

М. А. Федотов*

КОНСТИТУЦИОННЫЕ ОТВЕТЫ НА ВЫЗОВЫ КИБЕРПРОСТРАНСТВА

Аннотация. Анализируя особенности взаимоотношений различных субъектов в области информационно-коммуникационных технологий, автор приходит к выводу о необходимости формирования новой отрасли права — права киберпространства. Показано, что современные инструменты правового регулирования (как на национальном, так и на наднациональном уровне) не обладают достаточной эффективностью для упорядочения данных взаимоотношений. В связи с этим подчеркивается важность таких способов регулирования информационно-телекоммуникационного пространства, как саморегулирование и программный код. Также предлагаются конкретные поправки к Конституции Российской Федерации, направленные на большее обеспечение информационных прав граждан.

Специфика киберпространства, по мнению автора, заставляет пересмотреть традиционный подход к действию любой правовой нормы в пространстве, во времени и по кругу лиц, поскольку в интернет-среде понятие «пространство» лишается однозначной географической определенности, понятие «время» не привязано ни к какому часовому поясу, а понятие «круг лиц» включает не физических и юридических лиц, а компьютеры и другие устройства, участвующие в сетевом взаимодействии и идентифицируемые по их IP-адресам и другим технологическим деталям.

Установление по примеру некоторых авторитарных стран правила о возможности подключения человека к Сети лишь при предъявлении документа, удостоверяющего личность, ведет только к замедлению развития соответствующей страны, к ее выпадению из общего мирового процесса, но никак не стимулирует очищение киберпространства от всего того, что противоречит общепризнанным представлениям о правомерном и должном.

Киберпространство постоянно задает все новые и новые вопросы, касающиеся охраны интеллектуальной собственности, а предлагаемые законодателями-традиционалистами ответы, будучи выдержаны в привычной логике разрешений и запретов, с одной стороны, порождают массовое, тотальное нарушение установленного правового порядка, а с другой — способствуют накоплению в нем внутренних логических противоречий.

Ключевые слова: Конституция Российской Федерации, право киберпространства, Интернет, облачные технологии, саморегулирование, программный код, трансформативный конституционный режим, кодифицированный конституционный режим.

DOI: 10.17803/1729-5920.2016.112.3.164-182

В 1996 г. удивительный американский правовед Лоуренс Лессиг решил... прочитать конституцию в киберпространстве. Его статья в юридическом журнале Университета Эмори так и называлась — «Читая Конституцию в ки-

берпространстве»¹. В этой статье он предложил различать два вида конституционных режимов: кодифицированный (codifying) и трансформативный (transformative). Кодифицированный, т.е. построенный на неких кодах, алгоритмах,

¹ Lessig L. Reading the Constitution in Cyberspace // URL: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=41681.

© Федотов М. А., 2016

* Федотов Михаил Александрович, доктор юридических наук, профессор, руководитель кафедры ЮНЕСКО по авторскому праву и другим правам интеллектуальной собственности, Научный исследовательский университет «Высшая школа экономики» 101000, Россия, г. Москва, ул. Мясницкая, д. 20

конституционный режим запрограммирован на сохранение неких существенных свойств конституционной или правовой культуры. Напротив, трансформативный конституционный режим направлен на изменение существующей конституционной или правовой культуры, он проникнут стремлением сделать его иным в будущем. Картина кодифицированного режима — это Улисс, пытавшийся поставить мачту. Картина трансформативного режима — революционная Франция.

По мнению Лессига, американский Билль о правах 1791 года был образцом кодифицированного конституционного режима, поскольку стремился обезопасить некоторые практики и ценности от изменений. Напротив, конституционные поправки времен Гражданской войны носили трансформационный характер, поскольку были нацелены на то, чтобы перестроить то, что уже состоялось в американской социальной и правовой практике, вырвать из американской души традицию неравенства, заменить ее практикой равенства.

Лессиг весьма скептически смотрит на перспективы кодифицированного конституционного режима, особенно с учетом того, что киберпространство делает совершенно ясным, насколько трудно реализовать такую конституцию на практике. В качестве примера он берет Четвертую поправку к Конституции США, которая гласит: «Право народа на охрану личности, жилища, бумаг и имущества от необоснованных обысков и арестов не должно нарушаться; ни один ордер не должен выдаваться иначе как при наличии достаточного основания, и он должен быть подтвержден присягой или торжественным заявлением и содержать подробное описание места, подлежащего обыску, личностей или предметов, подлежащих аресту». На этом примере он показывает, как новые информационные технологии облегчают государству контроль над частной жизни граждан, формально не нарушая при этом конституционный запрет, и одновременно облегчают гражданам нахождение убежища от государственного контроля.

Если с этой точки зрения посмотреть на Конституцию Российской Федерации 1993 года, то легко заметить, что она тоже в значительной степени кодифицированная — в том смысле, который придает этому термину Лоуренс Лессиг. Она нацелена на сохранение статус-кво

и потому неизбежно все более и более отстает от природы виртуальной реальности.

Еще со студенческой скамьи мы заучили, что конституционное право является основой всех других отраслей права. Следовательно, пока Конституция не обретет своего интернет-измерения, всякие попытки правового регулирования деятельности в киберпространстве методами национального законодателя обречены на неудачу. Только прочитав и поняв Конституцию в киберпространстве, мы сможем прийти к формированию целостной системы регулирования информационных отношений, которая неминуемо должна сложиться в условиях расширяющегося проникновения информационно-сетевых технологий в жизнь современного общества. Такое понимание информационного права, как права киберпространства, российского аналога англоязычного Cyberspace Law, впервые было представлено мной 27 января 2000 г. на конференции по актуальным проблемам информационного права в Московской государственной юридической академии имени О.Е. Кутафина (МГЮА). Если представить, что информационно-коммуникационные сети — это не просто новое средство коммуникации, а новая сфера обитания человеческой цивилизации, новая сфера человеческой активности и новая сфера применения права, то легко понять, что информационное право должно иметь особый метод правового регулирования, ибо регулирование общественных отношений будет осуществляться в первую очередь в киберпространстве.

«Иными словами, — писал я в 2000 г., — человек будет не просто пользоваться телекоммуникационными сетями, он будет вступать в правовые отношения, испытывать на себе правовое регулирование через телекоммуникационные сети, внутри телекоммуникационных сетей. Вот почему информационное право в конечном счете возникнет именно как совокупность правовых норм, реализуемых в киберпространстве. Здесь неминуемо появятся такие подотрасли права, как информационное уголовное право, информационное уголовно-процессуальное, информационное гражданское и т.д. Проникая в киберпространство, традиционные отрасли права (уголовное, гражданское, административное и прочие) непременно должны видоизменяться, адаптироваться к необычным условиям правоприменения»².

² Труды по интеллектуальной собственности : материалы науч.-теорет. конференции. Москва, МГЮА, 27 января 2000 г. М., 2000. Т. 2 : Актуальные проблемы информационного права. С. 18.

Позднее представление об информационном праве как праве киберпространства приобрело сторонников среди специалистов. Так, А. А. Тедеев в своих теоретических работах неоднократно подчеркивает, что «предметом информационного права как права киберпространства должны выступать общественные отношения не просто по обороту информации, а только возникающие, изменяющиеся и (или) прекращающиеся в информационной среде глобальных компьютерных сетей»³.

Чтобы представить темпы проникновения интернет-технологий в современное общество, достаточно сравнить скорость распространения современных телекоммуникационных сетей с темпами развития сети приема традиционных аудио- и аудиовизуальных СМИ. Так, в США радиовещание смогло расширить число своих пользователей до 50 млн человек за 38 лет, телевидение — за 13 лет, Интернет — за 4 года.

Число пользователей Интернета продолжает неуклонно расти по всему миру. Причем, если рост числа пользователей имеет естественные пределы, предопределенные численностью населения, то рост числа интернет-ресурсов, доменных имен и различных сервисов ограничен лишь масштабами человеческого воображения. Можно утверждать, что именно в этой сфере наиболее яркое подтверждение получает известный тезис Альберта Эйнштейна: **«Воображение важнее знания. Знание ограничено. Воображение охватывает весь мир.** Когда понимаешь, насколько далеко человечество продвинулось с пещерных времен, сила воображения ощущается в полном масштабе. То, что мы имеем сейчас, достигнуто с помощью воображения наших прадедов. То, что у нас будет в будущем, будет построено с помощью нашего воображения».

