Some states favor summary judgment in defamation actions, while others are neutral or disfavor summary judgment. *Id.* Also, depending on the particular state, a plaintiff's ability to force disclosure of the identity of a defamation defendant's sources may be totally precluded or conditioned upon prerequisites. *Id.* at 388. In addition, the statutes of limitation for defamation actions vary by state. *Id.*

30. *Constitutional Limitations on Choice of Law*, *supra* note 24, at 384.

In a defamation action, a plaintiff may sue (i.e., personal jurisdiction is proper) in any state in which the plaintiff can prove that someone received the defamatory message.[31] "However, that forum's law will not necessarily govern the suit. It is that forum's choice of law rules that direct the court to the applicable law."[32] As is evident, choice of law is a critical tool for the sophisticated attorney[33] in interstate defamation actions; it is one tool that could easily determine the ultimate outcome of the case.[34]

B. The Restatement (Second) of Conflict of Laws Approach for Defamation

Whether the case ends up in the federal court system by way of diversity jurisdiction or in the state court system, a judge must always apply the forum state's choice-of-law rules.[35] In addition, in order for a state law to be selected in a constitutionally permissible manner, a state must have a significant contact or contacts creating a state interest such that the choice of its law is neither arbitrary nor fundamentally unfair.[36]

Under the Restatement (Second),[37] the first step is to determine whether the alleged defamatory material was published in one state, or two or more states. Where alleged defamatory material is published in only one state, there is a presumption that the law to be applied is "the . . . law of the state where the publication occurr[ed]."[38] This presumption can only be rebutted by demonstrating that "some other state has a more significant relationship . . . to the occurrence and the parties, in which event the . . . law of the other state will be applied."[39] Thus, all relationships being equal, the law where the defamed party is domiciled controls by default. In multistate defamation actions, where the defamatory statement is contained

---

31. *See* Keeton v. Hustler Magazine, Inc., 465 U.S. 770 (1984) (finding sufficient contacts to support personal jurisdiction where defendant had sold less than one percent of its magazines). "The traditional doctrine in . . . defamation cases provides that such actions may be brought in any jurisdiction where the defamatory remarks were published." *Old Doctrines on a New Frontier*, *supra* note 11, at 56.

32. *Conflicts on the Net*, *supra* note 17, at 88.

33. Regardless of the crucial nature that choice of law potentially plays in any given interstate defamation action, choice of law sometimes remains uncontested in court—often applied *sub silentio*.*See The Scientological Defenestration*, *supra* note 5, at 363.

34. *See Let the Chips Fall*, *supra* note 3, at 1052-53.

35. *Id.* at 1050.

36. Allstate Ins. Co. v. Hague, 449 U.S. 302, 326 (1981).

37. The Restatement (Second) deals with choice-of-law issues both when alleged defamatory material is published in one state only, or when such material is published in two or more states (multistate defamation). *See generally* RESTATEMENT (SECOND), *supra* note 13, §§ 149, 150.

38. *Id.* § 149.

39. *Id.*

"in any one edition of a book or newspaper, or any one broadcast over radio or television, exhibition of a motion picture, or similar aggregate communication[,]"[40] there is a strong presumption that the state with the most significant relationship will be "the state where the person was domiciled at the time, if the matter complained of was published in that state."[41] In multistate defamation actions involving corporations or other legal persons, "the state of most significant relationship will usually be the state where the corporation, or other legal person, had its principal place of business at the time, if the matter complained of was published in that state."[42]

Again, in order to overcome all presumptions stated above, one must demonstrate that another state has a more significant relationship to the dispute.[43] Judges make this determination by applying the choice-of-law principles listed in section 6 of the Restatement (Second).[44] The seven factors relevant to the determination of the applicable law include: (1) the needs of the interstate and international system,[45] (2) the relevant policies of the forum,[46] (3) the relevant policies of the interested states,[47] (4) the

40. The inclusion of the statement "or similar aggregate communication" in the list of communication media in section 150 of the Restatement (Second) demonstrates that the list is not intended to be exhaustive. In fact, such a statement tends to show that the American Law Institute understood that communications technology is a field that is ever-changing and therefore, saw fit to "leave the door open" for the inclusion of other mediums of communication, such as cyberspace. *See* RESTATEMENT (SECOND), *supra* note 13, § 150.

41. *Id.* § 150(2). "The state of a plaintiff's domicile is generally the place where most of his reputational contacts are found; therefore, 'the state of plaintiff's domicile generally has the greatest concern in vindicating plaintiff's good name . . . .'" Wilson v. Slatalla, 970 F. Supp. 405, 414 (E.D. Pa. 1997) (quoting Fitzpatrick v. Milky Way Prods., Inc., 537 F. Supp. 165, 171 (E.D. Pa. 1982)). "Thus, domicile should provide a generally accurate starting point for determining which state's law should apply." Barry J. Waldman, *A Unified Approach to Cyber-Libel: Defamation on the Internet, a Suggested Approach*, 6 RICH. J.L. & TECH. 9, para. 26. (1999) *available at* http://www.richmond.edu/jolt/v6i2/note1.html [hereinafter *A Unified Approach to Cyber-Libel*].

42. RESTATEMENT (SECOND), *supra* note 13, § 150(3).

43. *Id.* § 150 cmt. e. For example, "[a] state, which is not the state of the plaintiff's domicil, may be that of most significant relationship if it is the state where the defamatory communication caused plaintiff the greatest injury to his reputation." *Id.* Such a situation may exist where the plaintiff is known better in a particular state than the state of his domicil, or the defamatory material was related to an activity of the plaintiff that is principally located in a state other than his domicil. *Id.*

44. *Id.* § 6(2).

45. The needs of the interstate system represent the needs of conflicts methods "to make the interstate and international systems work well." *Id.* § 6 cmt. d.

46. Policy factors two and three can be combined to focus upon determining whether each state is interested based on "the purposes, policies, aims and objectives of each of the competing local law rules urged to govern" the controversy. *Id.* § 145 cmt. b. The Restatement (Second) makes no attempt to weigh the relative competing interests. *See id.* The Restatement (Second) simply seeks to identify them as another factor to determine the

protection of justified expectations,[48] (5) the basic policies underlying the particular field of law,[49] (6) certainty and uniformity of result,[50] and (7) ease in determining and applying the law.[51]

The Restatement (Second) also provides a list of relevant contacts to be taken into account when applying the factors listed in section 6, which include: "(a) the place where the injury occurred, (b) the place where the conduct causing the injury occurred, (c) the domicil, residence, nationality, place of incorporation and place of business of the parties, and (d) the place where the relationship, if any, between the parties is centered."[52] As far as the law of defamation is concerned, "[t]he place of the plaintiff's domicil, or on occasion his principal place of business, is the single most important contact for determining the state of the applicable law."[53] These considerations serve to ensure that a court will not apply the law of a state with little interest in the case.[54]

Comments to the Restatement (Second) clearly establish that the section 6 and 150 lists are not meant to be exclusive.[55] "[A] court will on occasion give consideration to other factors in deciding a question of

---

appropriate choice of law. Moreover, this recognition of the interest that a state may have in the outcome of a given controversy mirrors the recurrent choice-of-law values of justice, fairness, and the most socially acceptable result.

47. *See supra* note 46.

48. Factors four and six can be combined to focus upon "[the parties'] justified expectations and certainty and predictability of result." *See* RESTATEMENT (SECOND), *supra* note 13, § 145 cmt. b. These considerations deal with the proposition that "it would be unfair and improper to hold a person liable under the local law of one state when he had justifiably molded his conduct to conform to the requirements of another state." *Id.* § 6 cmt. g. This factor is also "of particular great importance in areas where the parties are likely to give advance thought to the legal consequences of their transactions." *Id.* § 6 cmt. i. Although predictability and party expectations may not seem to be of significant relevance in the area of tort law (i.e., interstate automobile accidents), such values are of much greater importance in the area of defamation law. *See id.* § 145 cmt. b.

49. This factor recognizes "situations where the policies of the interested states are largely the same but where there are nevertheless minor differences between their relevant local law rules." *Id.* § 6 cmt. h. The Restatement (Second) urges that in such situations, courts should endeavor to apply the law of the state that will best achieve those policy objectives underlying the particular field of law involved. *Id.*

50. *See supra* note 48.

51. Ease in the determination and application of the law to be applied simply recognizes that "[i]deally, choice-of-law rules should be simple and easy to apply." *See* RESTATEMENT (SECOND), *supra* note 13, § 6 cmt. j.

52. *Id.* § 145(2). When determining which law is to be applied, the basic assumption that underlies the importance of contacts is that "[t]hose states which are most likely to be interested are those which have [§ 145] contacts with the occurrence and the parties." *Id.* § 145 cmt. e.

53. *Id.* § 145 cmt. e.

54. *Defamation Via Modern Communication*, *supra* note 22, at 654.

55. RESTATEMENT (SECOND), *supra* note 13, § 6 cmt. c.

choice of law."[56] Further, the factors listed in both lists are not arranged in any order of relative importance.[57] "Varying weight will be given to a particular factor, or to a group of factors, in different areas of choice of law."[58]

In sum, the approach in the Restatement (Second) seeks to preserve state policies by requiring courts to apply the law of the state with the most significant relationship with the dispute.

III. DEMYSTIFYING CYBERSPACE

As is the case with most breakthroughs in technology, people are eager to denigrate the efficiency of traditional legal rules, including choice of law.[59] Early in the 1990s, as the Internet spread throughout the world like a forest fire, people became enamored with it. Poetic sentimentalities in the face of a brave new era gave rise to phrases such as "surfing the Web," "visiting a Web site," "netizens," "entering chat rooms," and the "virtual world." Indeed, the term "cyberspace" itself denotes some other "place" outside of traditional space and time; a place where anything and everything is possible at the touch of a button. In short, cyberspace established itself in the American psyche as a world of its own.[60]

In line with this clichéd ideology, some people assert themselves as "residents of Cyberspace, [resistant] to law emanating from outside of Cyberspace."[61] One "netizen" of cyberspace went so far as to declare a "Declaration of Independence of Cyberspace," which states, "Governments of the Industrial World, you weary giants of flesh and steel, I come from Cyberspace, the new home of Mind. On behalf of the future, I ask you of the past to leave us alone. You are not welcome among us. You have no sovereignty where we gather."[62] This self-styled "declaration" epitomizes netizen dogma.

Cyberspace is no longer a "new frontier," but a fixed communication device that is commonplace and woven into the fabric of American society.

---

56. *Id.*

57. *Id.*

58. *Id.* For example, the Restatement (Second) recognizes that "[s]ituations do arise . . . where the place of injury will not play an important role in the selection of the state of the applicable law . . . . such as in the case of multistate defamation [where] injury has occurred in two or more states." *Id.* § 145 cmt. e (internal citations omitted).

59. *The Scientological Defenestration*, *supra* note 5, at 362.

60. For a similar position, see *The Unexceptional Problem*, *supra* note 2, at 1172 (arguing that "[c]yberspace evokes a sense that the real activity is not occurring in physical space, but in some ethereal fifth dimension.").

61. Aron Mefford, *Lex Informatica: Foundations of Law on the Internet*, 5 IND. J. GLOBAL LEGAL STUD. 211, 218 (1997) [hereinafter *Lex Informatica*].

62. *Id.* This "Declaration of the Independence of Cyberspace," was written by John Perry Barlow and transmitted via the Internet on February 8, 1996. *Id.*

The fixation with cyberspace as another world is rapidly losing its poetic luster and becoming just another exhausted metaphor used for the amusement of the sci-fi generation. As one commentator eloquently stated, "As we master and understand [cyberspace], we demystify it."[63]

Cyberspace, contrary to netizen dogma, is not a "world." Cyberspace is another source of information, not a new state of being. A person does not sleep, eat, or play "there" anymore than they sleep, eat, or play in the pages of *Time* magazine. A person's reputation, whether defamed by a hard copy of *USA Today* or by the *USA Today* Web site, is still injured in the real world. It is conceivable, even though most likely unachievable, that—in the far distant future—humans might conceive of a way to physically place their bodies in the cyber-ether, thus truly becoming "netizens." In such a world, cyberspace could conceivably be their sovereign. Until that dream comes to fruition, however, the term "netizen" denotes no more than a person in real-space, under the law of real sovereign states, gazing into the dull reality of a real-space computer screen (most likely playing FreeCell or shopping on Ebay).

IV. COUNTERING THE ARGUMENTS AGAINST TRADITIONAL CHOICE-OF-LAW DOCTRINES IN CYBERSPACE

Thus far, criticisms of the traditional choice-of-law regimes for cyber-defamation can be classified into two groups, which may occasionally overlap. Within the first group rests those arguments based on a perceived premise that something is uniquely different about cyberspace.[64] Within the second group rests cloaked arguments that are asserted as "because of the uniqueness of Cyberspace," but ultimately are deep-rooted arguments routinely used to disparage traditional choice-of-law regimes, as well as other areas of law, in "real" space.[65]

These proposals for changing choice-of-law principles for cyber-defamation rely on the perceived notion that defamation in cyberspace is somehow different and, therefore, cyber-defamation needs different choice-of-law rules.[66] This perception is false. By demystifying cyberspace, it becomes all too clear that there is nothing about cyber-defamation that in any way challenges the adequacy of traditional choice-of-law regimes, including the Restatement (Second).[67]

---

63. *The Unexceptional Problem*, *supra* note 2, at 1174 (in support of the traditional application of personal jurisdiction for cyber-disputes).

64. *See infra* Part IV.A.

65. *See infra* Part IV.B.

66. *The Scientological Defenestration*, *supra* note 5, at 363.

67. *The Unexceptional Problem*, *supra* note 2, at 1167.

A. *Criticisms Based on a Lack of Boundaries in Cyberspace*

The most cited argument by far for why traditional choice-of-law rules are inadequate for cyber-defamation actions is the "boundless medium" argument.[68] "[M]ost traditional [choice-of-law] rules are based on the locations where activities take place[,]" including the Restatement (Second).[69] The argument is that these choice-of-law rules are inadequate for cyber-defamation actions because cyberspace is boundless; it defies national boundaries, and therefore, undermines the viability and validity of laws based on geographic borders.[70] These critics argue that cyberspace activities differ from real-space activities in that "they are free from any concept of locality or distance."[71]

Critics argue that "like most post-Restatement authorities . . . the Restatement (Second) offers courts little substantive guidance concerning choice-of-law decisions."[72] Regarding the Restatement (Second), critics argue that the geographical principles listed in section 145(2)[73] are confounded by cyberspace.[74] Critics wonder how these relevant contacts and principles are to be considered in cyberspace.[75] For example, how is "place of injury, place of conduct causing injury, principle place of business, and nationality" determined in cyberspace?[76] Some dismiss a user's ambivalence to political border crossing in exchange for the claim that "[f]requently, users are unaware that they have even 'crossed' a political border in the course of their virtual travels."[77] Some critics use "boundless medium" arguments to support the proposition that the choice-of-law principles in section 6 of the Restatement (Second) are vague and offer little direction because of cyberspace.[78]

---

68. *See infra* notes 69-78. *See also* SYMEON C. SYMEONIDES ET AL., CONFLICT OF LAWS: AMERICAN, COMPARATIVE, AND INTERNATIONAL 894 (1998); *Conflicts on the Net*, *supra* note 17, at 78; Heather McGregor, *Law on a Boundless Frontier: The Internet and International Law*, 88 KY. L.J. 967, 969 (2000) [hereinafter *The Internet and International Law*].

69. *Choose or Lose*, *supra* note 14, at 7.

70. *The Internet and International Law*, *supra* note 68, at 969 (citation omitted); *see also Lex Informatica*, *supra* note 61, at 236.

71. *Choose or Lose*, *supra* note 14, at 7.

72. *Let the Chips Fall*, *supra* note 3, at 1063.

73. *See supra* Part II.B.

74. *Conflicts on the Net*, *supra* note 17, at 94. *See Choose or Lose*, *supra* note 14, at 7.

75. *Conflicts on the Net*, *supra* note 17, at 94.

76. *Id.*; *see also* Craig Peyton Gaumer, *Conflicts, the Constitution, and the Internet*, 86 ILL. B.J. 502, 506 (1998) [hereinafter *Conflicts, the Constitution, and the Internet*] (asserting that in cyberspace, "[t]he only way to determine the principal 'place' of its business may be to review its records and ascertain in which state most of its customers are located.").

77. *Conflicts on the Net*, *supra* note 17, at 82.

78. *Let the Chips Fall*, *supra* note 3, at 1064.

Critics fail to support their proposition that the boundless medium of cyberspace makes traditional choice-of-law doctrines inapposite. The way in which most arguments against traditional choice-of-law approaches are laid out is that an author creates a hypothetical cyber-defamation dispute, and then applies a choice-of-law doctrine. Ultimately, without ever explaining why cyberspace is somehow different or unique in their analysis, they conclude by holding that traditional choice-of-law regimes are inadequate or useless in cyberspace. Consider the following variation by John D. Faucher used to demonstrate the inadequacy of the Restatement (Second) for dealing with cyber-defamation disputes:[79]

> A offers hundreds of bulletin boards from a mainframe computer in State A. A contracts with B, a movie critic from State B, to disseminate B's weekly movie review column. A publishes B's reviews over its Movie Line bulletin board. The Movie Line bulletin board has readers in all fifty states. In a review of a certain movie, B makes a false assertion. Specifically, B writes that C, the movie's star and a resident of the state of C, belongs to the Ku Klux Klan. After reading the review, African-American, Jewish, and Catholic computer users boycott the movie and its studio, Studio C. Studio C also resides in State C. C and Studio C sue B and A in federal court in the Western District of State C. They allege defamatory publication in State C, and seek compensatory and punitive damages. Defamation laws in State A, B, and C vastly differ.

In Faucher's Restatement (Second) analysis to this cyber-hypothetical, Faucher skips entirely the initial presumption that, unless another state has a more significant relationship to the dispute, the law of State C is to be applied in the dispute because the defamatory material was published in State C and the Plaintiffs' domicile and principal place of business are in State C. Instead, Faucher sets out to determine which state has the most significant relationship with the dispute, and asserts that it could just as easily be any one of the hypothetical states. Without difficulty, Faucher first breezes through the section 145 "physical" contacts list of the Restatement (Second), easily identifying that injury to reputation occurred in State C, conduct causing the injury took place in State B (the place from where the review was sent) and in State A (from where the review was disseminated), Plaintiffs are domiciled in State C, and Defendants are domiciled in States A and B. Based on the face of these contacts, Faucher argues that it is not immediately apparent which state has the "most significant contacts." Therefore, Faucher turns to the seven choice-of-law principles listed in section 6 of the Restatement (Second) in order to aid in the determination of which state has the most significant

79. *Id.* at 1054-56 (hypothetical not verbatim).

relationship to the dispute. Without going through any section 6 analysis, however, Faucher states that "[t]hese criteria are vague and offer little direction."[80] As a result of his cyber-hypothetical, Faucher summarizes by stating that "[b]ecause [the Restatement (Second)] process is long, difficult, and murky, the Restatement (Second) offers little help in [cyber-defamation] cases."[81]

As is typical in most critics' analyses, Faucher's analysis of the Restatement (Second) as applied to his cyber-hypothetical identifies nothing unique about the medium of cyberspace that makes the Restatement (Second) any more "long, difficult, and murky" to apply when compared to defamation in real-space. Faucher simply runs through the Restatement (Second) analysis, and then at the end suggests that because it is cyberspace, it is somehow different, and therefore traditional choice-of-law regimes are inadequate for cyber-defamation disputes.

In the end, Faucher fails to address the crucial questions. How is Faucher's analysis applied any differently in real-space? What does cyberspace uniquely offer that makes section 6 principles "vague and of little direction" when compared to the application of section 6 principles in the real world? These questions, and more, are left unanswered by the critics because cyberspace poses nothing unique to traditional choice-of-law regimes in the real world. Consider the following variation on Faucher's cyber-hypothetical involving a defamation dispute in real-space:

> A is the publisher of *America Today*, a nationally read newspaper located in State A. A contracts with B, a movie critic from State B, to disseminate B's weekly movie review column. A publishes B's reviews in the entertainment section of *America Today*, which has readers in all fifty states. In a review of a certain movie, B makes a false assertion. Specifically, B writes that C, the movie's star and a resident of State C, belongs to the Ku Klux Klan. After reading the review, African-American, Jewish, and Catholic *America Today* readers boycott the movie and its studio, Studio C. Studio C also resides in State C. C and Studio C sue B and A in federal court in State C. They allege defamatory publication in State C, and seek compensatory and punitive damages. Defamation laws in State A, B, and C vastly differ.[82]

The only thing different from Faucher's cyber-hypothetical and this real-space hypothetical is that in Faucher's cyber-hypothetical the defamatory material was published in cyberspace on a computer bulletin

80. *Id.* at 1064.

81. *Id.*

82. This hypothetical is based on the Faucher hypothetical. *Let the Chips Fall*, *supra* note 3, at 1054-56.

board available nationwide, whereas in this real-space hypothetical the defamatory material is published in real-space in a newspaper available nationwide. According to Faucher and other critics, traditional choice-of-law approaches, like the Restatement (Second), are inadequate choice-of-law approaches for cyber-defamation disputes; for choice-of-law purposes, however, there is absolutely no difference between Faucher's cyber-hypothetical and this real-space hypothetical.

An application of the Restatement (Second) to this hypothetical will present identical results as Faucher's cyber-hypothetical. Although Faucher did not provide the initial Restatement (Second) presumption in his cyber-hypothetical analysis, this critical presumption, if performed, remains the same in real-space. Specifically, unless another state has a more significant relationship to the dispute, the law of State C is to be applied in the dispute because the defamatory material was published in State C and Plaintiffs' domicile and principal place of business are in State C. Again, whether the defamatory review is published nationwide in cyberspace or real-space, the presumption in both hypotheticals remains unsurprisingly identical. Further, section 145 contacts equally remain identical and just as easily identifiable. Injury to reputation still occurs in State C. Conduct causing the injury still takes place in State B (the place from where the review was sent) and in State A (the place from where the review was disseminated). Plaintiffs are still domiciled in State C, and Defendants are still domiciled in States A and B. Incidentally, critics argue that section 145 contacts are confounded by boundless cyberspace,[83] yet Faucher, in his hypothetical used to prove inadequate traditional choice-of-law regimes for cyberspace, has no difficulty identifying these real-world physical contacts. Just as section 145 contacts remain identical in the real-space hypothetical, so too do such contacts remain just as easily identifiable.

Without going through any Restatement (Second) section 6 analysis, Faucher argues that section 6 principles are "vague and offer little direction" when applied in the context of his cyber-hypothetical.[84] Nevertheless, critics of the Restatement (Second) have always asserted that section 6 principles are somewhat difficult to apply, whether in real-space or cyberspace.[85] Policy analysis is a difficult business; that is why lawyering is a profession. Regardless, however "difficult, vague, or of little direction" these section 6 principles are in real-space, and are no more

83. *Conflicts on the Net*, *supra* note 17, at 94; *see also Choose or Lose*, *supra* note 14, at 7.

84. *Let the Chips Fall*, *supra* note 3, at 1064.

85. For a critical evaluation of traditional choice-of-law approaches, *see generally* Reynolds, *supra* note 15.

"difficult, vague, or of little direction" in cyberspace.

In order to answer whether cyberspace offers something unique to choice-of-law doctrines for defamation, making section 6 principles "vague and of little direction" as Faucher suggests, it is imperative to analyze section 6 principles in cyberspace versus section 6 principles in real-space. The following focuses on a few relevant principles listed in section 6 of the Restatement (Second) in order to demonstrate that these principles are in no way confounded by cyberspace.