Более того, информационное общество не просто вырастает из ставшего уже традиционным постиндустриального общества, а постепенно поглощает его, вместе со сложившейся

за последние века системой правового регулирования⁴. Современный человек все больше услуг получает через компьютерные сети, все больше потребностей он здесь удовлетворяет, все больше времени проводит во Всемирной паутине. Одновременно он обрывает новыми контактами, особенно если он интегрирован в ту или иную социальную сеть или иным образом участвует не только в потреблении, но и в производстве информации. Тем самым он участвует в глобальном процессе уплотнения социальных связей, накопления социального капитала именно в рамках трансграничной компьютерной сети. Известный американский социолог Роберт Путнам, впервые описавший процесс накопления социального капитала через уплотнение сетей взаимодействия людей и структур гражданского общества, отмечал, что общество, для которого характерна обобщенная взаимность, более эффективно, чем общество всеобщего разобщения, точно так же, как деньги эффективнее бартера. По его мнению, то, что заслуживает доверия, «смазывает» социальную жизнь⁵.

Так постепенно современный человек все в большей степени превращается в кибернавта, Ихтиандра мирового информационного океана — сначала в приезжего, потом в жителя и, наконец, в полноценного гражданина совершенно другой страны, в которой иной язык, иные нравы и обычаи, иные законы. Собственно, это не одна страна, а некое неограниченное множество «стран», уместяющихся в глобальном киберпространстве.

О ТРАНСГРАНИЧНОСТИ И ТЕХНОЛОГИЧЕСКОМ ЕДИНСТВЕ КИБЕРПРОСТРАНСТВА

Пока глобальное управление Интернетом ограничивается преимущественно унификацией технологических решений, связанных с использованием общих протоколов и т.п., есть уникальная возможность достаточно сво-

³ Тедеев А. А. Теоретические основы правового регулирования информационных отношений, формирующихся в процессе использования глобальных компьютерных сетей : автореф. дис. ... д-ра юрид. наук. М., 2007. С. 31.

⁴ Вопрос о пределах адаптации современного правового инструментария к реалиям информационного общества впервые рассмотрен нами на примере законодательства об авторском праве в статье: Cyberspace as an area of law // Copyright bulletin. UNESCO. 1998. Vol. XXXII. № 2.

⁵ Putnam R. D., Feldstein L. M. and Cohen D. Better Together: Restoring the American Community. — NY. : Simon & Schuster Paperbacks, 2004.

бодного формирования в нем своеобразных «киберстран», представляющих собой относительно устойчивые сообщества субъектов информационного взаимодействия. Причем это взаимодействие дифференцируется в рамках коммуникационного сообщества в очень широких пределах — от предоставления доступа неограниченному кругу посетителей к информации на том или ином интернет-ресурсе до совместного информационного действия тысяч и миллионов индивидуальных участников. В свою очередь, это совместное действие может выражаться в творческом акте, в коллективном протесте, в волеизъявлении на выборах и референдумах, в организации массовых беспорядков и т.д.

Сеть стимулирует появление новой ментальности, характерной для нарождающихся коммуникационных сообществ (интернет-сообществ) и опирающейся на объективные процессы расширения выбора во всех областях — от политики до стиля жизни, вытеснения иерархических организаций сетевыми, вытеснения представительной демократии демократией непосредственного участия, прямого гражданского действия или даже «облачной демократией»⁶. В результате формируется мировоззренческая открытость, потребление все новой и новой информации становится насущной потребностью человека, а интерактивность дает ему средства для информационного действия, взаимодействия, противодействия.

Может показаться, что миллионы интернет-сайтов и тысячи больших и малых сетей образуют хаос. В каком-то смысле это действительно так, но именно из хаоса естественным путем рождается порядок как структура правил и система отношений между структурами. Внутри каждого коммуникационного сообщества постепенно, в процессе информационного взаимодействия субъектов вырабатываются общие для всех участников правила поведения. Если эти правила соответствуют ожиданиям субъектов, то появляется доверие внутри сообщества, которое можно определить как возникающее у членов сообщества ожидание того, что другие

его члены будут вести себя более или менее предсказуемо, честно и со вниманием к нуждам окружающих, в согласии с некоторыми общими нормами поведения⁷.

Подобный процесс формирования общих правил поведения был подробно проанализирован применительно к различным относительно замкнутым сообществам в работах французского исследователя Жана Карбонье⁸. Сейчас такие правила формируются в относительно замкнутых коммуникационных сообществах, самопроизвольно складывающихся вокруг лиц, инициатив или идей, вызывающих отклик у других участников информационного взаимодействия. Социальные сети и блогосфера создают лишь благоприятные технологические условия для формирования коммуникационных сообществ. Сами же сообщества существуют самостоятельно и без всякой связи друг с другом в различных социальных сетях, на отдельных интернет-ресурсах, предоставляющих хостинг, блогинг, другие сервисы и т.д.

Было бы ошибкой утверждать, что никаких общих для всех интернет-ресурсов правил не существует: они есть, но касаются преимущественно технологических аспектов использования киберпространства. Именно технологическое единство киберпространства, с одной стороны, и его трансграничность — с другой, создают максимально благоприятные условия для выработки и последующей генерализации универсальных правил поведения в цифровой среде.

Трансграничность является одной из существенных характеристик киберпространства, хотя само оно до сих пор не имеет общепризнанного юридического определения в отечественном законодательстве. В связи с этим все юридические конструкции, построенные на обыденном понимании сети Интернет и не имеющие легальных определений основных понятий, страдают очевидной юридической ущербностью. И только в гражданском законодательстве мы можем обнаружить формулу, в которой киберпространство определено имплицитно, через понятие «такого образа» доведения произведений до всеобщего све-

⁶ Руденко В. Н. Прямая демократия: модели правления, конституционно-правовые институты. Екатеринбург : УрО РАН, 2003 ; Волков Л., Крашенинников Ф. Облачная демократия. Екатеринбург, 2011. URL: <http://cdem.ru/> (дата обращения: 19.08.2011).

⁷ См.: Фукуяма Ф. Доверие: социальные добродетели и путь к процветанию. М. : АСТ; Ермак, 2004.

⁸ См.: Карбонье Ж. Юридическая социология. М. : Прогресс, 1986.

дения, при котором любой может получить доступ к произведениям «из любого места и в любое время по собственному выбору» (пп. 11 п. 2 ст. 1270 Гражданского кодекса РФ). Эта формула является почти дословным воспроизведением нормы, содержащейся в ст. 8 Договора Всемирной организации интеллектуальной собственности (ВОИС) по авторскому праву 1996 г.

Представляется, что отечественный законодатель опрометчиво воспроизвел это определение из Договора ВОИС в части IV ГК РФ, не заметив, что понятие «любое место» совершенно не соответствует природе Интернета как информационно-телекоммуникационной сети. С учетом сетевого характера киберпространства следует различать «любое место Сети» и «любое место вне Сети». Если содержащееся в ст. 8 Договора ВОИС определение Интернета применительно к любому месту Сети оказывается истинно, то применительно к любому месту вне Сети — ложно: пользователь, компьютер которого не подключен к сети Интернет, не может получить доступ к произведению, размещенному в сети Интернет. Точно так же пользователь, компьютер которого подключен к сети Интернет, не может получить доступ к произведению, которое не размещено в сети Интернет. Иными словами, формируя интернет-тезаурус, следует иметь в виду, что составляющие его понятия, будучи действительны для сети Интернет, могут потерять всякий смысл вне Сети.

Но для того, чтобы государство смогло выработать правовые нормы, способные работать в Сети, оно должно сначала найти себя в киберпространстве и определить, где здесь проходят границы его суверенитета и юрисдикции. Трансграничный Интернет не признает государственных границ. Государственный суверенитет не знает понятия киберпространства и не ощущает своих границ в этом — по выражению американского писателя-фантаста, автора знаменитой трилогии «Киберпространство» Уильяма Гибсона, — «пространстве, которого нет»⁹. В этом смысле государство и Интернет существуют как бы в параллельных мирах.

Согласно классическим представлениям о государстве и праве действие любой правовой нормы определяется в трех плоскостях: в пространстве, во времени и по кругу лиц. Специфика киберпространства заставляет пересмотреть этот подход, поскольку в интернет-среде понятие «пространство» лишается однозначной географической определенности, понятие «время» не привязано ни к какому часовому поясу, а понятие «круг лиц» оказывается включающим не физических и юридических лиц, а компьютеры и другие устройства, участвующие в сетевом взаимодействии и идентифицируемые по их IP-адресам и другим технологическим деталям.

В принципе, возможны разные подходы к решению проблемы действия правовых норм, а следовательно, и к определению границ государственного суверенитета, в киберпространстве¹⁰. Сугубо гипотетически возможно адаптировать существующую классическую доктрину, дополнив ее касающимися Интернета положениями, либо выработать для киберпространства принципиально иную доктрину. В любом случае, учитывая трансграничность Сети, эффективное решение может быть достигнуто только конвенциональным путем, о чем речь пойдет ниже.

Можно констатировать, что пока развитие механизмов правового регулирования киберпространства идет по первому пути, через модернизацию существующих механизмов. Так, определенный прогресс в решении проблемы действия правовой нормы по кругу лиц достигнут благодаря формированию законодательства об электронной цифровой подписи. Безусловно, возможность идентификации пользователя Сети при вступлении с ним в те или иные правоотношения крайне важна для целей их охраны, однако проблема до конца не решена, поскольку анонимность является таким же сущностным свойством Интернета, как и трансграничность. Это предопределено отмеченной выше особенностью информационного взаимодействия в киберпространстве, когда сведения производятся, обрабатываются и потребляются компьютерами и другими се-

⁹ Научно-фантастическая трилогия «Киберпространство» (Sprawl trilogy — англ.) включает романы «Нейромант», «Граф Зеро» и «Мона Лиза Овердрайв». См.: URL: <http://ebookbrowse.com/william-gibson-the-sprawl-trilogy-1-neuromancer-pdf-d12084294> (дата обращения: 20.07.2011).

¹⁰ См.: Тедеев А. А. Теоретические основы правового регулирования информационных отношений, формирующихся в глобальных компьютерных сетях : монография. М. : Манускрипт, 2007.

тевыми устройствами, тогда как использующие их люди могут оставаться неузнанными, в том числе скрываясь за своими сетевыми именами (никнами, от nicknames), аватарами и т.д. Установление по примеру некоторых авторитарных стран правила о возможности подключения человека к Сети лишь при предъявлении документа, удостоверяющего личность, ведет только к замедлению развития соответствующей страны, к ее выпадению из общего мирового процесса, но никак не стимулирует очищение киберпространства от всего того, что противоречит общепризнанным представлениям о правомерном и должном.

Неоднозначной представляется проблема определения для киберпространства правил действия правовой нормы по территории. Гипотетически возможна локализация юридического факта в Интернете с использованием самых разных критериев: доменной зоны, местонахождения компьютера пользователя, местонахождения сервера, гражданства пользователя — физического лица, национальной юрисдикции пользователя-организации и т.д. Например, некоторые развивающиеся страны исповедуют так называемый принцип мирового преследования, когда национальный уголовный закон подлежит применению за преступления, совершенные с использованием Интернета на любой территории и любым лицом, если только это не будет пресечено юрисдикцией иностранного государства. Оптимальность такого подхода представляется сомнительной, особенно если попытаться распространить его на другие отрасли современного права и учесть объективные процессы дальнейшей глобализации мировых экономических, социальных, гуманитарных и иных отношений.

В частности, рассматривая дела, связанные с защитой интеллектуальной собственности в киберпространстве, судам все чаще приходится решать вопрос о том, какие законы и каким образом следует применить к юридическим фактам, возникшим в результате размещения произведений в глобальной сети. Чтобы проиллюстрировать эту проблему, представим, что некая студия раскрашивает черно-белый художественный фильм, размещает его на своем сайте и затем открывает к нему платный доступ через Интернет. Пользователи по всему миру теперь могут загрузить, переписать цветную версию фильма в цифровой форме на свои персональные компьютеры, оплатив доступ к ней по кредитной карточке. При этом в од-

них странах этот фильм уже находится в общественном достоянии, в других авторские права могут продолжать действовать, в третьих бесспорно действует право на неприкосновенность произведения, а колоризация фильма может рассматриваться как его искажение. Как в подобной ситуации правообладателю защитить свои права, запретив доступ к цветной версии фильма?

Подобный правовой конфликт уже известен в практике спутникового вещания. Но полной аналогии здесь быть не может: вещание предполагает наличие активных передающих центров, разбросанных в географическом пространстве, и пассивных получателей информации. Здесь суд как правоприменитель находится перед выбором между законодательством передающей и принимающей передачу страны.

Но, в отличие от вещания, в киберпространстве передающие и принимающие стороны взаимодействуют по Сети через десятки тысяч километров, мгновенно меняясь ролями. При этом число принимающих пользователей неопределенно и ограничено лишь общим количеством пользователей Сети, а место нахождения передающей стороны может не иметь географических координат. Как в такой ситуации должен действовать суд? Чье законодательство должно быть применено?

Как правило, в делах по защите авторских прав международные конвенции и договоры, начиная с Бернской конвенции об охране литературных и художественных произведений, предусматривают национальный режим. Этот принцип требует, чтобы суды применяли законодательство того государства, где испрашивается охрана, т.е., собственно, того, где произошло нарушение авторского права. Тот факт, что глобальная сеть Интернет имеет пользователей практически во всех странах мира, создает гипотетическую возможность обращения за судебной защитой нарушенного права едва ли не в любой стране. Но сумеет ли суд добиться исполнения своего решения в той стране, где находится сам нарушитель?

В XIX веке Фридрих Карл Савиньи проводил различие между специальным судебным законодательством, мотивированным общественными интересами, и гражданским законодательством, руководствующимся исключительно частными интересами. С одной стороны, государство, в силу существования общественных интересов, может запретить, например, труд детей, даже по договорам, за-

ключенным в другом государстве и разрешающим такой труд; с другой стороны, частные лица вступают в отношения, определяемые законодательством о собственности, договорным правом и гражданско-правовым деликтом. Савиньи соотносил эти отношения с законодательствами, разработанными для разных государств: например, недвижимость должна подчиняться законодательству того государства, на территории которого она находится¹¹. И это логично: недвижимость всегда находится на той или иной территории, она всегда локализована. Напротив, информация в киберпространстве постоянно движется.

Теоретически международные инструменты, касающиеся авторского права и смежных прав, охраняют любые произведения, которые потенциально могут находиться в данный момент в любой точке мира. Практически же правоприменитель, как правило, имеет дело с материальными предметами, находящимися на территории соответствующего государства: книгами, компакт-дисками, архитектурными проектами и т.д. Однако в информационно-коммуникационной сети пользователь может легко трансформировать практически любой объект авторских и смежных прав, сменив его материальную форму на нематериальную, например скопировав на жесткий диск своего персонального компьютера компакт-диск с фонограммой исполнения и разместив его на общедоступном сайте, открывая тем самым доступ к нему для пользователей, находящихся в других местах географического пространства.

В нашем гипотетическом примере владельцы исключительных прав на черно-белый фильм подают иск в суд по месту нахождения студии, требуя запретить ей использовать цветную версию фильма и возместить ущерб. Студия, естественно, настаивает на том, что по национальному законодательству об авторском праве срок охраны данного фильма уже истек и, следовательно, ни о каких санкциях речи быть не может. Правообладатели, напротив, утверждают, что раз конечные пользователи могут распоряжаться произведением в странах, где интеллектуальные права на этот фильм еще охраняются, то следует применять законодательство именно этих стран.

Будучи фактически брошен в киберпространстве на произвол судьбы, суд может при принятии решения отдать предпочтение тому закону, который наиболее благоприятен для потерпевшей стороны, поскольку правонарушение было совершено одновременно во многих странах. Но в таком случае суду придется учесть следующее.

Во-первых, стопроцентно эффективного решения суд в данном деле принять не сможет, поскольку специфика интернет-технологий не создает условий для его повсеместной, тотальной реализации. Более того, как отмечает профессор права Стэнфордского университета, руководитель Центра «Интернет и общество» (Center for Internet and Society) и основатель системы «Creative Commons» Лоуренс Лессиг (Lawrence Lessig), «пиринговый (p2p) файлообмен — одна из самых действенных интернет-технологий. Используя распределенные сети, системы p2p способствуют легкому распространению контента, немыслимому всего лишь поколение назад»¹².

Во-вторых, отчасти эффективным может быть судебное решение, обязывающее студию и/или хостинг-провайдера, находящихся под юрисдикцией национального суда, убрать цветную версию фильма с соответствующего интернет-ресурса и/или запретить доступ к нему пользователей «из любого места и в любое время по их собственному выбору».

В-третьих, не будем забывать: то, что в одних странах является правонарушением, не считается таковым в других странах, а значит, наложение требуемого истцами запрета в отношении доступа пользователей к цветной версии фильма «из любого места и в любое время по их собственному выбору» будет столь же законным и обоснованным в отношении пользователей в одних странах, сколь незаконным, необоснованным, ущемляющим права и законные интересы — в других.

В-четвертых, никакое судебное распоряжение, основанное на законодательстве одной страны, не сможет приостановить получение доступа к произведению пользователями в других странах, в том числе потому, что любая информация, единожды попавшая в Интернет, уже никуда не пропадает, а копируется и индексируется.

¹¹ См.: Новгородцев П. И. Историческая школа юристов. М., 1896.

¹² Лессиг Л. Свободная культура. Как медиаконцерны используют технологии и законы для того, чтобы душировать культуру и контролировать творчество : пер. с англ. М. : Прагматика Культуры, 2007. С. 45.