Principles (2) and (3) of section 6 combine to determine the interests of each state by gauging "the purposes, policies, aims and objectives of each of the competing local law rules urged to govern" the controversy.[86] The Restatement (Second) makes no attempt to weigh the relative competing interests.[87] It simply seeks to identify these interests as another factor to determine the appropriate choice of law. At a bare minimum, State C has a legitimate interest in protecting its citizens from fraudulent misrepresentation, but States A and B also have an interest in discouraging fraudulent conduct by persons operating from within its territory.[88] These competing interests are neither confounded nor altered by cyberspace. State C's interest in protecting the reputation of its citizens is not changed simply because someone decides to defame State C's citizen in cyberspace instead of real-space. Likewise, State A and B's interest in discouraging fraudulent conduct by persons operating from within their borders is just as real, regardless of what medium those individuals use to effectuate such slanderous conduct.

Principles (4) and (6) of section 6 can be combined to determine the parties' "justified expectations and certainty and predictability of result."[89] These considerations deal with the proposition that "it would be unfair and improper to hold a person liable under the local law of one state when he had justifiably molded his conduct to conform to the requirements of another state."[90] Specifically, these factors are "of great importance in areas where the parties are likely to give advance thought to the legal consequences of their transactions," such as in the area of contract law.[91] Predictability and party expectations are not significantly relevant in the area of tort law because persons that cause injury usually act without giving

86. *See* RESTATEMENT (SECOND), *supra* note 13, § 145 cmt. b.

87. *Id.*

88. *See* Henry H. Perritt, Jr., *Jurisdiction in Cyberspace*, 41 VILL. L. REV. 1, 5-6 (1996) [hereinafter *Jurisdiction in Cyberspace*] (identifying common interests held by states in interstate defamation actions).

89. RESTATEMENT (SECOND), *supra* note 13, § 145 cmt. b.

90. *Id.* § 6 cmt. g.

91. *Id.*

much thought (i.e., expectation) to the legal consequences of their actions.[92] Such principles may be of greater importance in the tort law area of defamation, however.

In addition, some commentators argue that the Restatement (Second) approach to cyber-defamation disputes, in its "case-by-case search for fairness . . . sacrifices certainty and simplicity."[93] Regardless of its cyber-premise, this argument is merely a traditional real-space criticism of the Restatement (Second). Whether the Restatement (Second) does "sacrifice certainty and simplicity," such a sacrifice is no greater because of cyberspace.

For example, newspapers, conscious of the legal consequences of their actions, will often structure their behavior around the availability of defenses and privileges to potential actions brought against them for defamation.[94] As sensitive as a newspaper may be to the potential of publishing defamatory material in an article, they also know the potential consequence when they do. That consequence is the inevitability that the state law of where the defamed party is domiciled will most likely govern the dispute.[95] Therefore, a newspaper publisher in no way can argue that it did not have any expectation that the law of the defamed party's domicile could apply. Whether defamatory material is published on the newspaper's Web site makes no difference to the newspaper's expectation. The defamed party's reputation is still injured in real-space, and real-space rules apply. Conversely, in those situations where someone publishes defamatory material without thought of the legal ramifications of his or her conduct, then justified expectations will play an insignificant role in the choice-of-law decision.[96] An individual's reputation is injured regardless of whether someone carelessly defames that person in cyberspace, as opposed to real-space. Clearly, cyberspace offers nothing unique to these principles of expectation and predictability embodied in the Restatement (Second).

Finally, principle (7) recognizes that "[i]deally, choice-of-law rules should be simple and easy to apply."[97] cyberspace does not make ascertaining the applicable law by traditional choice-of-law rules any more difficult. As discussed previously in both hypotheticals presented, the initial presumption of the Restatement (Second) remained exactly the same. Further, the identification of contacts listed in section 145 remained exactly

92. *Id.* § 145 cmt. b.
93. *Conflicts on the Net*, *supra* note 17, at 94.
94. *Constitutional Limitations on Choice of Law*, *supra* note 24, at 387.
95. *See* RESTATEMENT (SECOND), *supra* note 13, § 150(2).
96. *Id.* § 145 cmt. b.
97. *Id.* § 6 cmt. j.

the same.[98] Also, the analysis of section 6 principles was not confounded by cyberspace.[99] However difficult critics may think the Restatement (Second) is to apply to defamation disputes in real-space, this perceived difficulty is in no way more or less difficult to apply in cyber-defamation disputes.

Indeed, much criticism of choice of law in cyber-defamation disputes has been geared toward the Restatement (Second).[100] Despite criticisms, cyberspace is not conducive to the paradigm that sovereignty is traditionally a function of territoriality.[101] Cyberspace in no way challenges the world to reconcile geographical real-space with a nongeographical cyberspace. And why should it? Albeit extremely exciting, cyberspace is simply another medium for the communication of information. Regardless of whether someone defames a party over a broadcast, by fax, in print, or in cyberspace, the defamed party's reputation is still injured in a sovereign state where that state has a real-space interest in protecting its citizens' reputation from injury.

B. Real-Space Traditional Choice-of-Law Criticisms Disguised

The following represents those cloaked arguments that are asserted as "because of the uniqueness of cyberspace," but ultimately, are well-established arguments traditionally used to criticize traditional choice-of-law regimes, as well as other areas of law in real-space. While critics serve these arguments up as novel because of cyberspace, all of the following arguments exist not because of cyberspace, but because of a much broader dissatisfaction with traditional choice-of-law regimes as a whole. Regardless of the dissatisfaction that some may feel toward traditional choice-of-law approaches, that dissatisfaction is in no way amplified because of cyberspace.

One argument is that "[t]he physical acts of copying and distributing take time, during which [an individual] can obtain an injunction before suffering extensive damage."[102] However, in cyberspace the defamatory material can be distributed nationwide at a keystroke.[103] Thus, "[b]y the time the court hears the case, the damage has been done or the advantage has been exploited."[104] Although asserted to support the idea that traditional choice-of-law doctrines are inadequate for cyber-defamation disputes, the fact that humankind has created a medium of communication capable of speeding up the publishing process in no way is related to choice-of-law

98. *Id.*
99. *Id.*
100. *Conflicts on the Net*, *supra* note 17, at 94.
101. *Id.* at 82.
102. *Lex Informatica*, *supra* note 61, at 220.
103. *Id.*
104. *Id.*

doctrine. Whether or not this argument presents a problem should be dealt with by the defamation law of states. Choice-of-law rules cut across various areas of state law (i.e., torts and contracts) without modifying them.

A similar argument presented to support the inadequacy of traditional choice-of-law rules for cyber-defamation is that under the single publication rule, a defamed plaintiff can recover for all harm to his or her reputation in or outside the forum state.[105] Thus, in any given cyber-defamation action, it is conceivable that such harm to reputation could occur nationwide.[106] Nationwide defamation actions are just as common in real-space, however, through nationwide newspaper circulations, as they may be in cyberspace. Again, the problem is not with choice-of-law doctrine. Whether or not the single publication rule should be re-examined as it relates to cyberspace may be a question for state legislatures to address in their defamation law. As for choice of law in cyberspace, the single publication rule offers nothing different than what it offers in real-space.

Another argument used to support the notion that choice of law is confounded by cyberspace stems from the fact that defamation law draws a distinction between "private persons who may be unavailable to access the media to respond to the defamation and public persons who have greater access to mass media."[107] The argument is that current law does not account for the fact that private individuals may now respond to defamatory statements via cyberspace by posting a message to any number of Internet newsgroups.[108] "In effect, the defamed person can very quickly and easily become the mass media himself by using the Internet."[109] Nevertheless, whether cyberspace provides private individuals with an opportunity to respond to defamatory statements they previously did not have bares no relation to choice-of-law doctrine. A state legislature or court may or may not wish to re-examine and/or possibly alter the requisite degree of fault that private plaintiffs must prove in cyber-defamation disputes. However, choice of law in cyber-defamation disputes is not affected by or concerned with this new opportunity afforded by cyberspace for private individuals to respond to defamatory statements.

Lastly, some critics argue that cyber-defamation is confounded by traditional choice-of-law approaches because the opportunity for forum shopping in cyber-disputes is intensified.[110] For example, in a defamation action, a plaintiff may bring suit in any state in which the plaintiff can

105. *Defamation Liability and the Internet*, *supra* note 10, at 706.
106. *Id.*
107. *Lex Informatica*, *supra* note 61, at 219.
108. *Id.*
109. *Id.*
110. *Defamation Via Modern Communication*, *supra* note 22, at 614-15.

prove that someone received the defamatory message.[111] Thus, in any given multistate cyber-defamation action, a plaintiff may conceivably forum shop around fifty states for the most beneficial choice-of-law rules.[112] A plaintiff could initiate an action in a state with an insignificant interest in the dispute only to take advantage of that state's choice-of-law rules, thus controlling to a degree what substantive law governs the dispute.[113] Critics argue that "[t]his type of 'forum shopping' may not only adversely affect the defendant; it may also undermine the policies and laws of [states] which have substantially greater interest in the cause of action."[114]

It is somewhat ironic that states, in order to deal with the laws differing among them, created choice-of-law rules that *themselves* differ among states. Indeed, forum shopping is a problem. This Author is of the opinion that states should come to a consensus on one choice-of-law rule to not only decrease the opportunity for forum shopping that undermines the interests and polices of a given state, but also accord even greater comity among states. Regardless, forum shopping is no greater because of cyberspace. A nationwide cyber-defamation action poses no greater opportunity for forum shopping than a nationwide real-space defamation action. If *USA Today* contains defamatory material about an individual and it is read in all fifty states, the defamed party may forum shop in all fifty states for a beneficial choice-of-law approach. Likewise, if *USA Today* decides to publish the defamatory material on its Web site as opposed to its hard copy newspaper, and that material is read in all fifty states, the defamed party may still forum shop in all fifty states.

The only unique aspect of cyberspace is the heightened potential for a defamatory statement to have an effect nationwide. Once a defamatory cyber-statement does have an effect on a national level, however, that statement is no different than a real-space statement published in a nationally recognized magazine. Again, the problem of forum shopping exists with equal force in cyberspace and in real-space. Although now asserted as existing because of cyberspace, the forum shopping argument is nothing more than a classic criticism of the fact that traditional choice-of-law regimes differ among states. This argument is not novel because of cyberspace, but has always been a criticism grounded in real-space. This

111. *See* Keeton v. Hustler Magazine, 465 U.S. 770 (1984) (finding sufficient contacts to support personal jurisdiction where defendant sold less than one percent of its magazines). "The traditional doctrine in . . . defamation cases provides that such actions may be brought in any jurisdiction where the defamatory remarks were published." *Old Doctrines on a New Frontier*, *supra* note 11, at 56.

112. *Defamation Via Modern Communication*, *supra* note 22, at 614-15.

113. *Id.*

114. *Id.* at 616.

heightened potential for cyber-statements to gain national attention may call for states to rethink the potential severity of their defamation laws. Alternatively, this heightened potential may call for states to utilize the same choice-of-law approach for defamation. However, there is no reason to make new or modified choice-of-law rules for cyber-defamation disputes because, for choice-of-law purposes, such disputes in no way differ from real-space disputes.

C. *Problems with Proposed Alternative Approaches*

In response to the perceived inadequacy of traditional choice-of-law regimes for cyber-defamation disputes, scholars propose various alternatives in the law. Among these numerous alternatives, the main proposals are: (1) creating a federal common law for the Internet that would effectively eliminate the choice-of-law process,[115] and (2) simply making cyberspace a sovereign of its own.[116] No courts apply these novel regimes.[117]

In the rush to be the first to establish new choice-of-law regimes for cyberspace, some scholars seem to have forgotten the reason behind choice-of-law regimes: to respect state sovereignty. Despite the overarching argument that cyberspace offers nothing novel for traditional choice-of-law regimes in cyber-defamations, an analysis of these cyberspace approaches will also reveal that they offer little as alternatives to traditional choice-of-law approaches.

Faucher argues that to bring order and predictability to cyber-defamation cases, judges should create a federal common law to govern cyber-defamation.[118] According to Faucher: "Such an approach would allow judges to fashion a defamation law that is relevant to electronic communication" as well as "avoid the conceptual difficulties of applying choice-of-law rules to torts that have little relation to a single geographical area."[119] Faucher states: "If the law is uniform across all states . . . choice-of-law problems disappear."[120] Faucher's federal common law approach changes the law of cyber-defamation itself, as opposed to modifying traditional choice-of-law regimes for cyberspace.[121] Assuming, *arguendo,* that the creation of a federal common law does not violate the *Erie* and

115. *See Let the Chips Fall, supra* note 3, at 1051.

116. *The Internet and International Law, supra* note 68, at 982; *see also Conflicts on the Net, supra* note 17, at 108-10; *A Unified Approach to Cyber-Libel, supra* note 41, para. 20.

117. *The Scientological Defenestration, supra* note 5, at 368.

118. *Let the Chips Fall, supra* note 3, at 1067.

119. *Id.* at 1051 (internal footnote omitted).

120. *Id.* at 1068.

121. *See The Scientological Defenestration, supra* note 5, at 371-73.

Klaxon doctrines as Faucher suggests,[122] a federal common law for cyber-defamation would fundamentally violate the principles and policies of state sovereignty.

Faucher's solution to the perceived problem of choice of law in cyberspace is, essentially, to bypass the choice-of-law question entirely. Faucher argues that "the federal law would advance the forum's interest best because, under a federal common law, the forum is the United States rather than an individual state."[123] This argument is circular and loses sight of one crucial factor; the federal forum's minimal interest exists at the expense of a state's interest in a cyber-defamation action involving its citizens. The entire point of choice-of-law rules is ultimately to respect state sovereignty. A common law federal approach does not respect the sovereignty of any state's law. In fact, it would rob states of such sovereignty. Where choice-of-law rules exist to respect state sovereignty, a federal common law would exist to deny it. Faucher argues for an easy way out of perceived tough choice-of-law issues at the expense of everything choice of law exists to protect. Thus, Faucher's approach offends state sovereignty.

---

122. According to *Erie*, federal courts in diversity must apply substantive state law rather than federal common law; in fact, *Erie* held that federal common law does not exist. Erie R.R. Co. v. Tompkins, 304 U.S. 64 (1938). Despite *Erie*, Faucher relies on Georgene Vairo's assertion when stating that "federal courts have the authority to create federal law . . . when . . . the case involves a uniquely federal interest." *Let the Chips Fall, supra* note 3, at 1073 (citing Georgene M. Vairo, *Multi-Tort Cases: Cause for More Darkness on the Subject, or a New Role for Federal Common Law?*, 54 FORDHAM L. REV. 167, 203 (1985)). Faucher argues that cyberspace has enough of a unique federal interest to allow courts to create a common law by likening cyberspace to the federal government's regulation of interstate telephone service and aspects of some computer crimes. *See id.* at 1074. As one commentator notes, however: "This federal interest involves the technical capacity and security of the system. The federal interest does not involve the content of messages transmitted over the infrastructure." *The Scientological Defenestration, supra* note 5, at 371. Still, whether the federal government has such an interest, or whether such an interest may or may not be enough to justify the creation of federal common law for defamation, is outside the scope of this Note because whether such a power exists is irrelevant in determining whether traditional choice-of-law regimes are adequate for cyber-disputes.

Another roadblock that Faucher identifies in his quest for a federal common law is the *Klaxon* doctrine. In *Klaxon Co. v. Stentor Elec. Mfg. Co.*, the Supreme Court found that a federal court sitting in diversity must apply the state's choice-of-law rule and substantive law by finding that the *Erie* doctrine extended to both the choice-of-law rules and substantive law. 313 U.S. 487 (1941). Thus, another possible stop sign in the road to a federal common law for defamation is that "[c]reating a federal common law may constitute a choice-of-law rule, since the creation arises as a solution to a choice-of-law problem," thereby possibly violating the *Klaxon* doctrine. *Let the Chips Fall, supra* note 3, at 1074-75.

123. *Let the Chips Fall, supra* note 3, at 1076.

As well as offending state sovereignty, a federal common law for defamation seems difficult and unreasonable. As one commentator states: "When is the choice of law question for a particular cyber-dispute appropriately determined by this new model?"[124] "Simply 'touching and concerning' cyberspace, however, is not a sufficient reason to invoke an entirely new choice of law methodology."[125] For example, suppose *USA Today* publishes defamatory material in its newspaper distributed nationwide. Clearly, a defamation action arising out of these events would be governed by sovereign states, and the law applicable would be decided by traditional choice-of-law rules. Conversely, if *USA Today*, instead of publishing the material in its newspaper, publishes the defamatory material on its Web site, then, under Faucher's approach, this dispute would be covered by federal common law. However, what law governs—federal or state—when *USA Today* publishes the same defamatory material at the same time in both real-space (in a newspaper) and in cyberspace (on a Web site) as is predominantly the case? Does a plaintiff recover for Web site damages under federal law and newspaper damages under state law?

Regardless of these quandaries, it is entirely unreasonable that a state should lose its interest in protecting its citizens involved in a defamation dispute merely because a different medium was chosen to publish the defamatory material. There cannot reasonably be said to exist a federal interest in defamation via cyberspace that justifies stripping states of their principal interest, that of protecting their citizens. Indeed, a federal common law is not only difficult to apply, but also completely offensive to notions of state sovereignty. These are the primary interests choice-of-law rules exist to protect.

Alternatives proposing that cyberspace should be recognized as a sovereign within itself suffer from the same failing as Faucher's federal common law alternative. One such alternative similar to Faucher's approach is to make choice-of-law issues virtually irrelevant by having courts recognize a new law of cyberspace, called *lex cyberalty*.[126] The argument is that courts hearing cyber-disputes should look to *lex cyberalty* in order to determine the applicable "substantive standard of behavior."[127] Besides suffering from the same faults as Faucher's federal common law approach, it is unrealistic that this unwarranted approach would ever emerge because, for such a system to work, the states would have to relinquish their sovereign control over cyberspace.

---

124. *Conflicts on the Net*, *supra* note 17, at 89.
125. *Id.* at 90.
126. *The Scientological Defenestration*, *supra* note 5, at 369.
127. *Id.*

Choice of law is a difficult subject area because of what is at stake not only in an interstate system, but also in a unique federal system. Choice-of-law rules serve to facilitate comity between the states. Comity between states is of extreme importance, but so too is comity between the federal system and the state system. Of equal importance in a federal system, however, are the states' rights to reign supreme over the areas of law rightfully reserved to them. It is imperative for the functioning of both the interstate and federal systems that jurisdictional doctrines do not lose sight of the vital principles embodied in state sovereignty.

V. CONCLUSION

Despite the view of some, choice-of-law issues arising in cyberspace are only *sui generis* in substance, not form.[128] Instead of creating new regimes for cyber-defamation disputes, most courts apply traditional choice-of-law doctrines—usually *sub silentio*—and utilize old analogies to deal with the substance of cyberspace.[129] Stated another way: "Instead of following a virtual path for these Internet cases, most courts travel the well-worn path of traditional choice-of-law principles."[130] As cyberspace becomes more grounded and less mystifying, it becomes much clearer that cyberspace does not offer any unique problems for choice of law in defamation disputes.

The desire to criticize traditional jurisdictional rules is misplaced. The effects of cyber-defamation remain the same in real-space, and traditional choice-of-law regimes are in no way confounded by cyberspace. cyberspace is neither unique nor special for choice-of-law purposes, and as a result, there exists no reason to single out cyber-defamation as something

128. *Old Doctrines on a New Frontier*, *supra* note 11, at 56.

129. *The Scientological Defenestration*, *supra* note 5, at 363, 374; *see also* Reno v. ACLU, 521 U.S. 844, 896-97 (1997) (finding Internet communications analogous to traditional forms of speech); *see generally* EDIAS Software, Int'l v. BASIS Int'l, Ltd., 947 F. Supp. 413 (D. Ariz. 1996). This case arose out of a cyber-defamation dispute. *Id.* Despite that fact, the court, without explicitly stating its methods, chose the applicable law based on where the plaintiff's domicile and principle place of business were located and where the defamatory material was published, mirroring the Restatement (Second). *Id.* at 420; It's In The Cards, Inc. v. Fuschetto, 535 N.W.2d 11 (Wis. Ct. App. 1995). This case involved another cyber-defamation dispute where the court determined the applicable law by applying the law of plaintiff's domicile and principle place of business, which was where the defamatory material was published. As in *EDIAS Software*, the choice-of-law approach in *It's In The Cards* falls in perfect alignment with the Restatement (Second). *Id.*; Tamburo v. Calvin, No. 94 C 5206, 1995 WL 121539 (N.D. Ill. Mar. 17, 1995). *Tamburo* also involved a cyber-defamation dispute where the court found no difficulty or need to apply new choice-of-law regimes.

129. *EDIAS Software*, 947 F. Supp. 413.

130. *The Scientological Defenestration*, *supra* note 5, at 363.

in need of reformulated choice-of-law rules. Nor is there a need to abandon traditional choice-of-law rules. Besides, proposed alternatives are difficult to apply, unreasonable, and serve only to strip states of their sovereignty over cyber-defamation disputes.

As for whether traditional choice-of-law regimes are confounded by cyber-disputes arising out of other areas of law, it would seem that the answer would be no. Just as cyber-defamation poses no difficulty for traditional choice-of-law regimes, cyber-contracts, for example, should also pose no difficulty. Similarly, other traditional choice-of-law methods[131] should fare just as well in cyberspace as the Restatement (Second) does. Nevertheless, as far as the application of the Restatement (Second) to cyber-defamation disputes is concerned, there is nothing different or unique about cyberspace warranting the modification and/or abandonment of traditional choice-of-law regimes for cyber-defamation disputes. In the end, the constant slandering of traditional choice-of-law regimes for cyber-defamation disputes must give way to the dull reality of real-space.

131. *See* SHREVE, *supra* note 12.

ISSN:1692-8156

INTERNET CONFLICT OF LAWS: A SPACE OF OPPORTUNITIES FOR ODR*

CONFLICTO DE LEYES EN LA INTERNET: UN ESPACIO DE OPORTUNIDADES PARA LOS MEDIOS DE RESOLUCIÓN DE DISPUTAS EN LÍNEA

José Edgardo Muñoz-López**

Reception date: April 3rd, 2009
Acceptance date: April 17th, 2009

To cite this article / Para citar este artículo

José Edgardo Muñoz-López, *Internet Conflict of Laws: A Space of Opportunities for ODR*, 14 *International Law, Revista Colombiana de Derecho Internacional*, 163-190 (2009).

* Article produced within the Global Sales Law project, at the University of Basel. It was prepared by the author for the Fifth International Forum on Online Dispute Resolution (ODR), Liverpool, England, April 19th-20th, 2007.

** Legal practitioner and researcher whose main focus is in the fields of foreign investment, e-commerce, international contracts and commercial arbitration. Graduated in law from Universidad Iberoamericana, Mexico. He also holds a graduate degree in Law Studies from the University of Lyon, France, and a Master of Laws degree from the University of Liverpool, England. Currently (2008-2010) Research assistant in the Global Sales Law Project at the University of Basel and Doctorate Candidate in the same University. He has published in international journals and participated in international forums.
Contact: edgardo.munoz@unibas.ch.

Abstract

The inadequacy of current Conflict of Laws system, the lack of specialization, the high costs and long delays of court proceedings makes that traditional court adjudication as a means of resolving disputes is not always suitable for e-commerce disputes. Moreover, ADR (Alternative Dispute Resolution) offline is commonly impractical for B2C resolution of international e-commerce disputes and at times expensive enough so that B2B avoid engaging in them. This opens a Space of Opportunities for the use of ODR (Online Dispute Resolution) in e-commerce disputes. I aim to present in this venue some of the constructive ways in which ODR can be utilized to deal with the two main problems that emerge from relying on court judicial process, and ADR offline, to resolve e-commerce disputes: inadequacy of current Conflict of Laws system and the high costs and long delays of some e-commerce disputes.

Key words author: E-commerce, Conflict of Laws, Competent Jurisdiction, Applicable Law, Alternative Dispute Resolution, ADR, Online Dispute Resolution, ODR.

Key words plus: Electronic commerce - Juridies aspects, Conflict of Laws, Conflict management.