В-пятых, обосновав свой запрет нормами законодательств иностранных государств, суд может обязать студию прекратить доступ пользователей к цветной версии фильма на территориях этих стран. Однако и такое судебное решение в киберпространстве практически неисполнимо, в том числе потому, что здесь нет, во всяком случае — пока нет, ничьей национальной территории.

Подчеркнем, что киберпространство постоянно задает все новые и новые вопросы, касающиеся охраны интеллектуальной собственности, а предлагаемые законодателями-традиционалистами ответы, будучи выдержаны в привычной логике разрешений и запретов, с одной стороны, порождают массовое, тотальное нарушение установленного правового порядка, а с другой — способствуют накоплению в нем внутренних логических противоречий. Так, ответом мирового авторско-правового сообщества на бездоговорное размещение охраняемых произведений в Интернете стала упоминавшаяся выше статья 8 Договора ВОИС по авторскому праву 1996 г., предусматривавшая за автором исключительное право на «доведение своих произведений до всеобщего сведения таким образом, что представители публики могут осуществлять доступ к таким произведениям из любого места и в любое время по их собственному выбору».

Однако такое право имплицитно уже содержалось в положениях статей 11 (1) «ii», 11bis (1) «i» и «ii», 11ter (1) «ii», 14 (1) «ii» и 14bis (1) Бернской конвенции, поскольку в этих правовых нормах говорилось об исключительном праве автора разрешать «сообщение для всеобщего сведения любыми средствами» или «любым другим способом беспроводной передачи знаков, звуков или изображений» и т.д.

Видимо, чтобы предотвратить удвоение правового регулирования, Договор ВОИС использует формулу «без ущерба положениям» перечисленных выше статей. Но в таком случае данная формула как раз означает, что преду-

смотренное статьей 8 Договора ВОИС исключительное право не является изъятием из указанных выше общих правил Бернской конвенции, а следовательно, дублирует их применительно к киберпространству. Гораздо логичнее было бы применить формулу «в изъятие из положений». Но она означала бы исключение киберпространства из общих правил Бернской конвенции, а именно этого создатели Договора ВОИС всячески стремились избежать.

Более того, выше мы уже обращали внимание на некоторое несовершенство определения права на доведение до всеобщего сведения, связанное с неопределенностью понятия «любое место». По нашему мнению, оно имеет еще один недостаток, связанный с тем, что автор, единожды воспользовавшийся правом разрешить доведение своего произведения до всеобщего сведения, далее неминуемо сталкивается с тем, что представители публики могут осуществлять доступ к такому произведению не только из любого места Сети, но и в любом месте Сети.

Обратим внимание на то, что правовая позиция Верховного Суда РФ в этом вопросе выглядит достаточно осторожной. Во-первых, размещение объектов авторских и смежных прав в информационно-телекоммуникационных сетях толкуется высшей судебной инстанцией судов общей юрисдикции как использование данных объектов. Во-вторых, запись произведения или объекта смежных прав в память компьютера является использованием этого объекта, если по инициативе лица, совершившего запись, неопределенный круг лиц получает доступ к этому объекту. В-третьих, полученные в результате такого использования экземпляры объектов являются контрафактными. В-четвертых, лица, осуществившие подобные действия, признаются нарушителями авторских или смежных прав. К указанным лицам могут быть отнесены, в частности, владельцы сайта, на котором были размещены контрафактные произведения или объекты смежных прав¹³.

¹³ См.: п. 25 постановления Пленума Верховного Суда РФ от 19.06.2006 № 15 «О вопросах, возникших у судов при рассмотрении гражданских дел, связанных с применением законодательства об авторском праве и смежных правах» // Бюллетень ВС РФ. 2006. № 8.

Аналогичным образом рассматривается неправомерное размещение произведения в сети Интернет как нарушение исключительного права на произведение и в п. 34 постановления Пленума Верховного Суда РФ № 5 и Пленума ВАС РФ № 29 от 26.03.2009 «О некоторых вопросах, возникших в связи с введением в действие части четвертой Гражданского кодекса Российской Федерации» // Бюллетень ВС РФ. 2009. № 6.

При этом, очевидно, Верховный Суд РФ презюмирует, что лицо, разместившее объект интеллектуальной собственности в Интернете, не является автором или иным правообладателем, поскольку нет никаких правовых оснований лишать правообладателя юридической возможности довести объект своих интеллектуальных прав до всеобщего сведения.

Представляется, что право на доведение до всеобщего сведения, входящее в комплекс правомочий исключительного права на произведение (пп. 11 п. 2 ст. 1270 ГК РФ), схоже с правом на обнародование произведения (ст. 1268 ГК РФ). Если произведение не было обнародовано ранее, то его первое размещение в сети Интернет, т.е. доведение до всеобщего сведения, должно считаться формой обнародования, поскольку п. 1 ст. 1268 ГК РФ содержит открытый перечень способов обнародования, понимая его как действие, которое впервые делает произведение доступным для всеобщего сведения «любым способом».

С момента обнародования произведения наступает исчерпание права на обнародование, которое в реальности не может изменить даже право на отзыв произведения (ст. 1269 ГК РФ) — этот абсолютный анахронизм, предоставляющий автору право изъять из обращения ранее выпущенные экземпляры произведения, возместив причиненные этим убытки. Естественно, право на отзыв совершенно нереально в условиях киберпространства, что, однако, проигнорировано Гражданским кодексом, предусмотревшим изъятия только в отношении программ для ЭВМ, служебных произведений и произведений, вошедших в сложный объект.

Рассматривая доведение до всеобщего сведения как разновидность обнародования произведения, легко понять исчерпаемость права на доведение до всеобщего сведения. Как писатель теряет контроль над своей книгой, разошедшейся многотысячным тиражом, так и автор, разместивший свое произведение в киберпространстве, утрачивает далее контроль над каждой копией. При всем желании он не в состоянии изъять из обращения все копии своего произведения, тем более что цифровая копия неотличима от цифрового оригинала, и в этом смысле копия имеет столько же оснований считаться оригиналом, сколько

оригинал — копией. Не желая видеть реальность виртуального мира, законодатель рискует остаться в куда более оторванном от жизни мире собственных логических конструкций.

О ПЕРСПЕКТИВАХ МЕЖДУНАРОДНОГО РЕГУЛИРОВАНИЯ В КИБЕРПРОСТРАНСТВЕ

Даже достаточно простой приведенный выше пример ясно показывает, сколь важно двигаться к выработке общих международных правил регулирования деятельности в киберпространстве. Необходима скорейшая разработка международной конвенции, которая бы, во-первых, установила зоны национальной юрисдикции в Интернете по аналогии, например, с Арктикой; во-вторых, установила общие правила локализации норм национального законодательства в киберпространстве, в том числе во времени и по кругу лиц; в-третьих, признала право каждого на доступ к киберпространству в качестве одного из прав человека; в-четвертых, установила правила соблюдения в Интернете международных конвенций о правах человека, а также других международных конвенций.

Думается, что опыт формирования международного космического права был бы весьма полезен в качестве образца при создании актов международного права, призванных регулировать деятельность в киберпространстве. Главным постулатом формируемого таким образом International Cyberspace Law (ICL) должно стать: то, что наказуемо вне Сети (offline), должно быть наказуемо и в Сети (online). Только в этом случае ICL не окажется построенным на принципах, противоположных тем, что складывались в юридической теории и практике многие тысячелетия.

В этом смысле показателен пример Конвенции о киберпреступности, заключенной в Будапеште 23 ноября 2001 г. В 2005 г. по предложению МИД России, согласованному с Минюстом России, МВД России, Мининформсвязи России, ФСБ России, СВР России и Генеральной прокуратурой РФ, наша страна присоединилась к этой Конвенции путем ее подписания¹⁴. При этом Россия сделала, в частности, следующее заявление: «Российская Федерация исходит из

¹⁴ Распоряжение Президента РФ от 15.11.2005 № 557-рп «О подписании Конвенции о киберпреступности» // СЗ РФ. 2005. № 47. Ст. 4929.

того, что положения пункта “b” статьи 32 Конвенции сформулированы таким образом, что не исключается возможность такого их толкования и применения, которые не соответствуют, в частности, целям и принципам, изложенным в абзацах девятом и десятом преамбулы Конвенции, и могут нанести ущерб суверенитету и национальной безопасности государств-участников, правам и законным интересам их граждан и юридических лиц.

В связи с изложенным Российская Федерация определится в вопросе о своем участии в Конвенции при условии возможного пересмотра положений пункта “b” статьи 32 в порядке, предусмотренном пунктом 3 статьи 46 Конвенции, либо в ином порядке, избранном Сторонами.