RESUMEN

El inadecuado sistema de Conflicto de Leyes actual, la falta de especialización, el alto costo y la lentitud del proceso judicial hacen que la adjudicación tradicional en los tribunales y cortes del Estado no sea siempre la mejor vía para resolver conflictos del comercio electrónico. Por otro lado, los medios alternos para la resolución de controversias (ADR), tales como el arbitraje y la mediación, son muchas veces imprácticos para la resolución de conflictos entre empresas y consumidores. Otras veces, suficientemente costosos para que las empresas mismas resuelvan los conflictos entre ellas a partir de los ADR. Esta situación abre un espacio de oportunidades para la utilización de medios para la resolución de disputas en línea (ODR). En esta ocasión, me propongo mostrar algunas de las maneras en que constructivamente se pueden utilizar los ODR para dar respuesta a dos de los mayores problemas que se originan de la adjudicación de disputas, a partir de la Adjudicación Estatal y los ADR tradicionales: el inadecuado sistema de Conflicto de Leyes, y el alto costo y la lentitud para resolver conflictos que se originan en el comercio electrónico.

Palabras clave autor: *Comercio electrónico, conflicto de leyes, corte competente, ley aplicable, resolución alternativa de conflictos, resolución de conflictos en línea.*

Palabras clave descriptor: *Comercio electrónico – Aspectos jurídicos, Derecho internacional privado, Solución de conflictos.*

SUMMARY

INTRODUCTION.- I. CONFLICT OF JURISDICTIONS: COMPARATIVE STUDY.- *A. B2B Competent Court.- B. B2C Competent Court.*- II. CONFLICT OF LAWS: COMPARATIVE STUDY.- *A. B2B Applicable Law.- B. B2C Applicable Law.*- III. ADR FOR E-COMMERCE.- *A. ADR as appropriate means.- B. Current consumers' issues.*- IV. ODR CONTRIBUTIONS TO ADR OFFLINE.- V. CONCLUSION.- APPENDIX A.- BIBLIOGRAPHY.

Introduction

Disagreements between contracting parties are common both in real and in cyberspace. However, the gestation of conflicts and their resolution differs in each space. E-commerce disputes originate with particular characteristics due to the internet nature and the way internet transactions are entered into.

Accordingly, the traditional State system based in public courts, and eventually ADR offline, are not always suitable to manage disputes, which originate in cyberspace. I can mention four main barriers or problems that emerge from relying on both systems of resolution of disputes, all of them apply to Courts, the last two apply to some ADR offline.

The first problem is the inadequacy of current private international law when applied to a non-territorial internet. Courts have problems to conciliate cyberspace's nature with the traditional competent jurisdiction and choice of law concepts, which have been funded by the notion of territoriality. The second problem is the incapability and unwillingness of courts to spend the time to keep updated on the changes both in technology and processes. This represents the biggest obstacle to the development appropriate (specialized) skills for the settlement of e-commerce disputes. The third and four problems are related to cost and time. E-disputants experiences are that in court litigation, and eventually in International Mediation and Arbitration, cost is very high (due to its international element), and delays are very long. This provokes resistance to the risk of court litigation and to the high expenses and delays of some ADR offline procedures.

In Part Two and Three of this work, the current state of the *conflict of laws* system is reviewed from a comparative perspective. In Part Four, it is demonstrate how the *conflict of laws* problem to establish jurisdiction and applicable law for e-commerce disputes can be solved by the use of ADR mechanisms. Also in Part Four, it is presented some of the current issues relating to ADR for consumers disputes. Part Five describes how ODR finds a Space of Opportunities to enhance ADR offline mechanisms. Part Six concludes.

I. CONFLICT OF JURISDICTIONS: COMPARATIVE STUDY[1]

E-commerce principally consists of buying, selling, marketing, and servicing using computer networks. For Lawrence Lessig, e-commerce represents one of the aspects of the internet revolution.[2] Internet architecture favoured the expansion of the market.

The abolition of borders in markets led to the dismantlement of the international private law system. The nature of the internet means that current rules of Private International Law (PIL) cannot be applied properly to e-transactions. There are two main reasons which sustain the premise that national legislation is inappropriate to govern the internet. Firstly, it is inappropriate because of the international character of the internet. Secondly, it is out of place because national legislation has always been designed for a material-order.[3]

Indeed, the conventional PIL approach inevitability looks to geography when determining the competent jurisdiction and deciding on the law for a dispute. Considering that for e-commerce, places are practically unallocated, questions like the one, '*where do activities occur, or where are the activities deemed to have occurred?*' may work for territorial PIL but not on the internet. This puts in crisis the whole system of conflict of laws which deems to deal with disputes having an international element.

For e-commerce disputes it means that preliminary issues, such as the assertion of competent jurisdiction and choice of law, become complex and unpredictable. In this section and in section 3 of this presentation we review the problems emerging from the application of current PIL.

---

1 This section mainly reviews two main systems of conflict rules for contracts: that in place in the European Union and that of the United States.

2 Lawrence Lessig, *The Future of ideas: the Fate of the Commons in a Connected World*, 114 (Vintage Books, New York, 2002).

3 Pierre Sirinelli, *Le village virtuel et la creation normative*, in *Which Court Decides? Which Law Applies*?, 14 (Katharina Boele-Woelki & Catherine Kessedjian, Kluwer Law International, The Hague, Boston, c1998).

A. B2B Competent Court

The purpose of the *conflict of laws* is to determine how a national court shall behave when confronted with a legal dispute, with an international element.[4]

The European Union, through the Brussels Regulation (BR),[5] has adopted a common set of rules to establish *competent jurisdiction* in each of the member states.[6] The court to which an e-commerce party intends to raise a claim must ensure that it has jurisdiction to rule on the issue.[7] BR provides in art. 2 (1) a general ground to establish competent jurisdiction. The article refers to the court of the member state where the defendant is domiciled.[8] (The definition of a company's domicile is found in article 60).[9]

As an alternative article 5.1 (a)(b) establishes *Special Jurisdiction.*[10] Under this provision the defendant party in matters relating to a contract, can be sued in the courts for the place of performance of the

---

4 Susan M. Nott, *For Better or Worse? The Europeanisation of the Conflict of Laws,* 24 *Liverpool Law Review*, 1-2, 3-17, 3 (2002).

5 Council Regulation (EC) No. 44/2001, of 22 December 2000, on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters [Official Journal of the European Communities, OJ L 12 of 16.01.2001].

6 Art. 1. 1. "*This Regulation shall apply in civil and commercial matters whatever the nature of the court or tribunal. 3. In this Regulation, the term 'Member State' shall mean Member States with the exception of Denmark.*" See for example cases: *LTU v. Eurocontrol* 19977 1 CMLR 293. *Netherlands State v. Ruffer* 1981 3 CMLR 293.

7 Christopher M. V. Clarkson & Jonathan Hill, *Jaffey on the Conflict of Laws,* 189 (2nd ed., Butterworths, 2002).

8 Article 2 (1). "*Subject to this Regulation, persons domiciled in a Member State shall, whatever their nationality, be sued in the courts of that Member State.*"

9 Article 60. 1. "*For the purposes of this Regulation, a company or other legal person or association of natural or legal persons is domiciled at the place where it has its:*
(a) statutory seat, or
(b) central administration, or
(c) principal place of business.
2. For the purposes of the United Kingdom and Ireland 'statutory seat' means the registered office or, where there is no such office anywhere, the place of incorporation or, where there is no such place anywhere, the place under the law of which the formation took place."

10 Article 5. "*A person domiciled in a Member State may, in another Member State, be sued: 1. (a) in matters relating to a contract, in the courts for the place of performance of the obligation in question;*
(b) for the purpose of this provision and unless otherwise agreed, the place of performance of the obligation in question shall be:
- In the case of the sale of goods, the place in a Member State where, under the contract, the goods were delivered or should have been delivered.
- In the case of the provision of services, the place in a Member State where, under the contract, the services were provided or should have been provided."

obligation in question: the place of performance of the obligation in question is: - in the case of the sale of goods, the place in a Member State where, under the contract, the goods were delivered or should have been delivered; - in the case of the provision of services, the place in a Member State where, under the contract, the services were provided or should have been provided, on matters relating to this contract.

The first questions arise: How can a Court establish the place of the specific performance in a contract of software licensing or of a sale of software, if everything can take place on the internet, where many parties in different territories are involved?

Furthermore, Article 5.5 provides that a person domiciled in a member state may, in another member state, be sued: (5) "*as regards a dispute arising out of the operations of a branch, agency or other establishment, in the courts for the place in which the branch, agency or other establishment is situated*." How many branches does '.com' company can have in through all Europe? Can a specific *country domain name* be considered as a branch *e.g.* co.uk/, en.fr/, ne.it/, em.es/, etc.? Does it mean that many European courts can establish jurisdiction?

In the US the assertion of personal jurisdiction must be consistent with the constitutional requirement of due process; "*minimum contacts*" criterion. To satisfy the due process requirement of the U.S. Constitution,[11] a defendant must have "*sufficient minimum contacts*" with the forum such that the maintenance of the suit does not offend "*traditional notions of fair play and substantial justice*."

Under what circumstances may a United State's court assert jurisdiction over the e-commerce party based on contacts that the company has with the forum territory via use of the internet?

In the Internet context, defendants have generally claimed that a remote forum cannot establish jurisdiction because the contacts are only established through a server that is not within the forum.[12] Defendants assert that their activities are not directed at the forum

11 US Constitution, amends. V, XIV.

12 Joel R. Reidenberg, *Technology and Internet Jurisdiction*, 153 *University of Pennsylvania Law Review*, 1951 (2005). http://ssrn.com/abstract=691501.

state. The contrary would mean that an e-company could be sued in all of the 50 states where its advertisements can be accessed?

There are two approaches that are dominant in US law to establish competent jurisdiction. The first of them is the three-category approach set forth in *Zippo Manufacturing Co. v. Zippo Dot Com, Inc.*[13] In this case it was distinguished between active and passive web sites. At the present case I was held that remote, passive web sites, did not accord personal jurisdiction to the forum. The Court stated:

> When a defendant makes a conscious choice to conduct business with the residents of a forum state 'it has clear notice that it is subject to suit there. … If Dot Com had not wanted to be amenable to jurisdiction in Pennsylvania, the solution would have been simple - it could have chosen not to sell its services to Pennsylvania residents.

Dissatisfaction with Zippo led to a revision to make it more consistent with the minimum contacts criterion. In *ALS Scan, Inc. v. Digital Service Consultants, Inc.*,[14] the Court looked to online targeting and to deleterious effects within the forum to determine if personal jurisdiction was appropriate. The court held that information transmitted into the jurisdiction over the Internet that causes harm within the jurisdiction provides minimum contacts.

The second approach in US is called "*the effects test*." In *Panavision International, L.P. v. Toeppen*,[15] the court established jurisdiction where a domain name was registered in order to divert internet traffic away from the forum.

These same inter-states principles would apply in determining whether a US court can assert authority over companies abroad.[16] This makes it very difficult to assess where jurisdiction can actually be found. A worst-case scenario would provide personal jurisdiction in every physical location where a e-business can be accessed or where it is susceptible to cause some effects.

---

13 952 F. Supp. 1119 (W.D. Pa. 1997).
14 293 F.3d 707 (4th Cir. 2002).
15 141 F.3d 1316 (9th Cir.1998).
16 *Graduate Management Admission Council v. Raju*, 241 F. Supp. 2d 589 (E.D. Va. 2003). *Metro-Goldwyn-Mayer Studios Inc. v. Grokster, Ltd.*, 243 F. Supp. 2d 1073 (C.D. Cal. 2003). *Yahoo! Inc. v. La Ligue contre le Racisme et l'Antisemitisme*, 379 F.3d 1120 (9th Cir. 2004).

B. B2C Competent Court

In EU, certain restrictions have been placed on the principle of party autonomy.

These restrictions typically apply in situations where there exists a qualified degree of difference between the parties in terms of their respective negotiating strengths. An important example of such a situation is when a business sells goods or services to a consumer. Consumers are deemed as being in a weaker position than the business. Thus, the jurisdictional rules of the BR stipulate that the vendor may only sue the consumer in the country where the latter is domiciled, while the consumer may always sue the vendor in the consumer's country of domicile.[17]

BR article 15 is intended to make it easier to bring Internet-based marketing and contractual operations within the ambit of the special jurisdictional rules for consumer contracts. However, article 15 remains rather nebulous on many significant points relating to e-commerce. For example, there is no detailed guidance on the meaning of the expression '*directs such activities*' (Art 15.1.3) in the context of Internet-based marketing and contracting.

Moreover, BR does not specify what is exactly meant by an *interactive website*. We can only assume that interactivity entails a facility for exchange of information between the website and those visiting it, including a facility for placement of purchase orders.

---

17 Article 15: "*In matters relating to a contract concluded by a person, the consumer, for a purpose which can be regarded as being outside his trade or profession, jurisdiction shall be determined by this Section, without prejudice to Article 4 and Article 5(5), if:*
(1) it is a contract for the sale of goods on instalment credit terms; or
(2) it is a contract for a loan repayable by instalments, or for any other form of credit, made to finance the sale of goods; or
(3) in all other cases, the contract has been concluded with a person who pursues commercial or professional activities in the Member State of the consumer's domicile or, by any means, directs such activities to that Member State or to several countries including that Member State, and the contract falls within the scope of such activities.
Where a consumer enters into a contract with a party who is not domiciled in a Member State but has a branch, agency or other establishment in one of the Member States, that party shall, in disputes arising out of the operations of that branch, agency or establishment, be deemed to be domiciled in that Member State.
This section shall not apply to a contract of transport other than a contract which, for an inclusive price, provides for a combination of travel and accommodation."

Other uncertainties concern, *inter alia*: whether digitised products may constitute goods; whether a website may constitute a '*branch, agency or other establishment*' (Art. 15.2); and the issue of protection of the vendor's good faith (including the extent of such protection).

In the United States as a general matter, jurisdiction for cases brought by consumers is determined as follows: (i) in the absence of a choice of forum clause in a contract, businesses are subject to specific personal jurisdiction in places where they target and sell goods to consumers; (ii) many American courts have refused to uphold choice-of forum clauses in consumer contracts on the ground that they are unfair and unreasonable.

In addition, US courts have generally held that consumer protection authorities can assert jurisdiction over foreign businesses harming American consumers.

II. Conflict of Laws: Comparative Study

As previously mention, there are two main reasons for considering the current PIL system inappropriate for establishing the law applicable to e-commerce transactions. On the one hand, conflict rules for the applicable law to a dispute lead to the application of national law to international problems. This is unsuitable because national law has been developed for national and not for international situations and, for that reason, it does not always provides the best answers to international business problems.[18] On the other hand, the techniques used in conflicts of laws rules are not always effective. They always look to connecting points in international situations but remain blind to cyber-realities.[19] It is difficult, and sometimes arbitrary, to localize some complex e-business in one applicable law.

18 Filip de Ly, *International Business Law and Lex Mercatoria*, 57 (North-Holland, Amsterdam, 1992).

19 *Ibid*, 58.

A. B2B Applicable Law

The issue of *choice of law* in the EU is also problematic. The Rome Convention (RC) allows the parties to choose which law to rule their contracts.[20] In a world without boundaries like cyberspace, it makes sense to allow contracts to govern which law applies and which do not. The competent European court will be required to appreciate whether or not there exists an implied choice of law under article 3 of the RC.[21] In the absence of expressed choice, the contract is governed by the law of the country with which it is most closely connected. The RC, as most *choice of law* rules, refers to the principle of the proper law, the law with most significant relationships or relevant contact.

Article 4.1 Paragraph 2 clarifies the expression by declaring: "*...a contract is* most closely connected *with the country where the party who is to effect the* performance which is characteristic *of the contract has, at the time of conclusion of the contract, his habitual residence, or, in the case of a body corporate or unincorporated, its central administration*." The formula is deliberately vague. It represents a difficult task, since there is a risk of uncertainty as to the solution selected.

The "*characteristic*" performance is that which constitutes the centre of gravity of the contract.[22] Basically, the party providing the characteristic performance is the person to whom the payment is due, *i.e.* the delivery of goods or the provision of a service. In a contract of software licensing the party providing the characteristic performance would be the one that allows the use of the software itself; and for the sale of products is certainly the party which must be paid for the goods delivered. But how can one distinguish the

20 Adrian Briggs, *The Conflict of Laws*, 54 (Oxford University Press, Oxford, 2002).

21 Convention on the law applicable to contractual obligations (80/934/EEC). Article 3. "*Freedom of choice. 1. A contract shall be governed by the law chosen by the parties. The choice must be expressed or demonstrated with reasonable certainty by the terms of the contract or the circumstances of the case. By their choice the parties can select the law applicable to the whole or a part only of the contract*."

22 "*The submission of the contract, in the absence of a choice by the parties, to the law appropriate to the characteristic performance defines the connecting factor of the contract from the inside, and not from the outside by elements unrelated to the essence of the obligation such as the nationality of the contracting parties or the place where the contract was concluded. ...The concept of characteristic performance essentially links the contract to the social and economic environment of which it will form a part... Which usually constitutes the centre of gravity and the socio-economic function of the contractual transaction*." *Ibid*.

domicile of a web-company that negotiate and enter into contracts from different internet interfaces through its subsidiary companies that can be accessed through different domain names registered in many jurisdictions and accessible world-wide?

Moreover, EU courts could disregard the presumption of Art 4.1.2 "*if it appears from the circumstances as a whole that the contract is more closely connected with another country.*"[23] This looks like a transgression.[24] This means that if the characteristic performance cannot be determined, an EU court can apply a different law, if it appears from the circumstances as a whole, that the contract is more closely connected with the law of another country.

This vague approach, as it prevails today in the EU, is not adequate for e-commerce. It is a bad way to handle *applicable law* for internet disputes.[25]

The US *conflict of laws* system is not better designed. It lacks clear rules and consists of several different, co-existing approaches.

Although the most significant relationship approach can be identified as in other *conflict of laws* rules, this approach provides nothing more than general guidelines and leaves considerable leeway for US judges to decide the question of applicable law. It is important to mention that the applicable law may often depend on the jurisdictional result, since US courts have an inclination to apply the *forum law*.[26]

For instance, in *Twentieth Century Fox Film Corp. v. iCrave TV*, a film studio fought successfully to apply US copyright law and obtained an injunction against a Canadian service that could legally stream video

---

23 Article 4(5).

24 "The exception clause *of Article 4(5) must be used carefully and rarely since its frequent application leads to unforeseeability as to the applicable law – an unforeseeability [...].*" "*Only if it emerged that the law designated is not appropriate because other circumstances clearly militate in favour of another law would the court then use the exception clause*." This is precisely the rule laid down in a *Decision of the Dutch Hoge Raad*, whereby the court must first apply the presumption of Article 4(2) and rule out the law thus obtained only if it is obviously unsuited to the instant case. *Green Paper on the conversion of the Rome Convention into a Community instrument and its modernisation*.

25 Matthew Burnstein, *A global network in a compartmentalised legal environment*, in *Which Court Decides? Which Law Applies?* 28 (Katharina Boele-Woelki & Catherine Kessedjian, Kluwer Law International, The Hague, Boston, c1998).

26 Simone van der Hof, *The Relevance of Party Autonomy with respect to International Online B2B Contracts – A European and US Perspective*, 4. http://hcch.e-vision.nl/upload/wop/e-comm_vdhof.pdf.

in Canada from servers in Canada. US courts tend to apply its *forum law* when in their consideration it justifies the application of US law and not when it leads to the application by a *conflict* rule.[27]

B. B2C Applicable Law

In the EC, the RC contains special rules to protect the weaker parties, such as consumers. The mere fact that a contract specifies that a particular law is to be applicable shall not deprive a consumer of the protection of mandatory rules of the law normally applicable to them.

Where the parties have made not provided otherwise in their contract, a consumer contract is governed by the law of the country where the consumer is habitually resident.

In the United States the applicable law may often depend on the jurisdictional result, since US courts have an inclination to apply the forum law,[28] especially in cases of protection of consumers located within the their territory.

III. ADR FOR E-COMMERCE

ADR offers alternative means to deal with international e-commerce disputes. ADR can be more flexible and specialized than traditional Court adjudication. As a starting point, ADR can be used to evade the *conflict of laws* complicated process. However, E-disputants experiences are that in some ADR off-line cost is very high (due to its international element), and delays are sometimes long. This provokes resistance to traditional ADR.

A. ADR as appropriate means

In ADR no *conflict of laws* system is immediately applicable.[29] For instance, mediators do not make use at all of conflict rules, or any

---

27 John Rothchild, *Jurisdiction over E-Commerce Transactions: United States Law*. 2. http://hcch.e-vision.nl/upload/wop/e-comm_rothchid.pdf.

28 Simone van der Hof, *op. cit.*, 4.

29 De Ly, note 18 above, 91.

national law. The parties themselves solve their disputes through a process of negotiation, and international arbitrators are not bound to deal with conflict rules. Let me explain how the *conflict of laws* process is highly simplified in international commercial arbitration, which may be considered as the only adjudicative procedure of ADR.

The principle of party autonomy also applies for international arbitration. This means that the parties can agree that any controversy or dispute arising out of, or relating to, their e-contract, will be settled solely and exclusively by binding arbitration in X country. They can also agree that such arbitration will be conducted in accordance with the prevailing laws in *Y* country, but that the law of country *Z* will govern the merits of the case. The arbitral agreement is, in this regard, very effective because it grants jurisdiction to the arbitral tribunal and prevents courts from ruling with regard to the decision on the merits of the case. The problem of *competent jurisdiction* and *choice of law* is completely solved. Certainty and predictability is achieved as parties know where, who and how their dispute will be settled.

Moreover, even in the case where the parties entered into an arbitration agreement which does not establish the seat of the arbitration, *curial law*, nor *choice of law* for the merits of the case, the arbitration *conflict of laws* process would be easier and would provide more certainty and predictability than the courts' *conflict of laws* procedure.

When no choice has been expressed by the parties, the arbitrator will determine the place of arbitration so that there can be no misunderstanding regarding the place.[30] If the parties did not choose the law for the proceeding (*curial law*) the governing law is the law of the seat of the arbitration (*Lex loci arbitri*).[31] Parties are free to agree the law governing their substantive rights and obligations. For their own convenience, they may decide to refer to the law of a particular country, to public international law[32] or to *lex mercatoria* or, to equity and good conscience. When they have chosen the applicable law the courts and tribunals will respect that choice.

---

30 *Ibid*, 85.

31 Jonathan Hill, *The Law relating to International Commercial Disputes*, 477 (Lloyd's of London Press, London, New York, 1994).

32 See, for instance, the Vienna Convention for the International Sale of Goods. http://www.cisg-online.ch.

In the absence of choice the basic principle is that the *curial law* determines the law the arbitrator must apply.[33] In practice they use the *conflict of law* rules of the law to the proceedings, which is generally the law of the seat. However, arbitrators have more freedom as to the application of the conflict rules and show a more transnational reflex. They do not tend to take a *homeward view*, that is, they do not manipulate the conflict rules so that the *Lex fori* would be the applicable law to the merits, as is often the case with court judges.

In most countries, the arbitrator is free, in the absent of a choice of law, to apply those rules of law which he considers appropriate.[34] Also, in international commercial arbitration attention has been paid to contract clauses and trade usages as viable resolution rules. For instance, article VII (1) of the European Arbitration Convention[35] provides that arbitrators shall take account of the terms of the contract and trade usages, whether or not the parties have indicated the applicable law. Similarly, under article 28 (4) of the Uncitral Model Law, the arbitral tribunal shall take into account the usages of the trade applicable to the transaction.[36]

Also, arbitration is chosen because parties are more willing to execute an arbitral award than a court judgement. This expectation is based upon the high percentage of voluntary compliance with institutionalised arbitral awards.[37] What is more, the existence of the New York Convention[38] makes it easier for an international arbitral award to be recognized and enforced in a foreign jurisdiction, than it is for a foreign national court judgement.[39]

---

33 Hill, note 31 above, 481.

34 For instance France; article 1496 of the French New Code of Civil Procedure: "*The arbitrator shall determine the dispute in accordance with the rules of law that the parties have chosen; in default of such a choice, in accordance with those which he shall deem appropriate. He shall consider in any case the customs in commercial activities.*"

35 European Convention on International Commercial Arbitration. http://www.law.berkeley.edu/faculty/ddcaron/Documents/RPID%20Documents/rp04011.html.

36 UNCITRAL Model Law on International Commercial Arbitration (1985). http://www.jus.uio.no/lm/un.arbitration.model.law.1985/.

37 According to the International Chamber of Commerce, 90% of the awards are spontaneously complied. *2004 Statistical Report*, *ICC International Court of Arbitration Bulletin*, 16/1, 21.

38 United Nations Convention on the Recognition and Enforcement of Foreign Arbitral Awards (New York, June 10th, 1958). http://www.uncitral.org/uncitral/en/uncitral_texts/arbitration/NYConvention.html.

39 De Ly, note 18 above, 85.

In brief, ADR offline offers an appropriate means to deal with international e-commerce disputes, while evading the *conflict of laws* complicated process.

B. Current consumers' issues[40]

In most countries there are no specific provisions that prohibit contractual agreements between parties to be bound by ADR after a dispute has arisen.[41]

However, the general practice appears to be that contractual provisions binding parties to ADR prior to a dispute having arisen may be regarded as an "*unfair*" contract term (mostly because of expenses issues) or contrary to public policy, notably if it deprives the consumer to the right to go to court.[42]

Legislation in EU for example mandates that consumer contracts entered prior to a dispute containing an arbitration clause are automatically invalid as unfair. Similarly, in the United Kingdom, an arbitration agreement is automatically void as unfair for consumers specifically if it relates to a claim for a small amount.

In contrast, in the United States, a consumer is free to consent to be bound by ADR but that contract law will apply to ultimately determine the validity of a contract to engage in and be bound by ADR. For example, in the United States, a contract is not invalid simply because it deprives the consumer of the right to go to court – the validity of a contract in this situation is decided on a case-by-case basis. The general rule is that such contracts are valid, irrevocable, and enforceable, except where they violate general principles of contract law, such as fraud, duress or unconscionability.

---

40 Organisation for Economic Co-operation and Development, OECD, Committee for Information, Computer and Communications Policy Committee on Consumer Policy, Working Party on Information Security and Privacy, 8 (July, 2004).

41 For example, Mexico, Austria, France and Italy noted that in the case of agreements signed at the conclusion of an ADR process, contractual autonomy is recognised and agreements signed by the parties will be binding according to contract law.

42 Countries which adopted this approach included Australia, Austria, Canada, Denmark, Finland, Italy, Japan, Netherlands, Spain and Sweden.

Legislation in Japan also indicates that an agreement to refer future disputes to arbitration is valid as long as it relates to determined relations of right and disputes arising there from.

In most jurisdictions the reasons sustaining the invalidity of those ADR agreements are often based on the high cost of some ADR that would unbalance participation of parties and the opportunity for consumers to present their cases.

For instance, critics say arbitration and some international mediations can mean high filing fees. Filing a case in national courts is often very cheap if not free of charges for consumers, depending on the amount claimed. Filing fees for arbitration can cost thousands of dollars, depending on the case and the arbitration institution. Fees for hearing rooms and the arbitrator's time can run tens of thousands of dollars more and discourage individuals from pursuing a case. As well as the traveling expenses incurred in some international disputes.

IV. ODR CONTRIBUTIONS TO ADR OFFLINE

It is evident that the volume of B2B and B2C electronic commerce will continue to increase dramatically for the next decade. Consequently, it is reasonable to assume that disputes arising in the internet between small, medium and large size companies or between business and consumers can be resolved through the use of the internet.

ODR has adapted a range of traditional ADR processes for use online, including arbitration and mediation. In this sense, ODR has all the advantages of the ADR mechanism including the capacity to evade the *conflict of laws* problem of traditional court adjudication.

But ODR goes beyond ADR offline, as ODR uses the power that computer technology has, to support the storage and dissemination of information. This power can be used to solve the two main problems encountered in some ADR off-line procedures: high cost and long delays in international mediation and arbitration.[43]

43 For a comparative analysis of cost and time of ADR off-line *vis à vis* ODR cost and time procedures see Appendix A.

ODR provides an environment where communication power can be balanced. ODR can empower weaker parties, including small companies and consumers, by taking away some imbalance issues. For instance, ODR is said to avoid travel expenses, thereby reducing geographic constraints and take away a power imbalance. Rather than avoid disputes because of high cost or long distances, enterprises and consumers can seek resolution of disputes with bigger companies, which may not be possible without computer technology. Thus, consumers and businesses that may be perceived as "*petite*" at the bargaining table are no longer in this position.

Online mediation can be via email[44] or through a secure website.[45] There are many providers of online mediation including Dispute Manager, WebMediate, and Square Trade among others.[46] There are also many providers of online arbitration, including Nova Forum, Private Judge and Word & Bond.[47]

Cyber-mediation may be the only feasible option for individuals who are unable to afford travelling long distances, or for those involved in e-commerce disputes for low amounts of money.

With attorney's fees being perhaps the greatest expense in traditional litigation, or even sometimes traditional mediation and arbitrations, parties may be able to save a lot of money in cyber-mediation, where hiring an attorney is often unnecessary. For example, if the parties have determined liability and their dispute is solely over the amount of a monetary settlement, then the fully automated cyber-mediation websites discussed above may be sufficient to resolve their dispute.[48]

In addition, substantial cost savings may also result because online mediation does not require parties to pay for long-distance phone calls or teleconferencing.

---

44 Email - a virtually instantaneous transfer of text messages.

45 Instant Messaging - a variant on email that can be used asynchronously and also allows synchronous online chat.

46 Melissa Conley Tyler, *Seventy-six and Counting: An Analysis of ODR Sites*, in *Proceedings of the UNECE Second Forum on Online Dispute Resolution,* 8 (Ethan Katsh & Daewon Choi, eds., Center for Information Technology and Dispute Resolution, University of Massachusetts, 2003). www.odr.info/unece2003/pdf/Tyler.pdf.

47 Conley, note 46 above, 9.

48 To know about the fees charge for some of the most important ODR providers see Appendix A.

Perhaps the most recognized benefit of ODR mechanisms is that the disputants do not have to travel lengthy distances to negotiate. Since online disputes can arise between individuals from great distances, and even different countries, at least one of the parties will be required to travel far if they decide to rely on a traditional dispute resolution procedure.

Certainly, parties can participate in ODR from their respective business locations or residences; this may lead to reduced costs and the expenditure of less time. There is no need to rent a neutral facility to conduct the mediation and relevant documents and materials are readily available and do not have to be transported great distances.

V. CONCLUSION

We know that the main elements to consider in *choice of dispute resolution mechanisms* for E-commerce are access barriers such as costs and time, transparency of proceedings and resolutions, and increased cross-border litigation. The main access barriers (problems) to national courts are their use of inadequate private international rules, costs, long delays, rigid procedures and lack of specialization.

ADR offline can be successfully used to evade the *conflict of laws* complicated process. The jurisdiction problem is immediately solved. Certainty and predictability is achieved as parties know where, who and how their dispute will be settled.

ODR goes beyond as it not only solve the problem of the conflict of laws process but also is successful in reducing legal costs and time consumption for business disputants. Computer technology spread of massive amounts of free information is further lowering access barriers to mediation and arbitration cases. ODR is not just flexible, specialized and expeditious but also empowers the individual. ODR processes allow parties to adopt positional bargaining and problem-solving modes to solve e-commerce disputes. ODR offers more appropriate procedures for e-commerce because different (cyber) circumstances and (cyber) interests require creative procedures.

Appendix A
Cost and Time of ADR offline Procedures

ADR-offline providers	Fees and average cost	Average of delay
ICC ADR	**Appendix** **Schedule of ADR Costs** A. The party or parties filing a Request for ADR shall include with the Request a non-refundable registration fee of US$1,500 to cover the costs of processing the Request for ADR. No Request for ADR shall be processed unless accompanied by the requisite payment. B. The administrative expenses of ICC for the ADR proceedings shall be fixed at ICC's discretion depending on the tasks carried out by ICC. Such administrative expenses shall not exceed the maximum sum of US$10,000. C. The fees of the Neutral shall be calculated on the basis of the time reasonably spent by the Neutral in the ADR proceedings, at an hourly rate fixed for such proceedings by ICC in consultation with Neutral and the parties. Such hourly rate shall be reasonable in amount and shall be determined in light of the complexity of the dispute and any other relevant circumstances. The amount of reasonable expenses of the Neutral shall be fixed by ICC.	
LCIA	**Schedule of Costs** I. Registration Fee The Registration Fee referred to in Article 3 of the Rules of the Arbitration Institute of the Stockholm Chamber of Commerce (the "SCC Rules") amounts to EUR €1,500. Arbitrators' fees are calculated according to the amount in Dispute in Euros: up to €25,000= 2,500 min/5500max, from 25,000 to 50,000= 2,500 + 2% of the amount above 25,000 min/ 5,500 +14% of the amount above 25,000 max, from 50,001 to 100,000= 3,000 + 2% of the amount above 50,000 min/ 9,000 +4% of the amount above 50,000 max…	There is no such thing as an "average" arbitration. However, if one discounts those cases which may be said to be atypically long or short (passing two years at one extreme and settling before the appointment of the Tribunal at the other) the present average duration of an LCIA arbitration is approximately 11 months.

ADR-offline providers	Fees and average cost	Average of delay
El Centro de Arbitraje de México (CAM)	Artículo 38: Depósito para cubrir los gastos del arbitraje Corresponde al Secretario General fijar el importe del depósito de fondos para cubrir los gastos de arbitraje utilizando el Arancel para el cálculo de los gastos del arbitraje que establece el Apéndice II. Según el calculador automático por un monto del litigio equivalente a $100.000 pesos mexicanos, la tasa administrativa será de un valor de $22.000 pesos mexicanos (US$2,000) y los honorarios de un árbitro serán de $48.000 pesos mexicanos (US$4,200).	
World Intellectual Property Organization (WIPO) *Arbitration Mediation*	Mediation Administrative fee is 0.10% of the value of the mediation, subject to a maximum of US$10,000. Mediators fees are US$300-US$600 per hour or US$1,500-US$3,500 per day. Administration fee for Arbitration are up to $2,5M = $2,000, from $2,5M to $10M = $10,000, over $10M = $10,000 + 0.05% to a maximum fee of $25,000. Arbitrator(s) fees for Arbitration are up to $2,5M, from $2,5M to $10M, over $10M = As agreed by the Center in consultation with the parties and the arbitrator. Indicative rate(s) $300 to $600 per hour.	

COST AND TIME OF ODR PROCEDURES

ODR providers	Fees and average cost	Average of delay
Camera Arbitrale di Milano *Online Mediation*	Fees for each party in EURO (VAT included) shall depend on the economic value of the dispute up to 500 = 25, from 501 to 1.000 = 40, from 1.001 to 5.000 = 80 from 5.001 to 10.000 =150, from 10.001 to 25.000 = 250 from 25.001 to 50.000 = 450, from 50.001 to 250.000 = 1.000, over 250.001 = 3.000.	From one to two weeks
Cibertribunal peruano *Concilation and Arbitration*	CONCILIATION The applicant US$60.00. The party invited US$60.00. The administrative expenses for the conciliation procedure depend on the amount of the controversy and the tariff table will apply. ARBITRATION Cost for Arbitration Appointment of arbitrator shall depend on the value of the dispute up to US$1,000 = 100, from 1,001 to 3,000 = 300, from 3,001 to 5,000 = 500, from 5,001 to 10,000 = 600. The administrative expenses for the arbitration procedure depend on the amount of the controversy and the tariff table will apply.	
Conflict Resolution.com Mediation	Most mediators charge between $100.00 and $300.00 per hour, divided equally between the parties. (Retired judges often charge more than $300.00 per hour).	
Mediation Arbitration Resolution Services (MARS)	Complaint Filing Fee $10.00 Complaint Response Fee without a Seal (Online Dispute Resolution Case Management Service) $10.00. Cost should a mediator/arbitrator need to become involved in a case (this fee is only incurred should you and the consumer/buyer not be able to settle the dispute on your own) $30.00. Should the mediator/arbitrator be required to settle the case and make an award in favor of the consumer/buyer, there will be a Complaint Resolution Fee of 3.00% of the award, charged to you.	

ODR providers	Fees and average cost	Average of delay
Mediation Now	The cost for online mediation, as with traditional mediation, varies from mediator to mediator, and with the complexity of the issues. In addition to the actual mediation session, mediators typically charge for their preparation time and also for any post-mediation tasks requested by the parties. There may be some cost savings associated with online mediation which might not be available with traditional mediation: • Use of physical conference and meeting space is not needed. • Since online mediation usually involves extensive written communication, the parties may be more deliberate and efficient in their communication. • Again, since there may be extensive written communication, the parties may find it easier to codify agreements reached. • The parties and the mediator do not have to travel to a central location.	
ODRWorld	FEES Currently we are having an introductory offer: Assisted Negotiation - US$15 per case for a period of 14 days Automated Negotiation – US$15 per case. If bids do not match, parties can have any number of attempts for a period of 14 days. Mediation – US$38 per case for a period of 14 days. Arbitration - US$380 – US$1,200 (depending upon the subject matter of the case). In the event parties wish to apply for extension, during the introductory period, extension will be provided for a further 14 days at the rate of US$15 for Assisted Negotiation and US$38 for Mediation.	A period of 14 days

ODR providers	Fees and average cost	Average of delay
Private Judge	Mediation Private Judge works with parties to facilitate an agreement. Fee: US$2,000 to US$5,000 per party per day. Arbitration Private Judge, after weighing the evidence and the law, renders a decision. Arbitration by international treaties. Cases billed on a project basis, based on the time and complexity of the dispute. Administration Fee: US$1,200.	A typical arbitration might last from one to ten days, but it can take longer in complex disputes.
SquareTrade *Mediation*	Standard Pricing US$29.95	
The Claim Room	For a settlement value up to and including £2,000 - £100 Over £2,000 and up to and including £5,000 - £200 Over £5,000 and up to and including £10,000 - £300 Over £10,000 - £400	
Webmediate.com	It is generally $30 to register a new matter with WebMediate. If your matter is successfully resolved through WebSettlement, the fee is 5% of all settlements under US$5,000 (not to exceed $100) and 2% of all settlements over US$5,000 (not to exceed $400), which fee is divided equally between the parties. WebMediation and WebArbitration fees are based on the time devoted by the WebMediator or WebArbitrator to the matter. Generally, the fee is US$250 per hour for these services, divided between the parties.	In general, WebMediation may be completed within 14 days In WebArbitration, the rules provide that the parties may take longer to submit their formal statements and rebuttals.

ODR providers	Fees and average cost	Average of delay
World Intellectual Property Organization (WIPO) *Arbitration Mediation*	Mediation Administrative fee is 0.10% of the value of the mediation, subject to a maximum of US$10,000. Mediators fees are US$300-US$600 per hour or US$1,500-US$3,500 per day. Registration fee for expedited Arbitration is US$1,000 and for Arbitration is US$2,000. Administration fee for expedited Arbitration are up to $2,5M = $1,000, from $2,5M to $10M = $5,000, over $10M = $5,000 + 0.05% to a maximum fee of $15,000. Arbitrator(s) fees for expedited Arbitration are up to $2,5M = $2,000, from $2,5M to $10M = $40,000, over $10M = As agreed by the Center in consultation with the parties and the arbitrator.	
The Asian Domain Name Dispute Resolution Centre (ADNDRC) Arbitration	1 to 2 domain names US$500 Presiding Panelist: US$1,000 Each Co-Panelist: US$500	57 days normal procedure

BIBLIOGRAPHY

Books

Burnstein, Matthew, *A Global Network in a Compartmentalised Legal Environment*, in *Which Court Decides? Which Law Applies?* (Boele-Woelki, Katharina & Kessedjian, Catherine, Kluwer Law International, The Hague, Boston, c1998).

Clarkson, Christopher M. V. & Hill, Jonathan, *Jaffey on the Conflict of Laws* (2nd ed. Butterworths, 2002).

Conley-Tyler, Melissa, *Seventy-six and Counting: An Analysis of ODR Sites*, in *Proceedings of the UNECE Second Forum on Online Dispute Resolution* (Katsh, Ethan & Choi, Daewon, eds., Center for Information Technology and Dispute Resolution, University of Massachusetts, 2003). www.odr.info/unece2003/pdf/Tyler.pdf.

De Ly, Filip, *International Business Law and Lex Mercatoria* (North-Holland, Amsterdam, 1992).

Hill, Jonathan, *The Law Relating to International Commercial Disputes* (Lloyd's of London Press, London, New York, 1994).

Hof, Simone van der, *The Relevance of Party Autonomy with respect to International Online B2B Contracts – A European and US Perspective.* http://hcch.e-vision.nl/upload/wop/e-comm_vdhof.pdf.

Lessig, Lawrence, *The Future of ideas: the Fate of the Commons in a Connected World* (Vintage Books, New York, 2002).

Mackie, Karl J., *A Handbook of Dispute Resolution: ADR in action* (Routledge, London, 1991).

Rothchild, John, *Jurisdiction over E-Commerce Transactions: United States Law.* http://hcch.e-vision.nl/upload/wop/e-comm_rothchid.pdf.

Journals

Katsh, Ethan, Rifkin, Janet & Gaitenby, Alan, *E-Commerce, E-Disputes, and E-dispute Resolution: in the Shadow of "eBay Law".* 15 *Ohio State Journal on Dispute Resolution*, 3 (2000).

Nott, Susan M., *For Better or Worse? The Europeanisation of the Conflict of Laws,* 24 *Liverpool Law Review*, 1-2, 3-17 (2002).

Reidenberg, Joel R., *Lex Informatica: The Formulation of Information Policy Rules through Technology,* 76 *Texas Law Review*, 553 (1998).

Reidenberg, Joel R., *Technology and Internet Jurisdiction*, 153 *University of Pennsylvania Law Review* (2005). http://ssrn.com/abstract=691501.

Treaties and other International Agreements

Convention on the Law Applicable to Contractual Obligations (80/934/EEC). http://www.rome-convention.org/instruments/i_rep_lagarde_en.htm.

Convention on the Recognition and Enforcement of Foreign Arbitral Awards (1958). http://www.uncitral.org/uncitral/en/uncitral_texts/arbitration/NYConvention.html.

Council Regulation (EC) No 44/2001, of 22 December 2000, on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters [Official Journal of the European Communities, OJ L 12 of 16.01.2001].

European Convention on International Commercial Arbitration. http://www.law.berkeley.edu/faculty/ddcaron/Documents/RPID%20Documents/rp04011.html.

UNCITRAL Model Law on International Commercial Arbitration (1985). http://www.jus.uio.no/lm/un.arbitration.model.law.1985/.

Vienna Convention for the International Sale of Goods. http://www.cisg-online.ch.

Reports

2004 Statistical Report, ICC International Court of Arbitration Bulletin, 16/1. 21.

OECD (2002b), Report on Legal Provisions Related to Business to Consumer Alternative Dispute Resolution in Relation to Privacy and Consumer Protection, OECD, Paris, www.olis.oecd.org/olis/2002doc.nsf/linkto/dsti-iccp-reg-cp(2002)1-final.

Cases

Graduate Management Admission Council v. Raju, 241 F. Supp. 2d 589 (E.D. Va. 2003).

LTU v. Eurocontrol 19977 1 CMLR 293.

Metro-Goldwyn-Mayer Studios Inc. v. Grokster, Ltd., 243 F. Supp. 2d 1073 (C.D. Cal. 2003).

Netherlands State v. Ruffer 1981 3 CMLR 293.

Yahoo! Inc. v. La Ligue contre le Racisme et l'Antisemitisme, 379 F.3d 1120 (9th Cir. 2004).

Zippo Manufacturing Co. v. Zippo Dot Com, Inc. 952 F. Supp. 1119 (W.D. Pa. 1997).

National Laws

Dutch Code of Civil Procedure

French New Code of Civil Procedure

United States Constitution

Websites

LexMercatoria.org, http://www.lexmercatoria.org/

The Hague Conference on Private International Law, http://www.hcch.net/

UNIDROIT, http://www.unidroit.org/

NOTES

Conflicts on the Net: Choice of Law in Transnational Cyberspace

ABSTRACT

No recent technological advance has captured the attention and imagination of the United States and the international community like the advent of global communications networks—the Internet, Cyberspace, the Information Superhighway. While the technology advances daily, a legal regime for ordering cyberspace has not yet evolved. Already, cases are reaching the courts in which plaintiffs complain of improper and unlawful activities by defendants in cyberspace. Both cyberspace's growing ubiquity and the anonymity found online will increase international use of the networks for interaction and commerce. This Note considers the conflict of laws implications of transnational cyberspace. The need to consider choice of law in the networked world arises because conventional choice of law approaches—such as lex loci delicti *and the most-significant relationship test—are location-oriented. This orientation falters in a cyberspace arranged not by countries, states, and provinces, but by networks, domains, and hosts. The author concludes that many choice of law questions should be resolved in contracts between users and access-providers. Other conflicts questions might require a whole new approach, perhaps using admiralty laws, the* lex mercatoria, *or choice of law in Antarctica as a model. Finally, a multinational choice of law accord might be required to solve choice of law conflicts in cyberspace.*

HeinOnline -- 29 Vand. J. Transnat'l L. 75 1996

TABLE OF CONTENTS

I. INTRODUCTION 77
II. TRANSNATIONAL CYBERSPACE 78
A. *Cyberspace as the Global Village* 79
B. *Cyberspace and Territoriality* 81
III. OBLIGATIONS IN TRANSNATIONAL CYBERSPACE 83
IV. A UNIFIED APPROACH TO CHOICE OF LAW IN TRANSNATIONAL CYBERSPACE 87
A. *Introduction* 87
1. A Note on Jurisdiction 87
2. Why Develop a Choice of Law Regime? 88
3. The Nexus Requirement: Which Cyber-Disputes Require a New Choice of Law Regime? 89
B. *Why are Conventional Regimes Insufficient in Cyberspace?* 92
1. Choice of Law for Actions in Tort 92
a. *Lex Loci Delicti* 93
b. Most Significant Relationship 94
2. Choice of Law for Contracts Without a Forum Selection Clause 95
C. *The Unified Approach to Choice of Law in Cyberspace* 96
1. Case 1: Resolving Choice of Law for Cyber-Disputes via Contracts 97
a. The Use of Forum Selection Clauses 97
b. Forum Selection Clauses in Cyberspace 99
2. Case 2: Conceptual Analogies for a New Jurisdiction of Cyberspace 102
a. Admiralty and Cyberalty 103
i. Different Access Providers, Different Flags 105
ii. Flags of Convenience in Cyberspace 107
b. The Law Merchant and Law Cyberspace 108
c. Choosing Law in Sovereignless Regions 110
i. Outer Space 110
ii. Antarctica 111

HeinOnline -- 29 Vand. J. Transnat'l L. 76 1996

d. Prospects for a Multilateral Choice of Law Treaty for Cyberspace 112
3. Case 3: Where Conventional Choice of Law Must Still Reign..... 114
IV. CONCLUSION 116

I. INTRODUCTION

> That Other World is vast too; to its inhabitants, their System is limitless.
>
> The Electronic World enmeshes the Earth, and reaches beyond it. Information is moved through the computer systems and processed by the artificial intelligences. The programs compute and search, retrieve and collate; they are already indispensable to science, industry, education, and government—to society in its present form.[1]

It was not long ago that smoke signals and drums represented the quickest means of communication.[2] In the latter half of the twentieth century, global electronic networks have revolutionized communication, spawning technology that is still in its infancy. The popular press is replete with articles about "cyberspace,"[3] "the information superhighway," and "the

---

1. BRIAN DALEY, TRON 7 (1982) (a science fiction novel, which the Walt Disney Studio made into a movie in 1982).

2. Linda M. Harasim, *Global Networks: An Introduction*, *in* GLOBAL NETWORKS 3, 4 (Linda M. Harasim ed., 1993). *See also* ARTHUR C. CLARKE, HOW THE WORLD WAS ONE: BEYOND THE GLOBAL VILLAGE 2-3 (1992).