Российская Федерация выражает готовность к сотрудничеству с государствами — членами Совета Европы и иными подписавшими Конвенцию государствами в решении данной проблемы на основе уважения и соблюдения целей и принципов Конвенции».

Судя по всему, российская инициатива не встретила понимания со стороны других участников Конвенции. Во всяком случае, проблемный пункт «b» статьи 32 Конвенции на момент написания данной статьи сохранился в неизменном виде, а Российская Федерация в 2008 г. вышла из Конвенции путем признания прежнего президентского поручения утратившим силу¹⁵.

Попробуем разобраться, что же в содержании ставшего камнем преткновения пункта могло «нанести ущерб суверенитету и национальной безопасности государств-участников, правам и законным интересам их граждан и юридических лиц».

Статья 32 Конвенции говорит о трансграничном доступе к хранящимся компьютерным данным с соответствующего согласия или к общедоступным данным. Согласно пункту «a» государство-участник может без согласия другого государства-участника «получать доступ к общедоступным (открытому источнику) компьютерным данным независимо от их географического местоположения». Представляется,

что данная норма вообще никакого правила не устанавливает, а лишь констатирует трансграничный характер киберпространства. Неудивительно, что она не вызвала никаких нареканий, хотя Федеральный закон от 04.07.1996 № 85-ФЗ «Об участии в международном информационном обмене»¹⁶ устанавливал достаточно много ограничений для трансграничного информационного взаимодействия и, в частности, предусматривал государственный контроль над осуществлением международного информационного обмена.

Пресловутый пункт «b» статьи 32 Конвенции предоставлял государству-участнику право без согласия другого государства-участника «получать через компьютерную систему на своей территории доступ к хранящимся на территории другой Стороны компьютерным данным или получать их, если эта Сторона имеет законное и добровольное согласие лица, которое имеет законные полномочия раскрывать эти данные этой Стороне через такую компьютерную систему».

Если сопоставить это положение с нормами российского информационного законодательства, то никакого противоречия не усматривается. Даже согласно статье 12 Федерального закона «Об участии в международном информационном обмене» доступ «к средствам международного информационного обмена и иностранным информационным продуктам осуществляется по правилам, установленным собственником или владельцем этих средств и продуктов в соответствии с законодательством Российской Федерации». В свою очередь, собственник (владелец) обязан обеспечить открытость установленных им правил доступа и возможность ознакомления с ними пользователя, а отказ в доступе может быть обжалован в суд либо в международный коммерческий арбитраж.

Представляется, что спорный пункт Конвенции вполне соотнобразуется и с полномочиями обладателя информации, как они определены в ст. 6 Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации». Именно

¹⁵ Распоряжение Президента РФ от 22.03.2008 № 144-рп «О признании утратившим силу распоряжения Президента Российской Федерации от 15 ноября 2005 г. № 557-рп “О подписании Конвенции о киберпреступности”».

¹⁶ Закон утратил силу в связи с принятием Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации».

обладатель информации вправе: разрешать или ограничивать доступ к информации, определять порядок и условия такого доступа; использовать информацию, в том числе распространять ее, по своему усмотрению; передавать информацию другим лицам по договору или на ином установленном законом основании; осуществлять иные действия с информацией или разрешать осуществление таких действий. Одновременно с этим обладатель информации обязан при осуществлении своих прав: соблюдать права и законные интересы иных лиц; ограничивать доступ к информации, если такая обязанность установлена федеральными законами. Следовательно, обладатель информации имеет право по своему усмотрению предоставлять доступ любому третьему лицу к имеющейся у него информации, в том числе через информационно-коммуникационную сеть, за исключением случаев, когда предоставление такой информации запрещено или ограничено федеральными законами, либо, напротив, является для обладателя информации обязательным.

Все это свидетельствует о необходимости вернуться к обсуждению вопроса об участии Российской Федерации в Конвенции о киберпреступности, тем более что на сегодняшний день к ней присоединились уже 47 стран, включая почти все страны — члены Совета Европы, а также Канаду, США, ЮАР, Японию. Правда, вопрос о причинах, побудивших три малые европейские страны, а именно Андорру, Монако и Сан-Марино уклониться от участия в Конвенции, требует дополнительного изучения, как, собственно, и причины выхода из нее нашей страны. В целом же история с присоединением Российской Федерации к Конвенции о киберпреступности и последующим выходом из нее подтверждает справедливость пессимистического вывода А. А. Тедеева, что «до настоящего времени международных договоров, направленных на регулирование каких-либо аспектов общественных отношений, формирующихся в процессе использования глобальных компьютерных сетей, Российской Федерацией не заключалось, и заключение их в будущем не планируется»¹⁷.

ОБ ОПАСНОСТИ СЕГМЕНТИРОВАНИЯ КИБЕРПРОСТРАНСТВА

Следует отметить, что трансграничность Интернета имеет пределы. Есть страны, в которых доступ граждан к Интернету запрещен (например, Северная Корея, Республика Куба и т.д.). В некоторых других странах доступ к Интернету строго цензурируется. Опасность дальнейшего ограничения глобальности киберпространства может таиться и в сегментировании Интернета через введение национальных доменных зон, строго привязанных к соответствующим государствам. Первые шаги в этом направлении уже сделаны — с согласия Корпорации по управлению доменными именами и IP-адресами (Internet Corporation for Assigned Names and Numbers, ICANN) и при большой заинтересованности некоторых правительств и их национальных регистраторов доменных имен.

Так, с октября 2007 г. ICANN начала тестирование IDN-доменов (Internationalized Domain Names) верхнего уровня на 11 национальных языках, среди которых есть и русский. На конференции ICANN в июне 2008 г. было принято решение о введении ряда доменных зон на национальных языках по ускоренной процедуре (Fast Track), а в ноябре 2008 г. российский Координационный центр национального домена сети Интернет¹⁸ подал заявку на делегирование нашей стране домена верхнего уровня «.рф». Россия стала одной из первых стран, которая получила собственную нелатинскую доменную зону. Приоритетная регистрация доменных имен в зоне «.рф» началась 25 ноября 2009 г., а техническое включение российского кириллического домена состоялось 13 мая 2010 г.

Примерно в это же время в средствах массовой информации стал дебатироваться вопрос о необходимости создания единой государственной поисковой системы, которая могла бы не только конкурировать с успешно работающими в Рунете поисковиками, но и помочь решить некоторые из проблем, отмеченных в Федеральной целевой программе «Электронная Россия». Среди этих проблем назывались, в частности, следующие: «Различные форматы хранения данных ограничивают

¹⁷ Тедеев А. А. Теоретические основы правового регулирования информационных отношений, формирующихся в процессе использования глобальных компьютерных сетей : автореф. дис. ... д-ра юрид. наук. С. 40.

¹⁸ URL: <http://www.cctld.ru/>.

возможность применения автоматизированных средств поиска и аналитической обработки информации, содержащейся в различных системах. <...> Неконтролируемый рост объема информации о гражданах, организациях и объектах хозяйственного оборота, содержащейся в государственных информационных системах, в условиях отсутствия эффективных механизмов контроля ее использования создает также угрозу нарушения прав граждан. Проблема отсутствия унифицированной инфраструктуры, типовых решений и стандартов в области обмена данными в электронном виде на межведомственном уровне, а также с населением и организациями становится особенно актуальной по мере дальнейшего развития государственных информационных систем и проникновения информационных и телекоммуникационных технологий в социально-экономическую сферу»¹⁹.

Нельзя не заметить, что создание национальной доменной зоны и государственной поисковой системы может интерпретироваться и как подготовительные шаги к отделению Рунета, который в равной мере может интерпретироваться сегодня и как доменная зона «.ru», и как совокупность русскоязычных интернет-ресурсов, от общей среды глобального киберпространства. Наличие национальной доменной зоны позволяет в принципе объявить эту зону находящейся под государственным суверенитетом Российской Федерации и тем самым открыть путь для установления законов, регулирующих деятельность в этой зоне. Одним из таких законов может быть установлен, например, запрет на доступ с территории Российской Федерации к интернет-ресурсам, расположенным в других доменных зонах, запрет на использование иностранных поисковых систем и т.д.

Конечно, такой катастрофический сценарий может реализоваться только как часть общего изоляционистского тренда, признаки которого пока не просматриваются. Напротив, сторонники кириллического домена верхнего уровня указывают, что их планы вовсе не предопределены изоляционистскими настроениями: введение кириллических доменов, утверждали они на торжественной церемонии открытия зоны «.рф», сделает доступными для регистрации миллионы уникальных имен, которые

сегодня заняты, откроет сокровища русской культуры для иностранной аудитории, будет способствовать утверждению России как мировой интернет-державы и т.п. «Мы рассчитываем, — заявил 14 мая 2010 г. министр связи и массовых коммуникаций РФ И. О. Щеголев в рамках международной выставки «Связь-Экспокомм — 2010», — что наиболее популярные ресурсы создадут в зоне «.рф» свои зеркала, прежде всего для тех пользователей, которые свободно не владеют английским языком. Со временем, я думаю, кириллическая зона будет развиваться и предоставлять самостоятельный продукт». Так, Минкомсвязи России намерено создать в этой зоне государственную электронную почту для общения граждан с государством.