> When Queen Victoria came to the throne in 1837, she had no swifter means of sending messages to the far parts of her empire than had Julius Caesar—or, for that matter, Moses. . . . The galloping horse and the sailing ship remained the swiftest means of transport, as they had for five thousand years.

CLARKE, *supra*, at 203. Harasim and Clarke reveal how revolutionary the communicative possibilities of global communications networks are, particularly when viewed against the backdrop of historically slow-moving advances in communication.

3. William Gibson coined "Cyberspace" in NEUROMANCER 51 (1984) (a science fiction novel).

> Cyberspace. A consensual hallucination experienced daily by billions of legitimate operators, in every nation. . . . A graphic representation of data abstracted from the banks of every computer in the human system. Unthinkable complexity. Lines of light ranged in the nonspace of the mind, clusters and constellations of data.

Id. at 51.

HeinOnline -- 29 Vand. J. Transnat'l L. 77 1996

Internet."[4] It is unusual to read a newspaper or newsmagazine without finding at least a passing reference to these new technologies. Although some authors have begun to address the legal implications of the interconnected planet, the legal world has not yet crafted a jurisprudence of cyberspace.[5]

This Note illustrates the varieties of disputes that arise in this new technological world, then focuses on the choice of law implications of a nongeographical, nonterritorial cyberspace.[6] Part II analyzes the architecture, contours, and dynamics of transnational cyberspace.[7] Part III surveys legal problems that arise in the context of cyberspace, particularly with regard to contracts and torts.[8] Part IV articulates a new paradigm for choice of law in transnational cyberspace that is compatible with the architecture of transnational cyberspace described in Part II.

II. TRANSNATIONAL CYBERSPACE

> Cyberspace is a globally networked, computer-sustained, computer-accessed, and computer-generated, multi-dimensional, artificial, or virtual reality. In this world, onto which every computer screen is a window, actual, geographical distance is irrelevant. Objects seen or heard are neither physical nor, necessarily, presentations of physical objects, but are rather—in form, character, and action—made up of data, of pure information. This information is derived in part from the operation of the natural, physical world, but is derived primarily from the immense traffic of symbolic information, images, sounds, and people, that constitute human enterprise in science, art, business, and culture.[9]

---

4. A survey of the Westlaw ALLNEWS database, performed September 30, 1995, revealed 20,209 stories in newspapers and newsmagazines containing "Internet," "Superhighway," or "Cyberspace" in the title.

5. A survey of the Westlaw JLR (Journals and Law Reviews) database, performed October 25, 1995, revealed 84 articles discussing legal issues in cyberspace.

6. Professor Dan L. Burk, cited regularly in the popular and academic presses for his work on the law of cyberspace, has termed jurisdictional issues "*the* major issue for the net." Dan L. Burk, *RE: US Jurisdiction over Cyberspace*, e-mail message to the CYBERIA-L listserv, Jan. 16, 1995 (copy on file with author).

7. The author presumes the reader's general familiarity with cyberspace, and Part II serves only to highlight the international dimensions of these computer networks. For the novice, a recommended introduction to cyberspace is JOSHUA EDDINGS, HOW THE INTERNET WORKS (1994).

8. This Note presumes that all defendants in hypothetical tort and contract litigation are individuals, so that acts of state and public international law are beyond the Note's scope.

9. Willard Uncapher, *Trouble in Cyberspace: Civil Liberties at Peril in the Information Age*, HUMANIST, Sept.-Oct. 1991, at 5, 9 (quoting CYBERSPACE: FIRST STEPS (Michael Benedikt ed., 1991)); SCI. AMER., Sept., 1991 (The September issue

HeinOnline -- 29 Vand. J. Transnat'l L. 78 1996

Global networks interconnect "users locally, regionally, and globally for business, research, education, and social interaction."[10] Just as one uses the blue mailbox at the corner,[11] one can now send a letter or file nearly instantaneously to another user—perhaps thousands of miles away—by way of electronic mail (e-mail).[12] Like cork boards and thumbtacks, which pass information from one person to many, electronic bulletin board systems (BBSs) and "newsgroups" allow a user to "post" a message and disseminate it across the globe to be read by anyone with access to the group.[13] Bulletin boards have literally millions of subscribers. Teleconferencing and the advent of multimedia allow "real-time" interaction among parties sometimes continents apart.[14] Users can acquire files and computer programs from computers half a world away using the File Transfer Protocol (FTP).[15] Finally, the World Wide Web (the Web), which introduced a user-friendly, full-color graphical interface, has recently become tremendously popular.[16]

A. *Cyberspace as the Global Village*

The earth is now an interconnected planet that some have termed a "global village."[17] Cyberspace has a remarkable capacity

---

is dedicated to discussing cyberspace and its impact on future global communications.).

10. Harasim, *supra* note 2, at 5-6. *See generally* David J. Loundy, *E-Law: Computer Information Systems and System Operator Liability*, 3 ALB. L. J. SCI. & TECH. 79 (1993) (providing a comprehensive introduction to both the technology and legal issues) (*E-law* version 2.0 is available at ftp://infolib.murdoch.edu.au/pub/subj/law/jnl/elaw/refereed/loundy.txt).

11. Communication sent via the U.S. Postal Service is termed "snail mail" by Internet users.

12. *See generally* Harasim, *supra* note 2, at 6.

13. UseNet is an international message-exchange network with almost 10,000 different "newsgroups" ranging from "misc.legal" to "alt.sex.bestiality." *See* Dan L. Burk, *Patents in Cyberspace*, 68 TUL. L. REV. 1, 8 (1993) [hereinafter Burk, *Patents*].

14. Several companies now offer software products that provide a method of voice telecommunication. By using the Internet, these companies avoid long-distance charges. Thus, live voice conferencing is now available through cyberspace. *See* Kevin Savetz, *Net as Phone: Kiss Long Distance Charges Good-Bye*, INTERNET WORLD, July 1995, at 67, 67.

15. *See* EDDINGS, *supra* note 7, at 69-73 (explaining FTP and "anonymous FTP," which allow remote log-in and downloading of files).

16. *See id.* at 129, 141-43; *see generally* J. ONLINE L., *published at* http://www.law.cornell.edu/jol/jol.table.html (a journal of law in cyberspace published on the World Wide Web). The Web is a segment of the Internet that organizes information into a series of menu pages linked to other pages. *See* EDDINGS, *supra* note 7, at 41-43.

17. University of Toronto professor Marshall McLuhan coined the term "global village" in the 1960s. *See also* Mitchell Kapor and John P. Barlow, *Across*

HeinOnline -- 29 Vand. J. Transnat'l L. 79 1996

for unifying the world. Understanding the legal implications of this interconnectivity requires some appreciation for the global architecture of cyberspace. The main global networks include Internet, BITNET, UseNet, FidoNet, and AT&T mail.[18] For shorthand, many people speak simply of the Internet (the net), the "meganetwork."[19] Essentially, "[t]he Internet is a network of networks; each individual network is administrated, maintained, and paid for separately by individual educational institutions and other organizations."[20]

While the United States government subsidizes the Internet in part, it has no real central management or ownership.[21] Professor Dan L. Burk provides this architectural overview:

> Information flow on the Internet resembles that in a river, highway, or circulatory system: local networks funnel information traffic into larger regional networks, which in turn are connected to high capacity "backbone" linkages. This network of computers, its electronic traffic enabled and directed by host computers at each interconnected site, links literally millions of users in dozens of countries all over the world.[22]

The crucial point is that the Internet, although globally accessible, is not a single network: it is a *network of networks*. This fact has important consequences for the choice of law issues to be considered *infra*.

In summary, cyberspace is the first communications medium that allows remote users to readily access information and equipment across the world.[23] According to estimates, the

---

the Electronic Frontier, July 10, 1990, *available at* http://www/eff/org/pub/EFF/electronic_frontier.eff ("Whatever it is eventually called, it is the homeland of the Information Age, the place where the future is destined to dwell.").

18. Harasim, *supra* note 2, at 6.

19. *Id.*

20. EDDINGS, *supra* note 7, at 13.

21. Rex S. Heinke & Heather D. Rafter, *Rough Justice in Cyberspace: Liability on the Electronic Frontier*, COMPUTER LAW., July 1994, at 1, 1, *available in* Westlaw, CLW Database.

22. Dan L. Burk, Transborder Intellectual Property Issues on the Electronic Frontier 2 (1994) (unpublished manuscript, on file with author) [hereinafter Burk, Transborder IP Issues]. Major research networks exist in many nations. In Great Britain, there is the Joint Academic Network, Starlink, and UKnet; in Germany, DFN and Dnetl; in France, FNET, ARISTOTE, and REUNIRI; in Canada, CDNnet; in Japan, JUNET; and in Korea, SDN. *See* Burk, *Patents*, *supra* note 13, at 17-20 (detailing the interconnectivity of worldwide networks). *See generally* EDDINGS, *supra* note 7, at 14-15 (graphical depiction of "The Global Internet").

23. Burk, *Patents*, *supra* note 13, at 3 (noting that an authorized user anywhere in the world can control computers and even electron microscopes remotely).

HeinOnline -- 29 Vand. J. Transnat'l L. 80 1996

Internet unites more than 20 million users[24] in 146 countries.[25] Electronic census takers expect this population to double each year in the foreseeable future.[26] Anyone with a computer terminal, modem, rudimentary knowledge, and access to the Internet can download information from, communicate thoughts to, and virtually visit anywhere else in the world.[27] The advent of global computer networks has made the global village a reality.

B. *Cyberspace and Territoriality*

> "The trouble with cyberspace, lawyers say, is that there's no 'there' there."[28]

Like any human endeavor, the Internet presents seemingly endless legal issues. The law has not yet met this technology with a coherent doctrine that takes into account the transnational dimensions of global computer networks.[29] Traditional notions of jurisdiction are outdated in a world divided not into nations, states, and provinces but networks, domains, and hosts.[30] Cyberspace confounds the conventional law of territorial jurisdiction and national borders.[31] In cyberspace, it does not

---

24. Heinke & Rafter, *supra* note 21, at 1. *See also* message from Dan L. Burk, *Subj: Worldwide Internet Growth*, November 5, 1994, to the CPSR LISTSERV (reporting international Internet statistics detailing 21% growth in the third quarter of 1994) (copy on file with author).

25. Rosaland Resnick, *Cybertort: The New Era*, NAT'L L.J., July 18, 1994, at A1.

26. Stephen Steinberg, *Travels on the Net*, TECH. REV., July 1994, at 20, 22.

27. One organization attempts to keep statistics regarding worldwide Internet participation. The data is available on the Web at http://www.nw.com. The survey tracks 24 nations. *Id.*

28. Resnick, *supra* note 25, at A1.

29. *See* Michael Kirby, *Legal Aspects of Transborder Data Flows*, 11 COMPUTER/L.J. 233, 233 (1991) ("National laws are developed which are ineffective to deal with multinational issues.").

30. Many authors have noted this phenomenon, though few have written on its legal implications. For prior treatments of choice of law in cyberspace see Linda O. Smiddy, *Choosing the Law and Forum for the Litigation of Disputes*, in TOWARD A LAW OF GLOBAL COMMUNICATIONS NETWORKS 299 (Anne W. Branscomb ed., 1986) (addressing, to a limited extent, the international choice of law implications of tort and contract actions, but focusing more on the implications for jurisdiction when nations themselves are parties); John D. Faucher, Comment, *Let the Chips Fall Where They May: Choice of Law in Computer Bulletin Board Defamation Cases*, 26 U.C. DAVIS L. REV. 1045 (1993) (considering United States conflict of laws principles).

31. *See* David Johnson, *Addressing the Daunting New Problems that Will Arise with Universal Communication*, COMPUTERGRAM, Reuters Info. Svcs. (June 23, 1994), *available in* Westlaw, CGRAM database ("Jurisdiction based on place can no longer be viable.").

HeinOnline -- 29 Vand. J. Transnat'l L. 81 1996

matter at all whether a site lies in one country or another because the networked world is not organized in such a fashion. Remote log-on,[32] telnet,[33] gopher,[34] and the World Wide Web all render political borders obsolete, to some extent.[35] For example, hypertext[36] on the World Wide Web enables users to "visit" one location (called a page or a site), where they are then presented with an opportunity to visit any of a number of other locations—in any of a number of other countries.[37] Frequently, users are unaware that they have even "crossed" a political border in the course of their virtual travels.[38]

Well-known jurisdictional doctrines such as "purposeful availment" lose meaning in cyberspace.[39] While sovereignty has traditionally been a function of territoriality,[40] the Internet is not conducive to this paradigm. Should cyberspace be stretched on a procrustean bed of conventional jurisdictional and choice of law paradigms that are wedded to yesterday's world of easily drawn and easily demarcated political borders? The networked world is different and requires a different approach.

---

32. *See* EDDINGS, *supra* note 7, at 3.

33. Telnet allows users to "log on" to a remote host computer as if they were sitting in front of that computer. *See id.* at 19.

34. Gopher is a menu-based way to navigate the Internet by allowing the users to quickly access information elsewhere and download that information to their own computers. *See* EDDINGS, *supra* note 7, at 131.

35. *See e.g.*, Burk, Transborder IP Issues, *supra* note 22, at 3 ("Computers on the Internet can be linked together to simultaneously process different parts of complex problems, creating in effect a giant supercomputer. These features of the network make distance and political borders invisible to users of the electronic universe. . . .").

36. Hypertext describes a document with nonlinear links (or connections) to other parts of the document or other documents. One can jump around in hypertext to explore other documents at one's own pace. EDDINGS, *supra* note 7, at 141.

37. A Web site at the University of Kansas allows a user to "spin" a graphical roulette wheel and then be "transported" to the site in any state or country on which the pointer lands. Available on the Web at http://kuhttp.cc.ukans.edu/cwis/organizations/kucia/uroulette/uroulette.html.

Most World Wide Web addresses contain no indication of the nationality of the site. How can one be fairly said to have accepted jurisdiction from a nation that one is unaware of having entered?

38. *See, e.g.*, Danny Hillis, *Kay & Hillis*, WIRED, Jan. 1994, at 103 ("The point is that pretty soon you'll have no more idea of what computer you are using than you have of where your electricity is generated when you turn on the light.").

39. When people "purposefully [avail themselves] of the privilege of conducting activities within the forum State," they are effectively "on notice" that they are subject to being sued there. *See* World-Wide Volkswagen v. Woodson, 444 U.S. 286, 297 (1980) (asking whether a defendant can "reasonably anticipate being haled into court" in a given jurisdiction).

40. Burk, Transborder IP Issues, *supra* note 22, at 3 ("Law is in general territorial, extending no farther than the borders of the jurisdiction whose government has enacted the law.").

HeinOnline -- 29 Vand. J. Transnat'l L. 82 1996

III. OBLIGATIONS IN TRANSNATIONAL CYBERSPACE

Before analyzing the choice of law implications of a transnational cyberspace, one must recognize the possibility of disputes regarding on-line conduct and net-related activity. Contracts and torts—the law of obligations—provide the best analytical framework for a choice of law discussion.[41]

Cyberspace presents a unique medium for the commission of inter- and multi-state torts. Professor Trotter Hardy notes that cyberspace makes it dramatically easier for citizens in one nation to become acquainted with citizens of other nations.[42] Additionally, the low cost of cyberspace communications makes wide-scale distribution of wrongful communications possible.[43] Thus, "the issue of international torts is likely to be much more significant in cyberspace than it has been to date in real space."[44]

The capacity for litigation arising from behavior on the Internet is essentially a function of the *quantity* of human interaction, which will likely increase. Moreover, the caution ordinarily exercised in face-to-face real space tends to recede in the world of anonymity and solitude that one finds in front of computer terminals.[45] The temptation to engage in otherwise reckless behavior increases the probability of "cybertorts."

Defamation[46] is typical of tortious conduct in the realm of transnational cyberspace.[47] Cyber-defamation can occur in any

---

41. Johnson and Marks list a number of situations that, for the purposes of this Note, present the possibility for legal dispute in cyberspace. Both over- and under-inclusive, this list provides an excellent overview of the sorts of disputes that may give rise to choice of law issues in litigation. David R. Johnson & Kevin A. Marks, *Mapping Electronic Data Communications onto Existing Legal Metaphors: Should We Let Our Conscience (and Our Contracts) Be Our Guide?*, 38 VILL. L. REV. 487, 490-91 (1993).

42. I. Trotter Hardy, *The Proper Legal Regime for "Cyberspace,"* 55 U. PITT. L. REV. 993, 1053 (1994).

43. *Id.* at 1052.

44. *Id.*

45. *See, e.g.*, Devin Shawn Edwards, Jurisdiction in Cyberspace (unpublished manuscript, on file with the author) (describing an Internet Relay Chat (IRC) session in which a young college woman engaged in a sexually explicit private conversation with another remote user). Usenet newsgroups such as "alt.tasteless.jokes" (frequently sexist, racist, and scatological humor) demonstrate this phenomenon. Inhibitions about posting such potentially offensive matter are dramatically lower in an anonymous cyberspace than in real space.

46. Defamation is a communication that tends to harm the reputation of another so "as to lower [the individual] in the estimation of the community or to deter third persons from associating or dealing with [the individual]." RESTATEMENT (SECOND) OF TORTS §§ 558-59 (1976).

47. Heinke & Rafter, *supra* note 21, at nn.9-14 (collecting cyber-defamation cases).

HeinOnline -- 29 Vand. J. Transnat'l L. 83 1996

number of forms—a message posted to a newsgroup or BBS, a file available via FTP or a database, or a note in e-mail.[48] The following hypothetical case exemplifies the transnational flavor of a dispute in cyberspace: X could defame Y in a Usenet newsgroup moderated by a Canadian whose data is stored on a U.S. computer. The communication might be made while X was in Great Britain accessing a French computer and Y was in Australia accessing a Norwegian computer.[49]

Business-related cybertorts could become common. For example, a case has arisen in which a Canadian company tampered with computer tapes stored in a U.S. firm's computers, effectively rendering the tapes useless.[50] Similarly, in 1988 a computer virus infected commercially available computer programs, leading to international concern for the integrity of software.[51] The infected software was copied from a computer in Canada, transferred to commercial software in Ohio, and injured the Aldus Company in Seattle, Washington.[52]

Many nations regulate and criminalize computer crime,[53] but such conduct is also tortious if viewed as conversion, trespass, or negligence. Various offenses collectively known as hacking, such as unauthorized access to a computer system, unauthorized access to particular computer-based information, and trafficking in stolen passwords or credit card account numbers,[54] might all be actionable in tort.

The computer virus poses an increasing threat to cyberspace. A virus is an intentionally created destructive computer program that can spread either through networked computers or by

---

48. *See generally* Kimberly Richards, *Defamation Via Modern Communication: Can Countries Preserve Their Traditional Policies?*, 3 TRANSNAT'L L. 613 (1990).

49. Cyber-defamation cases have already been litigated. *See, e.g.*, Hardy, *supra* note 42, at 1052 (citing Rindos v. Hardwick, unreported judgment 940164 (Sup. Ct. West. Austr. Mar. 31, 1994) (defamatory message circulated to approximately 23,000 members of a cyberspace discussion group)).

50. Anne W. Branscomb, *Jurisdictional Quandaries in Global Communications Networks*, *in* TOWARD A LAW OF GLOBAL COMMUNICATIONS NETWORKS 92 (Anne W. Branscomb ed., 1986) (discussing TRANSNAT'L DATA REP., Feb. 1987, at 7).

51. *See* Branscomb, *supra* note 50, at 94.

52. *Id.*

53. *See generally* Robert J. Sciglimpaglia, Jr., *Computer Hacking: A Global Offense*, 3 PACE Y.B. INT'L L. 199 (1991) (outlining criminal laws for computer-related activities in Canada, the United States, and Great Britain).

54. Conversion often occurs with credit card numbers. Faucher, *supra* note 30, at 1078 n.16.

HeinOnline -- 29 Vand. J. Transnat'l L. 84 1996

sharing disks among computers.[55] The capacity to do substantial damage to another's proprietary information is obvious.[56]

An example of a computer crime with potential tort consequences is the arrest of three Australians in 1990 on charges of tampering with computers in the United States and Australia via the Internet.[57] Similarly, a Cornell University graduate student unleashed a "worm"[58] that invaded thousands of computers across the United States.[59] The student was convicted[60] under the Computer Fraud and Abuse Act,[61] but not before he paralyzed and shut down a number of major computer systems, causing millions of dollars in losses.[62] Although probably "judgment-proof," Morris' actions exposed him to considerable tort liability, even though "his intention was not to disable systems."[63] In one frightening incident, hackers accessed the records of an intensive-care ward in a hospital in Los Angeles, California and doubled all patients' doses of medication.[64] The potential tort liability for such activities is staggering.[65]

---

55. *See, e.g.*, Dawn Stover, *Viruses, Worms, Trojans and Bombs: Computer "Infections,"* POPULAR SCIENCE, Sept. 1989, at 59. *See also* EDDINGS, *supra* note 7, at 175-81.

56. For a transnational perspective on computer viruses, see Chuck Sudetic, *Bulgarians Linked to Computer Virus*, N.Y. TIMES, Dec. 21, 1990, at 9. Sudetic reports that during the late 1980s, Bulgaria was the focal point for the transmission of computer viruses. *Id.*

57. Sciglimpaglia, *supra* note 53, at 201-03.

58. A worm is a computer instruction or hidden program wrongfully inserted into legitimate software. The worm may reproduce itself, infect multiple programs, and cause damage to other software. EDDINGS, *supra* note 7, at 180-81.

59. *Id.* at 181.

60. United States v. Morris, No. 90-1336 (D.C.N.Y. 1990), *aff'd* 928 F.2d 504 (2d Cir. 1991).

61. 18 U.S.C. § 1030 (1988). The Act prohibits unauthorized access to computers, unlawful computer transmissions, and makes it illegal to damage computer networks and data. The Act also gives injured parties a civil cause of action for damages or injunctive relief.

62. The worm harmed a significant number of businesses, universities, and even computers at the National Aeronautics and Space Administration (NASA). One author estimates the damage at $97 million. Kirby, *supra* note 29, at 239.

63. Mr. Morris did not attempt to alert anyone until after his worm had gone out of control. *Id.*

64. J. FRASER MANN, COMPUTER TECHNOLOGY AND THE LAW IN CANADA 158-59 (1987). Fortunately, the error was caught before any damage was done.

65. These activities, like many others treated in this discussion, are illegal under United States and foreign law. *See, e.g.*, 18 U.S.C. §1030(a)(5)(B) (1994) (prohibiting the alteration of medical records in a section entitled "Fraud and related activity in connection with computers"). The focus of this Note, however, is the civil realm.

HeinOnline -- 29 Vand. J. Transnat'l L. 85 1996

Other wrongs that may be committed in cyberspace include the dissemination of hate speech and threats.[66] In one situation, a computer bulletin board operated by the Aryan Nations Net in the United States promoted white supremacy and maintained a list of targets for extermination.[67] These messages were illegal in Canada, which prohibits the circulation of racially offensive literature.[68] While Canadian nationals could access the material, only through the cooperation of U.S. authorities could Canadian courts have obtained extradition orders or jurisdiction.

Beyond torts, the myriad contractual arrangements made through and in connection with the net have striking legal implications. Contracts can be formed, performed, and broken in cyberspace.[69] Offer and acceptance occurs in e-mail. On-line catalogs and order forms are readily found on the Web.[70] Disputes will certainly arise regarding the formation, performance, and payment of contractual obligations.

The following message culled from the "misc.legal" UseNet newsgroup presents an example of just such a situation:

> #69979
> From: [author's name omitted]
> Subject: Internet deals gone awry: MAIL FRAUD or SMALL CLAIMS COURT
> Date: Mon, 13 Feb 1995 15:07:29 GMT
>
> When Internet deals go bad, what can be done to fight back? (One of you lawyers send me email, I think I have a case.)
>
> Recently I made a "deal" with someone in another state. I thought I was getting a motherboard populated with 16MB of SIMMs, but after giving the Federal Express COD delivery person a money order for about $600, I opened the box to find a broken board with no memory.
>
> I called the Post Office and tried to cancel the Money Order: no such luck. I called Federal Express and tried to stop the delivery of the money order: no such luck.
>
> Now what can I do? (Legally, that is. . . .)