Можно согласиться с А. Г. Серго, что появление кириллической доменной зоны имеет целый ряд недостатков. Во-первых, домены в зоне «.рф» останутся недоступными для иностранных пользователей Интернета, не имеющих кириллической клавиатуры. Во-вторых, дополнительные проблемы появятся даже у пользователей Интернета в других странах, использующих кириллицу (Беларусь, Болгария, Сербия, Украина и др.), поскольку их алфавит содержит не все буквы русского языка. В-третьих, не избавит переход на кириллицу и от необходимости набирать «http://» и «www» в строке адреса, а значит, дополнительно переключать клавиатуру. В-четвертых, не будем сбрасывать со счетов и то, что пока не решена проблема написания **адресов электронной почты** на кириллице. В-пятых, появление **национальной доменной зоны не только не устраняет опасность спама, фишинга и киберсквоттинга, а, наоборот, расширяет поле деятельности сетевых мошенников.**

Примем во внимание, что доменные зоны на национальных языках появились не только в нашей стране. Одновременно с Россией домены верхнего уровня на национальных языках получили Объединенные Арабские Эмираты, Египет и Саудовская Аравия. Если этот процесс пойдет дальше и будет сопровождаться описанными выше изоляционистскими мерами, то неминуем распад глобального «мирового интернет-океана» на локальные «интернет-пруды», в каждом из которых будут свои правила

¹⁹ Постановление Правительства РФ от 28.01.2002 № 65 (в ред. от 09.06.2010) «О федеральной целевой программе “Электронная Россия (2002–2010 годы)”».

регулирования. Тем самым мировое сообщество рискует вернуться к состоянию коммуникационной раздробленности, впервые в истории преодоленному в последней четверти XX века именно благодаря новым информационно-коммуникационным технологиям.

О КОНСТИТУЦИОННЫХ ОРИЕНТИРАХ РЕГУЛИРОВАНИЯ ДЕЯТЕЛЬНОСТИ В КИБЕРПРОСТРАНСТВЕ

Хотя Конституция Российской Федерации принята сравнительно недавно, быстро меняющиеся реалии информационного общества уже превратили ее в Основной Закон прошлого века, ибо в ней крайне скудно представлены основополагающие принципы информационного права как права киберпространства, Cyberspace Law. Достаточно провести элементарный частотный анализ текста Конституции Российской Федерации 1993 г., чтобы убедиться в том, что информационные отношения затрагиваются в конституционных нормах в два раза реже, чем отношения, связанные, например, с природопользованием. Характерно, что интеллектуальная собственность, этот локомотив мирового прогресса в XXI веке, упоминается только в двух статьях — 44, 71 — Конституции РФ, а слово «знание» не использовано ни разу. И это при том, что сегодня человеческая цивилизация переживает поистине революционные преобразования, связанные с формированием экономики, основанной на знании, т.е. на информации и интеллектуальной собственности.

Действующая российская Конституция дает лишь некоторые ориентиры для правового регулирования информационных отношений. Вкратце перечислим эти ориентиры. Во-первых, запрещение собирать, хранить, использовать и распространять информацию

о частной жизни лица без его согласия (ст. 24, ч. 1). Во-вторых, право каждого свободно искать, получать, передавать, производить и распространять информацию любым законным способом (ст. 29, ч. 4). В-третьих, свобода массовой информации (ст. 29, ч. 5). В-четвертых, право каждого на достоверную информацию о состоянии окружающей среды (ст. 42). Наконец, в-пятых, Конституция (ст. 71, п. «и») относит к ведению Российской Федерации так называемые «федеральные информация и связь», порождая максимально возможную неопределенность в вопросе о том, существуют ли «нефедеральная информация» и имеют ли субъекты Федерации хоть какую-то компетенцию в сфере информации²⁰.

Если абстрагироваться от историко-правовых аспектов развития доктрины прав человека и принять во внимание лишь чисто технологические аспекты реализации перечисленных конституционных ориентиров, то можно увидеть, что они вполне применимы не только к XX, но и к XIX веку. Но отвечают ли они требованиям современного информационного общества? Могут ли они стать мостиком между International Cyberspace Law и текущим российским законодательством?

Несколько лет назад вместе с профессором М. А. Красновым мы попытались разработать комплексные предложения по реформе Конституции 1993 г.²¹ В качестве одного из направлений реформы — сразу скажем, весьма и весьма скромной — мы взяли закрепление некоторых норм, которые могут понадобиться по мере продвижения России в новое информационно-цивилизационное пространство.

Во-первых, мы посчитали важным в ст. 3 Конституции РФ указать, что помимо референдума и выборов законом могут устанавливаться также иные формы прямого народного волеизъявления. Например, волеизъявление через Интер-

²⁰ При обсуждении вопроса о компетенции субъектов Российской Федерации в сфере массовой информации в ходе подготовки постановления Пленума Верховного Суда РФ № 16 от 15.06.2010 «О практике применения судами Закона Российской Федерации «О средствах массовой информации»» камнем преткновения стали частично совпадающие пункт «в» статьи 71 и пункт «б» статьи 72 Конституции РФ, а также конституционная формулировка «федеральные... информация и связь», крайне неудачная в смысле выявления ее юридического смысла. В конечном итоге было решено, что правовое регулирование отношений, касающихся свободы массовой информации, осуществляется федеральными законами — далее следует их не исчерпывающий перечень, — «а также иными нормативными правовыми актами, принимаемыми в установленном порядке». Эта формулировка хороша тем, что сторонники обеих позиций могут толковать ее как подтверждение своей правоты. Но этим же она и плоха.

²¹ См.: Конституционное обустройство России: общественная экспертиза. М.: Грааль. 2000.

нет. Нечто подобное существует уже не первый год в некоторых графствах США, в Японии, других странах. С появлением облачных технологий появляются дополнительные возможности совершенствования механизмов демократии прямого гражданского участия — через углубление транспарентности государственного механизма, формирование систем дистанционного общественного контроля и гражданского участия в управлении делами государства.

Во-вторых, мы предложили в ч. 1 ст. 8 Конституции РФ гарантировать единство не только экономического, но и информационного пространства, свободное перемещение не только товаров, услуг, но и информации.

В-третьих, ч. 3 ст. 15 мы предложили дополнить словами о том, что законы должны быть доступны каждому, в том числе через информационно-телекоммуникационные сети. Аналогичные нормы следовало бы включить в ст. 90 в отношении актов Президента РФ и в ст. 100 — в отношении стенограмм и актов палат парламента. На сегодня отсутствие этих норм приводит к тому, что самый удобный способ доступа к законодательным базам данных, а именно дистанционный, оказывается почти исключительно платным. Кстати, в Республике Беларусь доступ к правовым базам Национального центра правовой информации является бесплатным для любого пользователя сети Интернет. Нельзя в этой связи не упомянуть правовые базы «КонсультантПлюс», бесплатный доступ к которым открыт для многих преподавателей и ученых-юристов.

В-четвертых, мы предложили распространить тайну переписки (ст. 23) на информационно-телекоммуникационные сети. Очевидно, что в отношении общения по электронной почте должна быть гарантирована такая же защита конфиденциальности, как и в отношении традиционных средств связи. Более того, необходимо защитить и тайну поиска и получения информации в Интернете при посещении тех или иных веб-сайтов. Тем более что сегодня технологии позволяют отслеживать посещение сайтов и соответствующим образом профилировать рекламу, которая предлагается пользователю.

В-пятых, мы предложили дополнить ст. 24 новой частью, содержащей прямой запрет органам государственной власти и органам местного самоуправления собирать, получать и предоставлять информацию о гражданах, в том числе через информационно-телекоммуникационные сети, за исключением той, которая необходима в демократическом правовом государстве и предусмотрена федеральным законом.

В-шестых, мы предложили дополнить ст. 31 Конституции РФ новой частью следующего содержания: «В случаях и порядке, предусмотренных законом, граждане могут участвовать в управлении делами государства, в том числе в выборах своих представителей, через информационно-телекоммуникационные сети».

В-седьмых, мы посчитали важным дополнить ст. 33 указанием на право граждан обращаться в государственные органы и органы местного самоуправления через информационно-телекоммуникационные сети.

В-восьмых, мы предложили в ст. 123 зафиксировать важную гарантию гласности и открытости правосудия, а именно: решение суда во всех случаях оглашается публично и должно быть доступно каждому, в том числе через информационно-телекоммуникационные сети²².