---

66. In one prominent case, officials charged a University of Michigan student with a federal crime for describing the torture and rape of a character named after a female classmate in a message posted to the Usenet newsgroup "alt.sex.stories." Robert Davis, *Graphic "Cyber-Threats" Land Student in Court*, USA TODAY, Feb. 10, 1995, at 3A. For a comprehensive treatment of this case, see http://www/eff/org/pub/Legal/Cases/Baker_UMich_case/.

67. *See* Branscomb, *supra* note 50, at 90.

68. *Id.*

69. For example, a recent newspaper article noted that a British company aims to begin "the first formal electronic stock exchange on the Internet." Richard L. Hudson, *British Start-Up to Trade Stocks on the Internet*, WALL ST. J., Feb. 3, 1995, at A7A.

70. For just a sampling of the shopping available on the World Wide Web, see http://www.yahoo.com and search for "Shopping." Sites include the Internet Shopping Network, the Internet Shopping Page, and the All-Internet Shopping Directory.

HeinOnline -- 29 Vand. J. Transnat'l L. 86 1996

> Sue him in Small Claims court... in his state? [I]n my state?
> Report it as Mail Fraud (but it was FedEx, not US Postal Service. . . .)
> Or am I flat-out scrod [sic]?
> Has any legal precedent been set yet in this area?
> Have any cases like this been fought and won? Lost?
> How do you fight brick-in-the-mail Internet fraud?
> [author's name omitted]

IV. A UNIFIED APPROACH TO CHOICE OF LAW IN TRANSNATIONAL CYBERSPACE

A. *Introduction*

One of the thorniest issues in a law of cyberspace is in the domain of private international law.[71] Whose laws apply when litigation arises from activity in a transnational cyberspace? *Private* international law—or conflict of laws[72]—is concerned exclusively with private disputes among individuals (or analogous entities like corporations), while *public* international law addresses issues such as state recognition, treaties, and war.[73] The multistate nature of cyberspace reveals the importance of conflict of laws questions in international civil litigation arising from Internet participation. Choice of law is "particularly difficult in the case of international computer networks where, because of dispersed location and rapid movement of data, and geographically dispersed data processing activities, several connecting factors could occur in a complex manner involving elements of legal novelty."[74]

1. A Note on Jurisdiction

Jurisdiction concerns the ability of a particular forum to *hear* a particular case (adjudicative jurisdiction) or *legislate* about a

---

71. This term originated in JOSEPH STORY, COMMENTARIES ON THE CONFLICT OF LAWS, FOREIGN AND DOMESTIC 9 (1st ed. 1834) (It is "fitly denominated private international law, since it is chiefly seen and felt in its application to the common business of private persons, and rarely rises to the dignity of national negotiations, or national controversies.").

72. The terms "private international law" and "conflict of laws" are roughly synonymous. BLACK'S LAW DICTIONARY 1196 (6th ed. 1990).

73. ANDREAS F. LOWENFELD, CONFLICT OF LAWS 853-54 (1986).

74. Burk, *Patents*, *supra* note 13, at 5 (quoting Organization for Economic Cooperation and Development, explanatory memorandum, *in* GUIDELINES ON THE PROTECTION OF PRIVACY AND TRANSBORDER DATA FLOWS OF PERSONAL DATA 13, 36 (1980)).

HeinOnline -- 29 Vand. J. Transnat'l L. 87 1996

particular matter (legislative jurisdiction). Personal jurisdiction[75] may lie wherever the defendant's conduct in connection with the forum indicates that the defendant reasonably anticipated being subject to the court there.[76] Unless otherwise noted, jurisdictional competence shall be assumed[77] because cyberspace "makes contact" with literally hundreds of nations, and cyber-defendants have acquired at least a virtual presence in these jurisdictions. Because material is accessible universally, jurisdiction might lie almost anywhere.

Conversely, choice of law considers *whose* law a state or nation with jurisdiction is to apply to the action. For example, in a defamation action, a plaintiff might sue (i.e., have jurisdiction) in any state in which the plaintiff can prove that someone received the defamatory message.[78] However, that forum's law[79] will not necessarily govern the suit.[80] It is that forum's choice of law rules that direct the court to the applicable law.

2. Why Develop a Choice of Law Regime?

The main objectives of choice of law are (1) to achieve "maximum fairness to the parties" and (2) to achieve "effective implementation and coordination of state or country policies."[81]

---

75. Personal jurisdiction is "the power of a court over the person of a defendant" and refers to the ability of a particular jurisdiction to sanction a particular defendant. BLACK'S LAW DICTIONARY 1144 (6th ed. 1990). Other authors have studied personal jurisdiction in cyberspace, but that discussion is beyond the scope of this Note. *See, e.g.*, Richard Zembek, Comment, *Jurisdiction and the Internet: Fundamental Fairness in the Networked World of Cyberspace*, 6.2 ALB. L.J. SCI. & TECH. (forthcoming Spring 1996); Edwards, *supra* note 45.

76. George A. Zaphiriou, *Basis of the Conflict of Laws: Fairness and Effectiveness*, 10 GEO. MASON U. L. REV. 301, 303-04 (1988) (citing World-Wide Volkswagen v. Woodson, 444 U.S. 286, 297 (1980) (asking whether a defendant can "reasonably anticipate being haled into court there.")).

77. It is possible that some nations' courts would decline jurisdiction on *forum non conveniens* grounds, but that doctrine is beyond the scope of this Note. *Forum non conveniens* is the discretionary power of a court to decline jurisdiction if justice would be better served were the case to be heard in a different forum. BLACK'S LAW DICTIONARY 655 (6th ed. 1990).

78. *See, e.g.*, Keeton v. Hustler Magazine, 465 U.S. 770 (1984) (finding sufficient contacts to support jurisdiction where defendant had sold less than one percent of its magazines). In *Keeton*, the plaintiff was a resident of New York suing an Ohio corporation with its principal place of business in California. *Id.* *See also* Faucher, *supra* note 30, at 1049 (suggesting that the victim of libel carried on computer bulletin boards may sue in any state in which the message was received).

79. The law of the forum state is termed *lex fori*. BLACK'S LAW DICTIONARY 910 (6th ed. 1990).

80. Faucher, *supra* note 30, at 1049.

81. *See, e.g.*, Zaphiriou, *supra* note 76, at 303.

HeinOnline -- 29 Vand. J. Transnat'l L. 88 1996

The *Restatement (Second) of Conflict of Laws* highlights these principles in its opening section:

> § 1. Reason for the Rules of Conflict of Laws
>
> The world is composed of territorial states having separate and differing systems of law. Events and transactions occur, and issues arise, that may have a significant relationship to more than one state, making necessary a special body of rules and methods for their ordering and resolution.

A consistent choice of law methodology achieves a just and uniform application of law.[82] One author notes three consequences of the absence of a coherent choice of law regime:[83] (1) forum shopping, which leads to the inconsistent application of law and inconsistent results, especially in the international context;[84] (2) diminished predictability due to the difficulty in ascertaining what law will apply, particularly in novel situations such as those occurring in cyberspace; and (3) reduced deterrence because uncertainty as to the applicable law leads to inefficient risk-taking.[85]

3. The Nexus Requirement: Which Cyber-Disputes Require a New Choice of Law Regime?

The purpose behind the formulation of a new conflicts regime for cyberspace is to resolve those tricky choice of law questions that arise in this brave new world. But not all disputes that involve cyberspace call for law chosen by this new regime. As Professor Hardy has noted, "Some cyberspace issues seem wholly unremarkable: it is evident to any legal eye that they are readily governed by the same rules applicable to other forms of communication."[86] Just as Hardy asks, "What makes a legal issue new?",[87] one must ask, "When is the choice of law question for a particular cyber-dispute appropriately determined by this new model?"

---

82. *See* RESTATEMENT (SECOND) OF CONFLICT OF LAWS § 6 cmt. d (1971) ("Probably the most important function of choice-of-law rules is to make the interstate and international systems work well. Choice-of-law rules, among other things, should seek to further harmonious relations between states and to facilitate commercial intercourse between them.").

83. Helen Shin, *Oh, I Have Slipped the Surly Bonds of Earth: Multinational Space Stations and Choice of Law*, 78 CALIF. L. REV. 1375, 1382-84 (1990).

84. Forum shopping enables a plaintiff to achieve more favorable results by choosing to sue in one forum and receiving the benefit of that forum's substantive law. BLACK'S LAW DICTIONARY 655 (6th ed. 1990).

85. Shin, *supra* note 83, at 1383-84.

86. Hardy, *supra* note 42, at 998.

87. *Id.* at 996.

HeinOnline -- 29 Vand. J. Transnat'l L. 89 1996

In the broadest, most unsophisticated sense, the dispute must be "internet-related" to be governed by this new model. But that does not go far enough. The law of property asks whether an interest or right "touches and concerns" the land so as to run with the land.[88] Simply "touching and concerning" cyberspace, however, is not a sufficient reason to invoke an entirely new choice of law methodology. There must be something about the dispute that evokes or typifies those failings of traditional choice of law regimes (i.e., some reason why old methods are not helpful).[89]

Admiralty law might help draw that line between a new cyber-dispute and a dispute that just happens to involve cyberspace. To be considered a maritime tort, so as to invoke the jurisdiction of admiralty courts and the choice of maritime law for the action, the tort must have a "significant connection to traditional maritime activity" (i.e., a "maritime nexus").[90] In the past, "[e]very species of tort, however occurring, and whether on board a vessel or not, if upon the high seas or navigable waters, [was] of admiralty cognizance."[91] Even if the tort bore no relationship to navigation or maritime commerce, it was deemed a maritime tort.[92]

However, in *Executive Jet Aviation, Inc. v. City of Cleveland*,[93] a case involving a plane crash into Lake Erie, the U.S. Supreme Court wrote:

> [T]he mere fact that the alleged wrong "occurs" or "is located" on or over navigable waters—whatever that means in an aviation context—is not of itself sufficient to turn an airplane negligence case into a "maritime tort." It is far more consistent with the history and purpose of admiralty to require also that the wrong bear a significant relationship to traditional maritime activity. We hold that unless such a relationship exists, claims arising from airplane accidents are not cognizable in admiralty in the absence of legislation to the contrary.[94]

Although the U.S. Supreme Court has made almost no attempt to define "traditional maritime activity" or "a significant connection to maritime commerce," the Fifth Circuit Court of

---

88. JON W. BRUCE ET AL., CASES AND MATERIALS ON MODERN PROPERTY LAW 419 (2d ed. 1989) ("'[T]ouch and concern' requires that the covenant directly relate to the land in some way and not concern merely a collateral matter of a personal nature.").

89. For a discussion of the failings of conventional approaches, see *infra* Part IV.B.

90. 1 STEVEN F. FRIEDELL, BENEDICT ON ADMIRALTY 11-1 (7th ed. 1992).

91. *Id.* at 11-2 (quoting The Plymouth, 70 U.S. (3 Wall.) 20, 36 (1865)).

92. FRIEDELL, *supra* note 90, at 11-2, 11-3.

93. 409 U.S. 249, 268 (1973).

94. Likewise, in *Crosson v. Vance* the Fourth Circuit held there to be no admiralty jurisdiction over a water-skiing accident. 484 F.2d 840 (4th Cir. 1973).

HeinOnline -- 29 Vand. J. Transnat'l L. 90 1996

Appeals established a test for this nexus requirement in *Kelly v. Smith*.[95] Four factors are considered to find a "maritime nexus": (1) the functions and roles of the parties, (2) the types of vehicles and instrumentalities involved, (3) the causation and type of injury, and (4) traditional concepts of the role of admiralty law.[96]

These decisions indicate that when both parties are essentially land-based and the same behavior would have given rise to tortious responsibility on land, courts tend to deny admiralty jurisdiction.[97] Thus, "[c]laims by painters or automobile drivers who fell from a bridge fail the nexus test, [and a] products liability suit by a passenger on a pleasure craft against a manufacturer of a gun that misfired while in the boat is non-maritime."[98]

Likewise, only contracts that relate "to ships and vessels, masters and mariners, as the agents of commerce" qualify for admiralty jurisdiction over contract actions.[99] Generally, the only contracts in the purview of admiralty law are those relating to (1) ships used in commerce or navigation on navigable waters, (2) the transport of items across the water, or (3) employment for maritime services.[100] The key principle is that it does not matter whether the contract is made or performed on land or water; what is relevant is the "admiralty nexus."[101]

To return to Professor Hardy's point, one should not be quick to treat all disputes that in some way—no matter how attenuated—touch and concern cyberspace as a new species of dispute. Not every dispute need be controlled by the new choice of law regime. For example, if User X in the United States writes a letter to the editor of *The New York Times* in which British User Y is defamed regarding Y's management of a bulletin board, no "cyber-case" has arisen; it is simply a real-space defamation suit and real-space conflicts rules can handle the choice of law. Likewise, an automobile accident between two people who happen to have Internet accounts is not a cyber-dispute and not relevant

---

95. 485 F.2d 520 (5th Cir. 1973). Several other circuits have adopted the Kelly formulation. FRIEDELL, *supra* note 90, at 11-9 n.29.

96. FRIEDELL, *supra* note 90, at 11-10. *See also* Molett v. Penrod Drilling Co., 826 F.2d 1419, 1426 (5th Cir. 1987) (adding other factors to the *Kelly* test: (1) the impact of the event on maritime shipping and commerce, (2) the desirability of a uniform national rule to apply to such matters, and (3) the need for admiralty "expertise" in the trial and decision of the case).

97. FRIEDELL, *supra* note 90, at 11-13.

98. *Id.* at 11-14, 11-15 (citations omitted).

99. Kossick v. United Fruit Co., 365 U.S. 731, 736 (1961) ("The boundaries of admiralty jurisdiction over contracts . . . being conceptual rather than spatial have always been difficult to draw.").

100. FRIEDELL, *supra* note 90, at 12-4.

101. *Id.*

HeinOnline -- 29 Vand. J. Transnat'l L. 91 1996

to application of the new model. The torts have occurred in real space and the current choice of law processes are sufficient to deal with these scenarios.[102]

In sum, just as admiralty requires a "maritime flavor," so too does the new choice of law model require a "cyberspace flavor" to govern the choice of law for a particular action. The difficulties in line-drawing (illustrated by the *Kelly v. Smith* multi-factor test) between maritime and nonmaritime torts applies with equal force in cyberspace. Perhaps the expertise rationale for admiralty jurisdiction articulated in *Molett v. Penrod Drilling Co.*[103] should emerge as the most salient factor in deciding whether an action is a cyber-tort or simply a generic tort. In *Molett*, the court found admiralty jurisdiction especially proper when the action should be heard in a court competent to exercise "admiralty expertise." In the ever-changing technical and legal environments of cyberspace, users will increasingly depend upon expertise in applying law and customs. The law of the forum that is best able to grasp those issues might be the best choice. Indeed, these considerations suggest the development of a substantive legal regime not unlike admiralty or the Law Merchant, which this Note discusses in Part IV.C., or the creation of the "cyber-courts" advocated by some writers.[104] All references to cyber-disputes, torts, and contracts are, by definition, those disputes with the required nexus to cyberspace so as to justify invoking the new model.

B. *Why are Conventional Regimes Insufficient in Cyberspace?*

1. Choice of Law for Actions in Tort

Because no multinational agreement exists with regard to torts in cyberspace, courts seeking to choose law will resort to conventional choice of law principles. Traditional choice of law for torts has focused on two theories: (1) the *lex loci delicti* approach of the *Restatement of Conflict of Laws* (the First Restatement) and (2) the most significant relationship approach of the *Restatement (Second) of Conflict of Laws* (the Second Restatement).

---

102. It is also appropriate here to note that even true cyber-disputes that arise between two individuals subject to the same real-space jurisdiction's laws do not need to be included in the new choice of law model. It is probably fair to say that both parties could expect to be subject to the law of their "common ground."

103. 826 F.2d 1419, 1426 (5th Cir. 1987). *See supra* note 96.

104. *See infra* note 217 and accompanying text.

HeinOnline -- 29 Vand. J. Transnat'l L. 92 1996

a. *Lex Loci Delicti*

The First Restatement applies a simple choice of law rule that is almost mechanical in its operation—the rule of *lex loci delicti*, the law of the place of the wrong.[105] The place of the wrong is the state where "the last event necessary to make an actor liable" for an alleged tort takes place.[106] Some nations still follow the *lex loci delicti* approach.[107]

In transnational cyberspace, however, the place of the wrong might be any of the 145-plus nations that are on-line.[108] More accurately, there is no *lex loci delicti*.[109] The state of the last act is ordinarily the state where injury occurs.[110] If injury occurs in cyberspace, it can be said that the place of the wrong *is* cyberspace itself.[111] Because there is no single answer to this choice of law problem, the forum will likely apply its own law to the dispute.[112] This *lex fori* default rule, of course, encourages forum shopping.[113]

The traditional rule is an adequate one in real space because of its certainty and ease of application. But the numerous examples in Part III of this Note reveal that one cannot easily identify "where" events transpire on the Internet.[114] *Lex loci delicti*, therefore, is not a sound choice of law regime for cyberspace.[115]

---

105. *See generally* J.D. LEE & BARRY A. LINDAHL, MODERN TORT LAW: LIABILITY & LITIGATION § 13.03 (Rev. ed. 1994).

106. *Id.*

107. *See* Shin, *supra* note 83, at 1392-93.

108. Faucher, *supra* note 30, at 1056-57 n.69.

109. *See* Hamilton DeSaussure & P.P.C. Haanappel, *A Unified Multinational Approach to the Application of Tort and Contract Principles to Outer Space*, 6 SYRACUSE J. INT'L L. & COM. 1, 12 (1978) ("For outer space, there is no *lex loci delicti commissi*. Thus, this venerable rule, so generously applied in both common and civil law countries, is impossible to follow for space related torts.").

110. RESTATEMENT (SECOND) OF CONFLICT OF LAWS, ch. 7 introduction.

111. For example, many users employ pseudonyms on the Internet. Conceptually, if true anonymity exists and the pseudonymous character in cyberspace is defamed, is there any injury per se in real space? In this light, cyberspace creates the possibility for injury only in the virtual sense.

112. *See, e.g.*, Keeton v. Hustler Magazine, 465 U.S. 770 (1984) (applying New Hampshire law to nationwide libel).

113. *See supra* note 84 and accompanying text.

114. *See supra* notes 41-70 and accompanying text.

115. *See* Smiddy, *supra* note 30, at 305 (discussing unsuitability of *lex loci* approach in the transborder data flow context).

HeinOnline -- 29 Vand. J. Transnat'l L. 93 1996

b. Most Significant Relationship

The Second Restatement adopts a "most significant relationship" approach to choice of law.[116] Section 145(2) lists the variety of contacts to be considered: the place of injury, the place where the conduct causing the injury occurred, the place of domicile or residence of the parties, and the place where the parties' relationship is centered.[117] These geographically-oriented principles are confounded by cyberspace.

It is apparent that this approach does not afford much guidance to a court attempting to choose the appropriate law; some factors might weigh toward one forum, others to another.[118] The Second Restatement offers seven criteria to weigh these factors: (1) the needs of the interstate and international system, (2) the relevant policies of the forum, (3) the relevant policies of the interested states, (4) the protection of justified expectations, (5) the basic policies underlying the particular field of law, (6) certainty and uniformity of result, and (7) ease in determining and applying the law.[119] It is not clear, however, that these vague and boundless criteria add anything to the discussion.[120]

The Second Restatement's balancing approach to choice of law is certainly more flexible than the First Restatement's rule, but its utility in cyberspace suffers from the same debilitating weaknesses. How are the relevant factors to be considered in transnational cyberspace? More importantly, how are contacts such as the place of injury, place of conduct causing injury, and nationality determined in the networked world?

Comment (e) to Section 145 of the Second Restatement notes: "Situations do arise, however, where the place of injury will not play an important role in the selection of the state of the applicable law . . . such as in the case of multistate defamation, [where] injury has occurred in two or more states." Section 150 considers the vexing problem of choice of law for multistate defamation, but the result is the same—the court should balance and weigh, but ultimately pick the "fair" law. This case-by-case search for fairness, of course, sacrifices certainty and simplicity.

---

116. RESTATEMENT (SECOND) OF CONFLICT OF LAWS § 145 (1971).

117. *Id.* § 145(2).

118. Faucher, *supra* note 30, at 1063 ("The Restatement (Second) articulates another theory that is ill-suited to electronic torts . . . [and] offers courts little substantive guidance concerning choice-of-law decisions.").

119. RESTATEMENT (SECOND) OF CONFLICT OF LAWS §§ 6, 145 (1971).

120. *See, e.g.*, Faucher, *supra* note 30, at 1065 n.114 (citing Rene David, *The International Unification of Private Law*, *in* 2 INTERNATIONAL ENCYCLOPEDIA OF COMPARATIVE LAW 8 (1969) (The most significant relationship test "means nothing except, perhaps, that the answer is not ready at hand.").

HeinOnline -- 29 Vand. J. Transnat'l L. 94 1996

A new choice of law regime for transnational cyberspace should serve the twin goals of conflict of laws: certainty and fairness.[121]

2. Choice of Law for Contracts Without a Forum Selection Clause

Without a forum selection clause, the choice of law for a contractual dispute devolves upon the law of that nation most closely connected with the relevant contractual issue.[122] Scoles and Hay believe that "[c]hoice-of-law in contract, in the absence of a valid stipulation of the applicable law by the parties, is even more difficult than in tort."[123] Section 188 of the Second Restatement addresses choice of law for contractual disputes, absent a clause in the contract:

> § 188. Law Governing in Absence of Effective Choice by the Parties
> (1) The rights and duties of the parties with respect to an issue in contract are determined by the local law of the state which, with respect to that issue, has the most significant relation to the transaction and the parties. . . .
> (2) . . . [T]he contacts to be taken into account in . . . determin[ing] the law applicable to an issue include:
> (a) the place of contracting,
> (b) the place of negotiation,
> (c) the place of performance,
> (d) the location of the subject matter of the contract, and
> (e) the domicile, residence, nationality, place of incorporation and place of business of the parties.

Thus, if the dispute arises over the formation of the contract, presumably the law of the nation in which the contract was made would apply. Likewise, if the dispute is performance-related, the applicable law is that where performance was to occur.[124]

The obvious fallacy with Section 188's method for choosing law for contractual disputes is its continual reference to the "place" and "location" of certain events. This Note demonstrates that cyberspace confounds notions of place and location. Relying on the place of contracting, the place of performance, and similar factors leads to the inevitable conclusion that *place* or *location* mean little or nothing when it comes to cyberspace contracts. It is easy to envision a scenario in which a contract between a commercial Internet provider and a newsgroup manager is formed

---

121. Zaphiriou, *supra* note 76, at 302-03.
122. *See* RESTATEMENT (SECOND) OF CONFLICT OF LAWS § 188 (1971).
123. EUGENE SCOLES & PETER HAY, CONFLICT OF LAWS 678 (2d ed. 1992).
124. *See* Zaphiriou, *supra* note 76, at 316 ("Thus the place of negotiation, place of execution, place of performance of the contract, place of residence, or place of business of the parties are all connecting factors that will point" to the choice of forum.).

HeinOnline -- 29 Vand. J. Transnat'l L. 95 1996

in cyberspace, payment is electronically made in cyberspace, and performance is accomplished by services rendered in cyberspace.[125]

Other attempts to resolve choice of law questions in contractual disputes by reference to "close connections" are equally unhelpful. The 1980 Convention on the Law Applicable to Contractual Obligations (Rome Convention) is binding in several European countries with respect to contracts.[126] Article 4(1) requires that, in the absence of express or implied choice, a contract be "governed by the law of the country with which it is most closely connected."[127]

The multifactor tests of the Second Restatement and the Rome Convention do little to solve the choice of law problems in cyberspace, especially when the factors relied upon are geared toward and suited for a real-space world of easily drawn political boundaries.