Наконец, в-девятых, Конституция должна гарантировать каждому свободный доступ к информационно-телекоммуникационным сетям общего пользования, к Интернету. Это позволит положить конец многочисленным политическим спекуляциям вокруг вопроса об обязательной регистрации всех пользователей Сети, всех сайтов, всех компьютеров и т.д.

Разумеется, всего этого явно недостаточно для того, чтобы адаптировать Конституцию РФ к реалиям информационного общества, а значит, заложить конституционные основы информационного права нового типа. Отсюда, однако, не следует, что необходима немедленная конституционная реформа. Напротив, мне представляется, что Конституция РФ 1993 года еще далеко не исчерпала свой потенциал: она нуждается скорее в неукоснительном соблюдении, нежели в реформировании.

²² Некоторые из этих предложений получили развитие в федеральных законах о доступе к информации, принятых в конце 2000-х гг.: в Федеральном законе от 09.02.2009 № 8-ФЗ «Об обеспечении доступа к информации о деятельности государственных органов и органов местного самоуправления» и Федеральном законе от 22.12.2008 № 262-ФЗ «Об обеспечении доступа к информации о деятельности судов в Российской Федерации».

Более того, некоторые из перечисленных выше идей вполне могут быть реализованы на уровне текущего законодательства путем включения соответствующих положений в Федеральный закон «Об информации, информационных технологиях и о защите информации», который призван быть структурообразующим нормативным правовым актом в системе отечественного информационного права. К сожалению, указанный закон оказался мало приспособлен к выполнению этой роли, в результате чего российское информационное законодательство развивается достаточно медленно и бессистемно. Яркий пример — Федеральный закон «Об участии в международном информационном обмене», о котором можно сказать, что он пришел незванным и ушел неузнанным, так и не найдя себе применения на практике²³.

О САМОРЕГУЛИРОВАНИИ И ИНЫХ НЕПРАВОВЫХ ИНСТРУМЕНТАХ РЕГУЛИРОВАНИЯ В КИБЕРПРОСТРАНСТВЕ

Можно согласиться с выводом профессора Лоуренса Лессига, впервые сформулированным им в упомянутой выше статье «Читая Конституцию в киберпространстве», что киберпространство неминуемо будет регулироваться четырьмя социальными регуляторами: законом, этическими нормами, формируемыми интернет-сообществом, законами рыночной конкуренции и, наконец, программным кодом.

Выше мы подробно останавливались на проблемах, связанных с регулированием киберпространства посредством правовых норм. Здесь же сконцентрируем внимание на неправовых регуляторах. Одним из них является этическое саморегулирование. Если закон регулирует поведение лица через угрозу применения, например, штрафа, то сетевое саморегулирование, включающее и этикет (*netiquette*), — через угрозу децентрализованных санкций со стороны членов интернет-сообщества. Как показывает практика, подобное регулирование может быть весьма эффективным. Например,

по призыву одной из сетевых общественных организаций с веб-сайтов были добровольно убраны 26 тысяч изображений детской порнографии. На принципах саморегулирования основывается и функционирование третейских судов. Так, при Всемирной организации интеллектуальной собственности успешно функционирует третейский суд по доменным спорам.

Как отмечалось на конференции ЮНЕСКО по инфоэтике в 2005 г., важной тенденцией трансформации средств массовой информации в киберпространстве стало их превращение в интерактивные форумы, что предъявляет новые профессионально-этические требования к журналистам и редакторам. Профессиональным журналистам приходится брать во многом пример с блогеров, но при этом подтверждать документами свои информационные сообщения, чтобы аудитория могла сама решать — доверять предоставленной информации или нет. Так как граждане имеют более широкий спектр информации под рукой, уровень подтверждения в прессе должен вырасти соответственно. В свою очередь, это должно привести к тому, что журналисты, использующие Интернет, будут настолько прозрачны, насколько это возможно, что касается их источников и методов, а также будут обеспечивать широкую публику легко доступным массивом публикаций по важным темам, показывая, как с течением времени развивается их обращение со средствами информации. «Во все большей степени роль профессиональных журналистов, — отмечается в материалах ЮНЕСКО, — будет заключаться в выполнении функций медиатора, собирающего бесчисленные данные и мнения в заслуживающее доверия, многозначное целое, позволяющее сформировать квалифицированное мнение. В свою очередь, гражданское общество и общественные институты по всему миру должны потребовать от медиаструктур приверженности такому подходу, который является одновременно и реалистичным и жизненно необходимым для демократического процесса»²⁴.

Говоря о российском опыте саморегулирования в киберпространстве, подчеркнем прежде всего давность его истории. Первые шаги

²³ Федеральный закон от 04.07.1996 № 85-ФЗ «Об участии в международном информационном обмене» утратил силу в связи с принятием Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации».

²⁴ Программа ЮНЕСКО «Информация для всех». Отчет 2004—2005 гг. — М. : ЮНЕСКО, 2006. С. 55–56.

в этом направлении были сделаны в нашей стране еще 27 мая 1966 г., когда был принят Национальный кодекс деятельности в области информатики и телекоммуникаций²⁵. Подписавшие Кодекс советские организации приняли на себя обязательства не нарушать охрану интеллектуальной собственности и тайну передачи сообщений, не практиковать вскрытие информационных систем, не извлекать прибыль из использования чужого товарного знака и т.д.

Определенную роль в саморегулировании играют также средства альтернативного разрешения информационных споров: Третейский информационный суд при Президенте РФ (1993), Судебная палата по информационным спорам при Президенте РФ (1993–2000), Большое жюри Союза журналистов России (с 1998) и Общественная коллегия по жалобам на прессу (с 2005). В практике этих органов нередко встречаются споры, связанные с жалобами на материалы, размещенные в интернет-СМИ. Разрешая подобные споры, органы саморегулирования одновременно формулируют профессионально-этические нормы.

Например, Большое жюри СЖР в решении от 07.04.2003 № 26 «Об обращении театрального критика Н. С. Шехтер в связи с публикациями “‘Милый друг’ оказался вдруг” и “Скандал с ‘Милым другом’” в газетах “Комсомольская правда-на-Дону” и “Наше время”» обратило внимание на «необходимость особой осторожности при обращении журналиста к информации, циркулирующей в Интернете. Такая информация, особенно из неустановленных источников, может быть преднамеренно размещена в Сети, с одной стороны, с целью дальнейшего распространения ложных сведений через традиционные СМИ, а с другой стороны, с целью ухода недобросовестных авторов от ответственности»²⁶.

С учетом трансграничности и непосредственности Интернета саморегулирование способно вырасти в серьезное средство защиты интересов человека и общества в Сети. Однако для этого механизмы саморегулирования должны обрести доверие интернет-сообщества,

что, в свою очередь, будет определяться следующими обстоятельствами, сформулированными нами исходя из общих представлений социологической науки о природе общественного и индивидуального доверия к тем или иным институтам²⁷.

Во-первых, правила саморегулирования должны вырабатываться самим интернет-обществом, а не навязываться ему со стороны.

Во-вторых, важна нормативная определенность этических правил, их четкость, ясность, недвусмысленность, внутренняя согласованность, приемлемость, полнота.

В-третьих, должны быть обеспечены прозрачность и открытость механизмов саморегулирования, включая публичность разбирательств и доступность информации о материальных и процессуальных нормах его функционирования, принципах и правилах принятия решений.

В-четвертых, необходимы стабильность и эволюционный характер совершенствования механизмов саморегулирования, предсказуемость и постепенность вносимых перемен.

В-пятых, институты саморегулирования должны формироваться самим интернет-обществом, они должны быть ему подотчетны, открыты для общественного контроля.

В-шестых, должно быть обеспечено безусловное уважение прав и законных интересов всех участников процесса саморегулирования, защита их достоинства, неприкосновенности и автономности.

Наконец, в-седьмых, едва ли не важнейшим условием эффективности саморегулирования является уважение обязательств, принятых на себя участниками процесса саморегулирования по отношению друг к другу.

Хотя сетевая природа киберпространства благоприятствует становлению здесь механизмов этического саморегулирования, предшествующий негативный опыт, имеющийся, в частности, в нашей стране (товарищеские суды, заслушивание персональных дел на партийных собраниях и т.п.), препятствует формированию уважительного отношения к подобным механизмам.

²⁵ См.: Копылов В. А. Информационное право : учеб. пособие. М. : Юристъ, 1997. С. 306—308.

²⁶ См.: Настольная книга по медийному саморегулированию / под ред. д. ю. н., проф. М. А. Федотова. М. : Творческий центр ЮНЕСКО, 2009.