C. *The Unified Approach to Choice of Law in Cyberspace*

Choice of law for disputes arising from transnational cyberspace will rarely be a simple matter. Conventional choice of law paradigms for tort actions—*lex loci delicti*[128] and the most significant relationship analysis[129]—break down on a globally interconnected information superhighway. The choice of law for contract disputes, in the absence of a forum selection clause, poses difficulties as well.[130] This Subsection will outline the author's proposed regime for a reconciled private international law of cyberspace.

Part II of this Note considers the transnational architecture of cyberspace.[131] Recalling the notion of cyberspace as a network of networks, there are two levels of "connectivity." At the first level, a user is connected to an "access provider." Each user in cyberspace must gain access to the Internet through an access

---

125. For example, in the well-known case *Cubby v. Compuserve*, 776 F.Supp. 135 (S.D.N.Y. 1991) (a cyber-defamation case), Compuserve had contracted with Cameron Communications, Inc. for Cameron to assume editorial control over the content of the information transmitted on the bulletin board. Cameron then subcontracted this work to another company, DFA. Heinke & Rafter, *supra* note 21, at 2-3.

126. Convention on the Law Applicable to Contractual Obligations, June 19, 1980, 1980 O.J. (L 266) 1. Contracts relating to wills, marriage, commercial paper, and certain other contracts are excluded. *Id.* art. I.

127. *Id.* art. 4(1).

128. *See supra* notes 105-15 and accompanying text.

129. *See supra* notes 116-21 and accompanying text.

130. *See supra* notes 69-70 and accompanying text.

131. *See supra* notes 28-40 and accompanying text.

HeinOnline -- 29 Vand. J. Transnat'l L. 96 1996

provider, which essentially serves as an "on-ramp" to the Information Superhighway. Today, commercial Internet providers such as Prodigy, the Microsoft Network, CompuServe, and America Online (AOL) provide a gateway to cyberspace.[132] All users might be considered "citizens" of their access provider. Thus, by reaching cyberspace through an access provider, it is possible to assign a "cyber-domicile" to each user. As a graduate student at Vanderbilt University, this Note's author is, in a sense, a cyber-domiciliary of the Vanderbilt network system; AOL users are cyber-domiciliaries of America Online, and so forth. This cyber-domicile concept can be used to resolve interuser choice of law problems.

At the second level, a user—through the access provider—becomes part of the larger cyberspace. This bi-level access scheme provides for three general species of cyberspatial disputes: 1) the dispute can arise between two users[133]who access cyberspace through either the same Internet provider[134] or providers in contractual privity with one another; 2) the dispute can arise between two users who access cyberspace through different Internet providers that are not in contractual privity with one another; and 3) the dispute can arise between a user in a cyberspatial capacity and a nonuser in real space.

1. Case 1: Resolving Choice of Law for Cyber-Disputes via Contracts

a. The Use of Forum Selection Clauses

Litigation will arise from contracts formed, performed, and broken in cyberspace. Because certainty in contractual obligations is of paramount importance to the parties, the practice of choosing the law by way of a forum selection clause in the contract has become the generally accepted means of handling choice of law for contractual disputes. A forum selection clause specifies which nation's law will apply.[135] Generally, a choice of law clause is joined with a choice of forum clause.[136] This

---

132. Internationally, Internet access provider competition is increasing rapidly. On November 28, 1995, American Online unveiled its service in a joint venture with Bertelsmann AG. Douglas Lavin, *American Online Enters a Crowded Europe*, WALL ST. J., Nov. 28, 1995, at B6.

133. Users include individuals as well as entities, such as corporations.

134. Typically, a contract governs the relationship between the individual and the provider.

135. *See* Smiddy, *supra* note 30, at 303.

136. Zaphiriou, *supra* note 76, at 315.

HeinOnline -- 29 Vand. J. Transnat'l L. 97 1996

ensures that the litigation forum will uphold the choice of law clause.[137] The choice of law contained in a contract encompasses that forum's substantive law and not its conflicts law.[138]

"[P]redictability is served, and party expectations are protected, by giving effect to the parties' own choice of the applicable law (party autonomy)."[139] This "party autonomy" objective is "especially prominent" when the contract is to be performed in several different jurisdictions.[140] Section 187 of the Second Restatement recognizes and encourages the practice of law and forum selection:

> § 187. Law of the State Chosen by the Parties
> (1) The law of the state chosen by the parties to govern their contractual rights and duties will be applied if the particular issue is one which the parties could have resolved by an explicit provision in their agreement directed to that issue.
> (2) The law of the state chosen by the parties to govern their contractual rights and duties will be applied, even if the particular issue is one which the parties could not have resolved by an explicit provision in their agreement directed to that issue, unless either
> (a) the chosen state has no substantial relationship to the parties or the transaction and there is no other reasonable basis for the parties' choice, or
> (b) application of the law of the chosen state would be contrary to a fundamental policy of a state which has a materially greater interest than the chosen state in the determination of the particular issue and which . . . would be the state of the applicable law in the absence of an effective choice of law by the parties.

The language of the Second Restatement and its interpretation by courts indicate that forum selection clauses are generally honored in the United States and abroad, so long as the choice is reasonable.[141] There are two important aspects of reasonableness as that term applies to contractual choice of law in cyberspace: (1) the requirement of "connecting factors" to the forum selected, and (2) the lack of a gross inequality of bargaining power, such that the choice appears to be oppressive to one party.

Traditionally, the parties' choice of the law of the place of contract formation, the place of performance, the domicile of

---

137. *Id.*

138. *See* RESTATEMENT (SECOND) OF CONFLICT OF LAWS § 187 cmt. h (1971).

139. SCOLES & HAY, *supra* note 123, at 657.

140. *Id.* at 657 n.3 (citing Lauritzen v. Larsen, 345 U.S. 571, 588 (1953) (seaman hired to sail to several countries)).

141. Zaphiriou, *supra* note 76, at 315; *see also* The Bremen v. Zapata Off-Shore Co., 407 U.S. 1 (1972) (authorizing the use of forum selection clauses); *cf.* U.C.C. § 1-105(1) (1994) ("[W]hen a transaction bears a reasonable relationship to this state and also to another state or nation the parties may agree that the law either of this state or of such other state or nation shall govern their rights and duties.").

HeinOnline -- 29 Vand. J. Transnat'l L. 98 1996

either party, the location of the corporate headquarters, or state of incorporation of a party would satisfy Section 187's reasonableness requirement.[142] In cyberspace, it is unclear where some of these locations might be, but reasonable arguments can be made for choosing the law of the domicile of either party.

The second aspect of reasonableness requires that the contract's choice of law accurately reflect the intention of both contracting parties; in other words, courts view the selection of law in adhesive contracts[143] suspiciously.[144] In *Carnival Cruise Lines v. Shute,*[145] however, the U.S. Supreme Court upheld a forum selection clause even when bargaining parity between the cruise line and its aggrieved passenger was lacking.[146] This case suggests that a forum selection clause between a large-scale Internet service provider and its customer is enforceable, even if the access contract between them is a standardized form contract or, perhaps just a visual notice on the log-on screen to the system.

b. Forum Selection Clauses in Cyberspace

The networked world is replete with already-existing contractual relationships between access providers and their cyber-domiciliaries. Professor Hardy notes that "access to Prodigy, Compuserve, America Online, the Well, Genie, Lexis Counsel Connect, as well as the countless small desktop BBSs run by hobbyists is already subject to contractual arrangements."[147] Universities incorporate rules of use before allowing students and faculty access to the Superhighway. The ease and simplicity with which choice of law problems may be disposed of through the use of forum and law selection clauses in these contracts is striking. Some access providers have already taken this route. Section 9.3 of America Online's Terms of Service

---

142. *See* SCOLES & HAY, *supra* note 123, at 671-72.

143. A contract of adhesion is a standarized contract offered exclusively on a "take it or leave it" basis without giving the consumer an opportunity to bargain. BLACK'S LAW DICTIONARY 40 (6th ed. 1990).

144. RESTATEMENT (SECOND) OF CONFLICT OF LAWS § 187 cmt. b (1971) ("[T]he forum will scrutinize [adhesive] contracts with care and will refuse to apply any choice-of-law provision they may contain if to do so would result in substantial injustice to the adherent."); *see also* SCOLES & HAY, *supra* note 123, at 666.

145. 499 U.S. 585, 593-94 (1991).

146. Justice Brennan in *Carnival Cruise* acknowledged that a complaining party, by satisfying a "heavy burden of proof," could show that a forum selection clause should not stand because it would be grossly onerous to that party. *Carnival Cruise*, 499 U.S. at 592-93.

147. Hardy, *supra* note 42, at 1029-30.

HeinOnline -- 29 Vand. J. Transnat'l L. 99 1996

Agreement (TOS) contains a simple forum and law selection clause to handle disputes between its users and AOL:

> The TOS shall be governed by and construed in accordance with the laws of the Commonwealth of Virginia, except with regard to its conflicts of law rules. Each party irrevocably consents to the exclusive jurisdiction of the courts of the Commonwealth of Virginia and the federal courts situated in the Commonwealth of Virginia in connection with any action arising under the TOS or relating to the AOL Service or AOL Software. . . .

Interuser disputes could quite easily be subsumed into this contractual arrangement. In this scenario, Virginia law would govern the lawsuit arising when AOL User X commits a tort against or breaks a contract with AOL User Y. This clause achieves the desired certainty, and eliminates forum shopping (assuming that all jurisdictions recognize the validity of forum and law selection clauses).

Cyberspace's choice of law problems would be accounted for if the access contract also contained language selecting a forum and law for disputes arising between one user and a second user of any other access provider with whom the first user's provider is in contractual privity. For example, AOL and CompuServe might require forum selection clauses in all users' service contracts. In turn, AOL and CompuServe would contract to the effect that disputes arising between an AOL user and a CompuServe user would be governed by a particular forum's law. Following this method, an association of access providers could work in unison to bring much needed certainty to the choice of law issues that will face their users when disputes arise among them.[148]

This contractual approach is the tidiest choice of law methodology possible because the parties are free to select the law that shall apply to disputes.[149] Typically, system operators set the terms of their "business."[150] Networks are highly decentralized;[151] rulemaking occurs at the lower network level, where the university, corporation, or commercial provider is "both the legislator and enforcer."[152] Thus, "[a] user can either comply with the ground rules, or find another system that will allow the

---

148. Professor Hardy, therefore, prematurely rules out the ability of the "contract approach" to deal with tortious conduct between citizens of one nation and those of another who use separate access providers. *See* Hardy, *supra* note 42, at 1051-52 ("[International torts are] wrongful conduct typically directed toward strangers, so the contract approach is ruled out."). This Note's model shows that even strangers may be bound by contractual arrangements.

149. *See supra* notes 133-46 and accompanying text.

150. *See* Johnson & Marks, *supra* note 41, at 488 n.4.

151. Henry H. Perritt, *Dispute Resolution in Electronic Network Communities*, 38 VILL. L. REV. 349, 352 (1993).

152. *Id.* at 352.

HeinOnline -- 29 Vand. J. Transnat'l L. 100 1996

desired activity."[153] The user who is dissatisfied with a particular access provider's choice of law selection may simply "vote with his or her mouse" and seek a new provider.[154] This "de facto voting power gives users as a group substantial strength in this arrangement."[155]

Professor Perritt views this approach as analogous to the governance of private associations.[156] He notes that private associations—like fraternities, churches, and country clubs—are largely self-governing, and that courts generally enforce the associational rules.[157]

Comment (f) to Section 187 of the Second Restatement states:

> The parties to a multistate contract may have a reasonable basis for choosing a state with which the contract has no substantial relationship. For example, when contracting in countries whose legal systems are strange to them as well as *relatively immature*, the parties should be able to choose a law on the ground that they know it well and that it is sufficiently developed. . . . So parties to a contract for the transportation of goods by sea between two countries with relatively undeveloped legal systems should be permitted to submit their contract to some *well-known and highly elaborated commercial law*.[158]

Forum selection clauses can bring order and stability to cyberspatial contracts by substituting the highly-developed real-space legal order for the uncertain and almost haphazard regime likely to result if courts are left to choose law in cyber-disputes.

Recall that Case 1 disputes arise between two users who access cyberspace through the same access provider or providers in contractual privity with one another. It appears that the

---

153. Johnson & Marks, *supra* note 41, at 488 n.4.

154. *See generally* Carnival Cruise Lines v. Shute, 499 U.S. 585, 593 (1991).

155. Johnson & Marks, *supra* note 41, at 489.

> Facially, contracts between sysops and users may appear to be contracts of adhesion, with the users possessing no negotiation or bargaining power. However, once the sysop has clearly and candidly articulated the applicable rules and obligations of the contract, the users are on notice of the nature of the contract. At this point, the users can choose to accept the terms as stated or walk away and find another system whose terms are more favorable. Moreover, online rules do evolve in response to complaints by communities of users—there is genuine collective negotiation over time.

Id. at 489 n. 7. "Sysop" is a contraction for the "system operator."

156. Perritt, *supra* note 151, at 361.

157. *Id.* at 361 n.33. In such situations, courts have "based their jurisdiction on the property, contract, or personal rights of members." *Id.* at 361-62.

158. RESTATEMENT (SECOND) OF CONFLICT OF LAWS § 187, cmt. f (1971) (emphasis added).

HeinOnline -- 29 Vand. J. Transnat'l L. 101 1996

inclusion of a forum and law selection clause in the access contract between user and provider and, at the next level, between provider and provider, solves Case 1's choice of law problems.[159] Associations of providers might contract for choice of law, or even some arbitration scheme.[160] The ease with which the contractual approach disposes of choice of law problems in cyberspace has led several authors to conclude that "[c]yberspace is, and should be, ruled mostly by contract."[161]

2. Case 2: Conceptual Analogies for a New Jurisdiction of Cyberspace

Case 2 involves a cyber-dispute between members of the Internet community at large, but no contractual nexus exists between plaintiff and defendant. The contractual approach this Note advocates is not helpful in this scenario. Professor Perritt agrees, noting that the decentralized rulemaking and enforcement that solves Case 1 disputes[162] becomes problematic when the Internet is viewed as a larger network community.[163] This scenario might require substantive law, not just conflict of laws rules.

A standard set of terms for resolving choice of law in cyberspace might be found in admiralty and maritime law,[164] the *lex mercatoria*,[165] or in a negotiated multinational choice of law treaty. The essence of these analogies is that an altogether new jurisdiction has emerged—the jurisdiction of cyberspace. These regimes answer the choice of law question because either: (1) the new jurisdiction has a substantive law of its own, and that law is the obvious "choice," or (2) the nations agree on a prescription for choosing law in such disputes. Under either scenario, the resolution of Case 2 disputes in this model depends on the

---

159. A sample law selection clause might be like the following:

Choice of law. Disputes with another Subscriber or a Subscriber to a Provider with whom [name of contracting provider] has contracted shall be governed by the law of [the choice of law] and such disputes shall be pursued only in [choice of forum]. This clause applies only to disputes arising out of events or conduct in or concerning the subscriber's participation on the Internet.

160. Perritt, *supra* note 150, at 391 (suggesting that nonjudicial dispute resolution techniques, such as arbitration by the American Arbitration Association, be used for resolving cyberspace disputes). *See also* Ethan Katsh, *Law in a Digital World: Computer Networks and Cyberspace*, 38 VILL. L. REV. 403 (1993).

161. Johnson & Marks, *supra* note 41, at 515.

162. *Supra* notes 132-33 and accompanying text.

163. Perritt, *supra* note 151, at 395-96.

164. *See infra* notes 166-207 and accompanying text.

165. *See infra* notes 208-18 and accompanying text.

HeinOnline -- 29 Vand. J. Transnat'l L. 102 1996

unification, to some extent, of either substantive law or private international law.

a. Admiralty and Cyberalty[166]

Appropriate conceptual analogies to the notion of transnational cyberspace are found in legal environments in regions where states typically may not assert sovereignty. One of the more appealing analogies arises in admiralty law.[167] Some writers have made aspirational references to a new doctrine of "cyberalty."[168] The high seas are conceptually very similar to cyberspace. Just as the territory a ship traverses is not subject to any one state's exclusive jurisdiction, so too the user in cyberspace traverses a sovereignless region that is not subject to any state's exclusive jurisdiction. Cyberspace as a domain itself—strangely multinational yet non-national[169]—and the analogy between choice of law for cybertorts and choice of law for torts on the high seas should be explored.

No state may claim sovereignty over the high seas.[170] How, then, is choice of law accomplished in the maritime cause of action? Initially, a distinction must be drawn between injuries on the high seas and those in territorial waters.[171] The cyberspace analogy applies to the former. When collisions occur on the high seas, the *lex maritima* is applied—the "general maritime law, as understood and administered in the courts of the country in which the litigation is prosecuted."[172] When the colliding ships fly the same flag of registry, courts apply the laws of that common flag.[173]

---

166. This Section owes much to the thoughtful analysis in William Tetley, *The Law of the Flag, "Flag Shopping," and Choice of Law*, 17 TUL. MAR. L.J. 139 (1993).

167. *See id.* at 143 ("Modern maritime transport, being essentially international or interjurisdictional, is subject to frequent problems concerning the appropriate choice of law. . . . Thus, maritime law is particularly suited as a source of material for the study of conflict of laws.").

168. *See, e.g.*, THE EFFECTS OF ELECTRONIC MAIL ON LAW PRACTICE AND LAW TEACHING (I. Trotter Hardy ed., 1994). Hardy proposes that "[m]aybe 'cyberspace' should really be treated as a PLACE and like the oceans, generate its own brand of 'admiralty' (cyberlaty? [sic]) law." *Id.* at 95; *see also* A NEW JURISDICTION FOR CYBERSPACE? TRANSCRIPT OF NEWJURIS: AN ELECTRONIC CONFERENCE HELD SEPT.-OCT. 1993 21 (Trotter Hardy ed., 1994) ("Is the Internet like the ocean?").

169. *See* Lauritzen v. Larsen, 345 U.S. 571, 584 (1953) (noting that shipping is "an enterprise conducted under many territorial rules and under none").

170. Shin, *supra* note 83, at 1381.

171. 2 J.D. LEE, MODERN TORT LAW § 23.24 (Rev. ed. 1988).

172. *Id.* § 23.26 (quoting The Belgenland, 114 U.S. 355, 369 (1885)).

173. *Id.*

HeinOnline -- 29 Vand. J. Transnat'l L. 103 1996

The most important principle to recognize is that "the general maritime law is not the law of any particular country but is part of the law of nations."[174] The analogy is clear: cyberspace, like the high seas, calls for a unified, common understanding of the law to be chosen to adjudicate disputes.

Many nations follow the general principle that "[t]he only safe and practical rule which can be followed [in maritime law] is to adopt the law of the ship's flag to govern in nearly all matters relating to a vessel, its captain and its crew."[175] Indeed, Justice Jackson has stated that "the weight given to the [ship's flag] overbears most other connecting events in determining applicable law."[176] This principle guides many nations' maritime choice of law rules.[177] Likewise, numerous provisions in international conventions resolve choice of law questions with the law of the flag.

Thus, the law of the flag has traditionally played a key role in the resolution of choice of law questions arising from conduct on the high seas. Under this approach, choice of law in cyberspace might be decided by reference to the law of the state in which the access provider is located. In this sense, one's cyber-domicile becomes one's domicile for choice of law purposes. There is precedent for such a view. *Lauritzen v. Larsen* noted that "the nationality of the vessel for jurisdictional purposes was attributed to all her crew."[178]

The law of the flag as a choice of law signpost suffers from serious difficulties when vessels fly flags of convenience or when collisions occur between vessels of different flags. Both of these problems persist in the adaptation of admiralty to cyberalty.

---

174. GRANT GILMORE & CHARLE L. BLACK, JR., THE LAW OF ADMIRALTY 482 (2d ed. 1975); *see also* Lauritzen v. Larsen, 345 U.S. 571, 581-82 (1953) ("[C]ourts of this and other commercial nations have generally deferred to a non-national or international maritime law of impressive maturity and universality. It has the force of law . . . from acceptance by common consent of civilized communities of rules designed to foster amicable and workable commercial relations.").

175. Tetley, *supra* note 166, at 140 (quoting E. LAFLEUR, THE CONFLICT OF LAWS IN THE PROVINCE OF QUEBEC 185 (1898)).

176. *Lauritzen*, 345 U.S. at 585.

177. Tetley, *supra* note 166, at 147-49 (cataloging nations that stipulate the law of the flag as the appropriate conflicts rule).

178. 345 U.S. 571, 586 (1953).

HeinOnline -- 29 Vand. J. Transnat'l L. 104 1996

i. Different Access Providers, Different Flags

Simple law of the flag analysis is not adequate to handle the choice of law problem of a transnational tort in cyberspace because the parties are unlikely to be traveling on the same "ship," or access provider. But how is maritime choice of law resolved when torts arise in two-ship collisions?[179] If the ships are of the same flag, the national law of the common flag should apply.[180] If the ships fly different flags, and both nations are parties to the Collision Convention of 1910, the terms of that convention apply.[181] The most interesting case results when ships of different flags collide and no multinational agreement is in force to resolve the conflicts question. In the United States, one writer has noted:

> If a general rule is demanded, all that can be said is that on the whole [U.S.] courts will apply the internal law common to both ships if there is one. If not, the courts have vacillated between the choice of the law of the defendant vessel and the law of the plaintiff vessel and when apparently unable to make the choice have applied the *lex fori*. . . .[182]

In cyberspace, the implications are obvious. If two users (sharing neither nationality nor access provider) "collide," the simplest choice of law decision is to apply (1) the *lex fori*, (2) the law of the plaintiff's domicile, or (3) the law of the defendant's domicile. Of course, this result might sacrifice fairness to one of the parties in the name of simplicity. This unsatisfying result drove the drafters of the Second Restatement to compose a better regime for nonmaritime actions.

The more sophisticated multifactor analysis of the Second Restatement is reflected in a U.S. maritime case with a multinational flavor similar to cyber-disputes, *Lauritzen v. Larsen*.[183] The issue in *Lauritzen* was which nation's law would apply to a maritime tort. Larsen, a Danish seaman, while temporarily in New York, joined the crew of the *Randa*, a ship of Danish flag and registry, owned by Lauritzen, a Danish citizen.[184] Larsen had signed the ship's articles (including a forum selection

---

179. *See generally* Tetley, *supra* note 166, at 168-71.

180. *Id.*

181. International Convention for the Unification of the Rules Relating to Collisions at Sea, Sept. 23, 1910, art. 12, 212 Consol. T.S. 178, 183, *reprinted in* IGNACIO ARROYO, INTERNATIONAL MARITIME CONVENTIONS 1541 (1991).

182. Tetley, *supra* note 166, at 169 (quoting D. Winter, *Maritime Torts: The Choice-of-Law Principles*, 3 INT'L & COMP. L.Q. 115, 124-25 (1954)). In England, the *lex fori* is applied to this situation. *Id.*

183. 345 U.S. 571 (1953).

184. *Id.* at 573.

HeinOnline -- 29 Vand. J. Transnat'l L. 105 1996

clause), which provided that the rights of the crew would be governed by Danish law.[185] Larsen was injured by negligent acts aboard the *Randa* in Havana Harbor.[186] He then sued his employer under the U.S. Jones Act[187] in the Southern District of New York.[188] A conflict of laws existed because Danish law imposed a damage limitation on his action, while the Jones Act did not.[189]

The U.S. Supreme Court held that Danish law, not the Jones Act, applied to the case.[190] In reaching this conclusion, the court balanced several factors: (1) the place of the wrongful act (*lex loci delicti*), (2) the law of the flag, (3) the allegiance or domicile of the plaintiff, (4) the allegiance of the defendant, (5) the place of contract, (6) the inaccessibility of a foreign forum, and (7) the law of the forum.[191]

Larsen argued strenuously that the shipowner's "frequent and regular" contacts with the United States justified application of the U.S. statute to the case.[192] Justice Jackson wrote:

> But the virtue and utility of sea-borne commerce lies in its frequent and important contacts with more than one country. If, to serve some immediate interest, the courts of each were to exploit every such contact to the limit of its power, it is not difficult to see that a multiplicity of conflicting and overlapping burdens would blight international carriage by sea. Hence, courts of this and other commercial nations have generally deferred to a non-national or international maritime law of impressive maturity and universality. It has the force of law, not from extraterritorial reach of national laws, nor from abdication of its sovereign powers by any nation, but from acceptance by common consent of civilized communities of rules designed to foster amicable and workable commercial relations.
>
> International or maritime law in such matters as this does not seek uniformity and does not purport to restrict any nation from making and altering its laws. . . . [I]t aims at stability and order. . . .[193]

---

185. *Id.*
186. *Id.*
187. At the time of *Lauritzen*, 46 U.S.C. § 688 (now located at 46 U.S.C. app. § 688 (1988)) read in pertinent part:

> Any seaman who shall suffer personal injury in the course of his employment may, at his election, maintain an action for damages at law, with the right of trial by jury, and in such action all statutes of the United States modifying or extending the common-law right or remedy in cases of personal injury to railway employees shall apply.

188. Lauritzen v. Larsen, 345 U.S. 571, 573 (1953).
189. *Id.* at 575.
190. *Id.* at 592-93.
191. *Id.* at 583-92.
192. *Id.* at 581-82.
193. *Id.* at 581-83 (citation omitted).

HeinOnline -- 29 Vand. J. Transnat'l L. 106 1996

Justice Jackson's writing clearly applies to cyberspace. Cyberspace represents a dramatic leap forward in global interconnectivity and has the capacity to revolutionize global communications and commerce. Much of cyberspace's "virtue and utility" lies in its "frequent and important contact with more than one country."[194] A balancing approach, like that in *Lauritzen*, relieves parties of a mechanical approach to choice of law methodology. In short, *Lauritzen v. Larsen* teaches that, according to U.S. law, the flag is only one relevant point of contact in the balancing scheme.[195] But as desirable as the *Lauritzen* multifactor approach is for its flexibility, the balancing approach really gives no clear answer, and fails to resolve choice of law in a region that is both transnational and non-national.

ii. Flags of Convenience in Cyberspace

Another problem that arises in the cyberalty framework is that of "flag shopping" and "flags of convenience."[196] A flag of convenience is a flag, literally "chosen" by a vessel, with which the vessel has little connection.[197] Reasons such as tax avoidance and preferable treatment under the state's substantive laws guide this choice, called flag shopping.[198] But attempts to gain favorable treatment by flag shopping have not been entirely successful.[199] Many nations will ignore a vessel's flag and, instead, examine the ownership of the vessel for purposes of contact analysis.[200] The domicile of the owners is one important contact to consider in choosing the applicable law.[201]

The analogy in cyberspace is easily seen. Offshore havens might arise that have favorable laws for Internet access providers. Professor Burk notes that some information-poor countries have "moved towards becoming 'data havens.'"[202] The laws of these havens might eliminate liability for contributory infringement of

---

194. *Id.* at 581.

195. *Id.* at 584-86.

196. *See generally* Tetley, *supra* note 166, at 168-71.

197. *See generally id.* at 173 n.224 (citing BOLESLAW A. BOCZEK, FLAGS OF CONVENIENCE: AN INTERNATIONAL LEGAL STUDY 2 (1962)).

198. Tetley, *supra* note 166, at 173-74 (estimating that 40% of the world's vessels fly flags of convenience).

199. *See id.* at 180-84.

200. *Id.* at 180. *See* Rainbow Line, Inc. v. M/V Tequila, 480 F.2d 1024, 1027 (2d Cir. 1973) ("[I]t is well settled that the courts will look through the facade of foreign registration and incorporation to the [U.S.] ownership behind it."); Hellenic Lines v. Rhoditis, Ltd., 398 U.S. 306, 309-10 (1970) (applying U.S. law to Greek-flagged ship because its owner had substantial and continuing contacts with the United States, its "base of operations.").

201. Tetley, *supra* note 166, at 179. *See also* Lauren v. Lauritzen, 345 U.S. 571, 583-93 (1953) (contact analysis).

202. Burk, *Patents*, *supra* note 13, at 52, 53 nn.386, 388.

HeinOnline -- 29 Vand. J. Transnat'l L. 107 1996

intellectual property[203] or make "cyber-defamation" nonactionable. Given the above discussion, however, it is not certain that other nations would honor the providers' flags of convenience.[204]

Professor Tetley believes that the problems of flag shopping and flags of convenience have eliminated the usefulness of the law of the flag as a choice of law device.[205] He agrees with the *Lauritzen v. Larsen*[206] approach: the flag is only one contact in a multifactor test.[207] Flag shopping only reaffirms the conclusion that the law of the flag does not entirely solve the choice of law conundrums in cyberspace.

b. The Law Merchant and Law Cyberspace

Cyberspace's unique legal issues have inspired some authors to point to the medieval *lex mercatoria*—the Law Merchant—as a conceptual framework for a new body of cyber-law (the Law Cyberspace).[208] The Law Merchant was a collection of customary practices among traveling merchants in Medieval Europe and Asia that was enforceable in "all the commercial countries of the civilized world."[209] The Law Merchant existed "in some sense apart from and in addition to the ordinary rules of law that applied to non-merchant transactions."[210] The *lex mercatoria* has been described as follows:

---

203. Professor Burk notes that some nations have no patent system at all. *Id.* at 33. With regard to software patents, some nations, such as Brazil and Bulgaria, grant no protection whatsoever. *Id.*

204. *See supra* note 94 and accompanying text.

205. Tetley, *supra* note 166, at 183.

206. 435 U.S. 571 (1953).

207. *Id.* at 584-85.

208. *See, e.g.*, Anne W. Branscomb, *Overview: Global Governance of Global Networks*, *in* TOWARD A LAW OF GLOBAL COMMUNICATIONS NETWORKS 1, 21 (Anne W. Branscomb ed., 1986); Hardy, *supra* note 42, at 1019 (1994). Much of this Part's analysis is owed to Professor Hardy, who moderates an Internet listserver, CYBERIA-L, that focuses on law in cyberspace.

209. Hardy, *supra* note 42, at 1020 n.60 (quoting Bank of Conway v. Stary, 200 N.W. 505, 508 (N.D. 1924)).

210. *Id.* at 1020. *See generally* Andreas F. Lowenfeld, *Lex Mercatoria: An Arbitrator's View*, *in* LEX MERCATORIA AND ARBITRATION 37, 54-55 (Thomas E. Carbonneau ed., 1990) (listing 20 "rules" of the Law Merchant).

HeinOnline -- 29 Vand. J. Transnat'l L. 108 1996

> The law merchant has been for centuries and continues to be today an international body of law, founded on the shared legal understandings of an international community composed principally of commercial, shipping, insurance, and banking enterprises of all countries. . . . We believe that the shared legal understandings of the international mercantile community should be seen as an *autonomous body of law, binding in appropriate cases upon national courts.*[211]

Why is the *lex mercatoria* a satisfying analogy to the legal problems posed by transnational cyberspace? Simply, the Law Merchant abrogates the need for the choice of law inquiry and the attendant balancing and weighing of interests. Part III of this Note concludes that traditional paradigms in choice of law analysis are inadequate on the transnational and non-national Internet. The Law Merchant is a body of law in itself, which enables an easy resolution to the choice of law question. The laws of the various nations are displaced, in a limited fashion, by the laws of a collection of merchants (here, users) with their own customs and usages of trade. Importantly, the customary Law Merchant is not a complete legal system. Nevertheless, because virtually all legal systems accept the binding nature of trade usages in contracts between merchants, there should be no fundamental obstacle to the general recognition of a customary law of international trade.[212]

In cyberspace, Case 2 disputes are ripe for such a conflicts model. Just as the merchants knew the customs and usages in the *lex mercatoria*, so too should users in cyberspace be charged with a knowledge of the customs and usages of the online world. The concept falters, however, in Case 3 disputes in which torts are committed and contracts broken between a user and a person or entity not subject to the Law Cyberspace.

One of the most appealing aspects of the Law Merchant as an analogy to cyberspace is its ability to respond and adapt rapidly to changes in the technical and legal environments.[213] Conventional sources of law are "generally . . . unable to adjust to changing commercial custom with the same ease as could a commercial system. . . . Strict rules lack[] the flexibility to vary in response to the peculiarities of the merchants, to their trade background and to their form of bargaining."[214]

---

211. Harold J. Berman & Felix J. Dasser, *The "New" Law Merchant and the "Old": Sources, Content, and Legitimacy, in* LEX MERCATORIA AND ARBITRATION 21-24 (Thomas E. Carbonneau, ed. 1990) (emphasis added).

212. *Id.* at 32.

213. Hardy, *supra* note 42, at 1021.

214. *Id.* at 1022 n.63 (quoting LEON E. TRACKMAN, THE LAW MERCHANT: THE EVOLUTION OF COMMERCIAL LAW 16 (1983)).

HeinOnline -- 29 Vand. J. Transnat'l L. 109 1996

In this age of cyberspace and global connectivity, reliance on statutes and *stare decisis* simply cannot keep up with a rapidly evolving technological environment. Traditional law, then, might condemn rules regulating conduct in cyberspace to perpetual obsolescence. Professor Hardy argues that "[a] 'Law Cyberspace' co-existing with existing laws would be an eminently practical and efficient way of handling commerce in the networked world."[215]

Professor Hardy notes that special courts sprung up in the Middle Ages to enforce the customs and usages of trade that comprised the Law Merchant. The jurisdiction of these courts was limited to disputes arising from commercial transactions.[216] The creation of cybercourts, as some have advocated, is a drastic step.[217] However, even in the absence of these special tribunals, a Law Cyberspace ameliorates the choice of law problems that Part III of this Note discusses. Simply, when a forum state seeks to apply a set of rules, it would look to the Law Cyberspace; the chosen law would be the collection of customs and accepted practices—codified or not—that had grown up with cyberspace.[218]

c. Choosing Law in Sovereignless Regions

i. Outer Space

As Part II of this Note illustrates, cyberspace is transnational, yet non-national. In a similar vein, outer space is a region within the reach and use of many nations, but not easily demarcated into jurisdictions. The coming years will no doubt see an increased use of the multinational space station (MSS) as a common way to investigate and utilize outer space. Helen Shin notes, however, that no agreement or treaty has addressed the issue of choice of law in space, even though conflict of laws questions are sure to arise.[219] Shin notes that disputes between individuals arising out of torts committed aboard a MSS must be resolved according to some state's laws, since the station "presumably [would] have no such laws of its own."[220] Shin also

215. Hardy, *supra* note 42, at 1021.

216. *Id.* at 1020-21.

217. *See, e.g., id.* at 1052-53 (suggesting that "cyberspace users form their own virtual courts").

218. *Id.* at 1036-41 (explaining the process for determination and acceptance of customs by courts).

219. Shin, *supra* note 83, at 1375.

220. *Id.* at 1378.

HeinOnline -- 29 Vand. J. Transnat'l L. 110 1996

considers the choice of law implications for outer space, where sovereignty and jurisdictional analysis fail.[221]

Shin concludes that choice of law should be made through arbitration undertaken according to the Model Law on International Commercial Arbitration promulgated by the United Nations Commission on International Trade Law (UNCITRAL), which established procedures for binding arbitration of disputes.[222] The signatories to this multinational accord and their nationals would thereby be bound to the jurisdiction of the arbitration panel. Thus, while conventional choice of law processes are probably insufficient for the multinational space station, new proposals hold promise.

ii. Antarctica

Another analogy to the transnational, yet non-national "region" of cyberspace is the "world's last sovereignless continent, Antarctica."[223] Although the Antarctic Treaty[224] governs public international law issues, no provision has yet been made with respect to jurisdiction and choice of law issues for tort and contract actions among individuals of different nations. In short, "Antarctica remains a 'jurisdictional no-man's land.'"[225] Traditional choice of law methodologies break down in Antarctica because "there is no *lex loci delicti*" and "Antarctica is the only land mass on the planet not subject to a unified private legal system."[226] Similarly, cyberspace is an example of a non-land mass without a choice of law regime.

In Jonathon Blum's analysis, the governing law in an action in which there is no proof of foreign law becomes the law of the forum in which the suit is brought (the *lex fori*). Thus, if *lex loci delicti* fails because the *lex loci* has no legal system, then *lex fori* is the answer. For example, in *Beattie v. United States*,[227] an Air New Zealand plane crashed in Antarctica. The D.C. Circuit held that choice of law was not an issue because there were no alternate legal systems from which to choose.[228] U.S. law was

---

221. Shin notes two regions where states may not assert sovereignty: Antarctica and the High Seas. Shin, *supra* note 83, at 1379-81. This Note considers both of these "sovereign-less" regions for their instructiveness on the choice of law in cyberspace.

222. *Id.* at 1378.

223. Jonathon Blum, *The Deep Freeze: Torts, Choice of Law, and the Antarctic Treaty Regime*, 8 EMORY INT'L L. REV. 667, 667 (1994).

224. The Antarctic Treaty, Dec. 1, 1959, 12 U.S.T. 794, 402 U.N.T.S. 71 (entered into force June 23, 1961).

225. Blum, *supra* note 223, at 668.

226. *Id.* at 680.

227. 756 F.2d 91 (D.C. Cir. 1984).

228. *Id.* at 104, 105.

HeinOnline -- 29 Vand. J. Transnat'l L. 111 1996

applied as the *lex fori*. In another case, the court applied U.S. law to a tort in Antarctica because the United States has a great deal of control over that area.[229]

Blum suggests two ways to resolve the Antarctic choice of law conundrum: (1) the parties to the Antarctic Treaty could develop a body of law specifically designed to apply to tortious conduct in Antarctica, or (2) the parties could promulgate a choice of law code that would decide such questions.[230] Blum's first option approximates the *lex* cyberspace or cyberalty concepts this Note discusses previously. In these scenarios, a new jurisprudence might arise that would obviate the need for choice of law. The choice is made simply by applying the "new" law. Blum is skeptical, however, that the parties to the Antarctic Treaty would divest themselves of sovereignty (whatever of it exists) over Antarctic actions.[231]

Blum's second option offers a multinational choice of law accord: a "Protocol on Choice of Law for the Commission of Torts in Antarctica."[232] This agreement would call for the application of either (1) the law of the plaintiff's home state in all tort cases, or (2) the *lex fori* in all cases. These two analyses, then, devolve into simplistic answers to the choice of law question—answers that revert to the most primitive choice of law decisions a court can make. Simplicity is elevated over both fairness and reason; however, the goal of fairness in choice of law deserves more than just simple results.

d. Prospects for a Multilateral Choice of Law Treaty for Cyberspace

The adoption of a supranational corpus of law, such as the Law Merchant or admiralty law, would obviate the need for a conflict of laws regime in cyberspace. The obvious political improbability of such a tack leads most authors to conclude that nations will refuse to surrender their sovereignty, their power to make law, or their power to control adjudication.[233] The next best solution to the choice of law conundrum, one might suppose, would be the unification of conflict of laws rules. Rather than

229. *See* Environmental Defense Fund v. Massey, 986 F.2d 528 (D.C. Cir. 1993).

230. Blum, *supra* note 223, at 690.

231. *Id.* at 690-95.

232. *Id.* at 695.

233. *See, e.g.*, Blum, *supra* note 223, at 694-95 ("In all likelihood, it was a foregone conclusion . . . [that nations] will not stand for the establishment of any body that threatens their (albeit frozen) sovereignty on [Antarctica].").

HeinOnline -- 29 Vand. J. Transnat'l L. 112 1996

crafting a new jurisdiction's entire substantive law, the nations need only agree on this jurisdiction's private international law.

Ample precedent exists for such a multinational conflict of laws accord. The Hague Conference on Private International Law and the Rome Institute for the Unification of Private Law (UNIDROIT) are dedicated to just such a mission. The Hague Convention is a permanent multinational group charged with preparing texts that unify choice of law rules.[234] The International Institute for the Codification of Private Law in Rome focuses primarily upon the unification of substantive rules of law.[235]

In recent years, the United States has actively participated in the global unification of certain areas of law.[236] Scoles and Hay list more than twenty multilateral treaties affecting private law that the United States has ratified,[237] four of which originated in the Hague Conference. Hague Conference agreements cover service of process and obtaining evidence abroad.[238] The United Nations Convention on the International Sale of Goods (the Sale of Goods Convention),[239] one of the more important multilateral treaties, entered into force in the United States on January 1, 1988. The Sale of Goods Convention essentially "revitalizes the ancient *lex mercatoria*."[240] Although a discussion of the Sale of Goods Convention is beyond the scope of this Note, the significance of ratifying an accord that unifies, to some extent, private international law should not be missed.

Just as a multinational accord has been reached on conflict of laws with regard to a number of subjects,[241] such as the law applicable to traffic accidents among nationals of different countries[242] and the law determining the status of aliens,[243] an agreement might be forged to unify choice of law rules for cyberspatial disputes. Indeed, the authors who have considered choice of law in sovereignless regions have prescribed just such a

---

234. Peter Winship, *Private International Law and the U.N. Sales Convention*, 21 CORNELL INT'L L. REV. 487, 488 (1988).

235. *Id.* at 488-89.

236. SCOLES & HAY, *supra* note 123, at 154.

237. *Id.* at 153-54 n.1.

238. *Id.*

239. U.N. Conference on Contracts for the International Sale of Goods, Final Act (April 10, 1980), U.N. Doc. A/Conf. 97/18, *reprinted in* S. Treaty Doc. No.98-9, 98th Cong., 1st Sess. *and* 19 I.L.M. 668 (1980).

240. Francis A. Gabor, *Stepchild of the New* Lex Mercatoria: *Private International Law from the United States Perspective*, 8 NW. J. INT'L L. & BUS. 538, 539 (1988).

241. *See generally* SCOLES & HAY, *supra* note 123, at 153 n.1.

242. Road Traffic Convention (Geneva, 1949), 3 UST 3008, 125 UNTS 22.

243. 46 Stat. 2573, 132 U.N.T.S. 301.

HeinOnline -- 29 Vand. J. Transnat'l L. 113 1996

course: Blum recommends a "Protocol on Choice of Law for the Commission of Torts in Antarctica";[244] Faucher proposes a federal statute to unify U.S. defamation law and preempt state choice of law decisions in United States cyber tort actions;[245] Shin advocates a convention incorporating the provisions of the UNCITRAL Model Law on International Commercial Arbitration for torts in outer space;[246] Kirby suggests that the member countries of the Organization for Economic Cooperation and Development (OECD) "work towards the development of principles . . . to govern the applicable law in the case of transborder [data] flows";[247] Sciglimpaglia leans toward an OECD approach to unifying "choice of law and extradition procedures" for transnational computer hacking;[248] and Hardy looks to the possible formation of "virtual courts" to devise appropriate rules for choosing or unifying the law respecting international torts in cyberspace.[249]

The common thread in each of these suggestions is that a coherent choice of law regime might be established through a multinational treaty for actions in transnational settings where conventional choice of law is impracticable. In the end, such a treaty might provide the easiest solution to the vexing problem of choice of law in transnational cyberspace. It should be recalled, however, that simple, easily articulated rules for choice of law sometimes sacrifice fairness. Blum's two options for the Antarctic protocol rely on only one factor—either the *lex fori* or the law of the plaintiff's domicile.[250] Unfortunately, ameliorating these simplistic rules inevitably sacrifices their "cleanliness" and ease of application.

3. Case 3: Where Conventional Choice of Law Must Still Reign

In Case 3, a cyberspace nexus exists, but both parties to the action cannot be said to have "availed" themselves of a law of cyberspace. It would be fundamentally unfair for the new model to encompass the action. Choice of law must derive from either the traditional modes of conflicts analysis or from the signing of a multinational choice of law accord by which the nationals of all

---

244. Blum, *supra* note 223, at 695-98.

245. Faucher, *supra* note 30, at 1066-73.

246. Shin, *supra* note 83, at 1411-12.

247. Kirby, *supra* note 29, at 243 (suggesting that the Hague Conference might help clarify some issues).

248. Sciglimpaglia, *supra* note 53, at 247-50 (suggesting that the OECD accomplish such a task).

249. Hardy, *supra* note 42, at 1052-53.

250. Blum, *supra* note 223, at 695-98.

HeinOnline -- 29 Vand. J. Transnat'l L. 114 1996

signatories become bound to the choice of law process in the agreement.[251]

Adapting novel choice of law strategies to disputes in cyberspace works well when both parties are users. However, the solutions considered in Case 1 and Case 2 are ineffective when harm to noncyberspace parties is involved.[252] It would be a poor policy to allow entities in cyberspace to control the forum for disputes involving those without connection to the Internet.[253] These real-space entities are not party to a cyberspace contract and have no reason to suspect that causes of action will be governed by a law chosen on account of cyberspace.[254]

It is easy to envision the data haven[255] whose service contract chooses the law of a state with no privacy, intellectual property law, or recovery for defamation. Defendants could thereby easily "immunize" their tortious conduct. Recall this Note's discussion regarding flags of convenience in the admiralty setting: it is fundamentally unfair to allow such tactics to strip a plaintiff of a remedy because the defendant has "outsmarted" the law in behaving strategically.[256]

We may simply be resigned to the traditional modes for choice of law in certain cyber-disputes.[257] The *Lauritzen v. Larsen*[258] approach, while imperfect, probably represents the current state of choice of law in transnational but non-national regions where points of contact are plentiful. The *Lauritzen* approach is adaptable and somewhat well-suited to resolving choice of law in cyberspace.

---

251. *See supra* notes 232-44 and accompanying text (discussing multinational conflict of laws agreements).

252. *See* Perritt, *supra* note 151, at 365 n.54 ("Contract cannot, however, bind third parties, which leaves a major gap in regulating liability for injury resulting from messages.").

253. *See also* Johnson & Marks, *supra* note 41, at 513 n.104:

> The contracts [approach to dispute resolution] cannot solve the problems associated with harm to third parties because a third party who may be harmed by libel, fraud, theft, etc. is not party to the contract. No bargain between a user and a system provider can, in itself, alter the responsibility of either one to a third party harmed by action of one or the other.

254. The Sale of Goods Convention reflects this reluctance to bind nationals of nonsignatory parties. The United States ratified the Convention on the condition that it apply only if both contracting parties have their places of business in signatory countries. Gabor, *supra* note 240, at 539.

255. *See supra* notes 202-03 and accompanying text (regarding forum and flag shopping).

256. *See supra* notes 196-204 and accompanying text.

257. *See supra* notes 105-27 and accompanying text (describing conventional approaches to choice of law in tort and contract actions).

258. 345 U.S. 571 (1973).

HeinOnline -- 29 Vand. J. Transnat'l L. 115 1996

IV. CONCLUSION

Conflict of laws is a subject that is difficult for both law students and practitioners. The advent of new technologies threatens to aggravate the problem by defying the concepts of sovereignty, territoriality, and even location. Cyberspace is, at its foundation, both multinational and non-national. Cyberspace challenges the world to somehow reconcile a geographical real-space with a nongeographical cyberspace. Many writers believe cyberspace should be treated as a separate jurisdiction. It is doubtful, however, that nation-states in real-space will relinquish control over the communications medium of the twenty-first century.

This Note suggests that the reconciliation of the choice of law conundrum in cyberspace might be accomplished by a three-pronged model based on three different situations: (1) disputes involving parties in privity with each other who act in their cyberspatial capacities; (2) those involving two users not in privity but acting in their cyberspatial capacities; and (3) those involving cyberspace with regard to the defendant, but not the plaintiff. For each of these scenarios, a different choice of law regime should be implemented. The new technologies mandate the synthesis of these approaches. If cyberspace does represent the arrival of the global village, then a new paradigm will be necessary to satisfy the conflict of laws that will arise in a village confused by a sovereign on every block.

Matthew R. Burnstein

HeinOnline -- 29 Vand. J. Transnat'l L. 116 1996