²⁷ Barber B. The Logic and Limits of Trust. New Brunswick, NJ : Rutgers University Press, 1983 ; Sztompka P. Trust: a Sociological Theory. Cambridge : Cambridge University Press, 1999.

Законы рыночной конкуренции также оказывают определенное регулятивное воздействие на киберпространство. В качестве примера можно сослаться на конкуренцию поисковых систем, браузеров, хостинг-провайдеров, регистраторов доменных имен и т.д. Рыночное регулирование осуществляется, в частности, через экономические условия доступа к Интернету и к определенным услугам в Сети.

Наконец, отметим чисто программные средства регулирования, когда роль правовой нормы берет на себя программный код. Это, по выражению Лоуренса Лессига, один из главных законов Интернета — тот самый код, который регулирует функционирование связанных между собой в киберпространстве компьютеров с помощью логических алгоритмов, фильтров, протоколов и т.п. Значение кода как механизма регулирования особенно велико, поскольку он позволяет лицам, не являющимся носителями власти, закреплять правила, влияющие не только на выбор информационных услуг, но и на поведение человека в киберпространстве в целом.

Функции кода в киберпространстве крайне разнообразны. Программные средства, например, ограничивают поведение пользователей наложением определенных условий, которые пользователи должны соблюдать, чтобы иметь возможность использовать диалоговый режим. Речь может идти, например, о требовании пароля доступа, о запрете анонимного посещения или множественности адресов электронной почты, о возможности шифрования, о допустимости фильтрации содержания, в частности со стороны родителей, и т.д. Всё это — примеры регулирования поведения людей с помощью кодов. Причем глобальный характер киберпространства предопределяет масштаб, который может приобрести проблема несовершенства программного кода.

В подтверждение этого тезиса сошлемся на пример, который Лоуренс Лессиг приводит в главе 17 своей, ставшей уже классической монографии «Код и другие законы киберпространства». Поскольку книга писалась в 1999 г., постольку естественно, что автор большое внимание уделяет «проблеме 2000 года» (Y2K), которая рассматривалась специалистами как реальная угроза выхода из строя всех компьютерных систем, использующих программное

обеспечение, в которых календари заканчивались 1999 годом. Как отмечает профессор Л. Лессиг, Y2K стал первым реальным кризисом, порожденным несовершенством программного кода, и первым вызовом, когда человеческой культуре в целом предстояло противостоять разрушительным последствиям близорукости программистов. «Точно так же, как мы должны беспокоиться по поводу плохого регулирования со стороны закона, — пишет Л. Лессиг, — нам следует беспокоиться по поводу плохого регулирования со стороны кодов. <...> Тысячи программистов делали свою работу, думая, что она — их собственность. Культура и правовая система, по существу, рассматривали их деятельность как разрозненные акции индивидов. И вот теперь, спустя годы после появления первого плохо скомпилированного кода, мы оказались лицом к лицу со своего рода экологическим бедствием: мы окружены кодами, которые могут в критических и непредсказуемых направлениях давать осечки, угрожающие как минимум миллионами долларов экономического ущерба, а то и гораздо худшими последствиями в духе сценариев Судного дня»²⁸.

Проблема программного кода как средства регулирования киберпространства и деятельности в нем весьма сложна ввиду принципиальной новизны этого социального регулятора и неясности его соотношения с другими регуляторами. Может ли законодатель устанавливать какие-то нормы, которые должны будут соблюдать создатели кодов? Видимо, может. Однако для этого он должен корректно включить киберпространство в сферу текущего правового регулирования, не противопоставляя реальный и виртуальный миры, а понимая, что эти миры существуют совместно и то, что происходит в одном, может иметь серьезные последствия в другом. Наглядный пример тому — международный скандал вокруг интернет-сайта Wikileaks, свидетельствующий о том, что виртуальная реальность киберпространства заставляет совершенно по-новому взглянуть на проблемы свободы мнений и защиты информации.

Подводя итог сказанному выше, отметим, что в данной статье мы лишь наметили некоторые очертания возможных подходов к формированию правовой основы регулирования киберпространства и человеческой деятельности в нем.

²⁸ Lessig L. Code and Other Laws of Cyberspace. NY. : Basic Books, 1999. P. 2 ; Idem. Code. Version 2.0. NY. : Basic Books, 2006. P. 338.

БИБЛИОГРАФИЯ

1. Новгородцев П. И. Историческая школа юристов. — М., 1896.
2. Карбонье Ж. Юридическая социология. — М. : Прогресс. 1986.
3. Конституционное обустройство России: общественная экспертиза. — М., 2000.
4. Руденко В. Н. Прямая демократия: модели правления, конституционно-правовые институты. — Екатеринбург, 2003.
5. Фукуяма Ф. Доверие: социальные добродетели и путь к процветанию. — М. : АСТ; Ермак, 2004.
6. Программа ЮНЕСКО «Информация для всех». Отчет 2004—2005 гг. — М. : ЮНЕСКО, 2006.
7. Лессиг Л. Свободная культура. Как медиаконцерны используют технологии и законы для того, чтобы душировать культуру и контролировать творчество : пер. с англ. — М., 2007.
8. Тедеев А. А. Теоретические основы правового регулирования информационных отношений, формирующихся в глобальных компьютерных сетях. — М., 2007.
9. Настольная книга по медийному саморегулированию / под ред. М. А. Федотова — М., 2009.
10. Труды по интеллектуальной собственности : материалы науч.-теорет. конференции. Москва, МГЮА, 27 января 2000 г. — М., 2000. — Т. 2 : Актуальные проблемы информационного права. — С. 18.
11. Barber B. The Logic and Limits of Trust. — New Brunswick, NJ : Rutgers University Press, 1983.
12. Lessig L. Code and Other Laws of Cyberspace. — NY. : Basic Books, 1999.
13. Lessig L. Code. Version 2.0. — NY. : Basic Books, 2006.
14. Putnam R. D., Feldstein L. M. and Cohen D. Better Together : Restoring the American Community. — NY. : Simon & Schuster Paperbacks, 2004.
15. Sztompka P. Trust: a Sociological Theory. — Cambridge: Cambridge University Press, 1999.

Материал поступил в редакцию 30 сентября 2015 г.

CONSTITUTIONAL ANSWERS FOR THE CHALLENGES OF CYBERSPACE

FEDOTOV Mikhail Aleksandrovich — Doctor of Law, Professor, Head of the UNESCO Department on Copyright and Other Intellectual Property Rights at the Higher School of Economics, 101000, Russia, Moscow, Myasnitskaya street, 20.

Review. Analyzing peculiarities of relations of various subjects in the field of information and communication technologies, the author comes to a conclusion about the necessity of formation of a new branch of law – law of cyberspace. It is shown that modern instruments of legal regulation on a national, as well as on a supranational level, do not possess sufficient effectiveness for ordering this relationship. In this connection the importance of such means of regulation of the information and telecommunication space is being emphasized as a self-regulation and program code. Particular amendments to the Constitution of the Russian Federation aimed at greater issue of information civil rights are also proposed.

The author believes that specificity of a cyberspace forces people to reconsider a traditional approach to any norm of law in the space, time and in the lap of persons, since the Internet environment deprives the concept "space" of unambiguous geographical definiteness, the concept "time" is not locked to any time zone, but the concept "lap of persons" turns to include not natural persons and legal entities, but computers and other devices participating in network interaction and being identified by computers' IP addresses and other technological parts.

In some authoritarian countries a person can be connected to the network only when providing a document proving his identity, and establishment of a similar rule only leads to the slowdown in the development of a respective country, its «falling out» of the overall world process; it does not stimulate cyberspace clearance of everything contradicting to what is recognized unlawful, undue and forbidden.

The cyberspace continually raises new questions relating to intellectual property protection, but the traditional legislator's responses, having been kept in a habitual logic of permissions and prohibitions, cause total and mass violation of established legal order, on the one hand, and contribute to accumulation of logical self-contradictions, on the other hand.

Keywords: Constitution of the Russian Federation, the law of cyberspace, Internet, "cloud" technologies, self-regulation, program code, transformative constitutional regime, codified constitutional regime.

BIBLIOGRAPHY

1. *Novgorodtsev P.I.* The Historical School of Jurists. — M., 1896.
2. *Karbon'e Zh.* [J. Carbonnier] Legal sociology. — M.: Progress. 1986.
3. Constitutional arrangement of Russia: Public expert examination. — M., 2000.
4. *Rudenko V. N.* Direct democracy: models of government, constitutional legal institutions. — Yekaterinburg, 2003.
5. *Fukuyama F.* Trust: The Social Values and the Creation of Prosperity. — M.: AST; Ermak, 2004.
6. UNESCO Program "Information for Everyone". The 2004-2005 report. — M.: UNESCO, 2006.
7. *Lessig L.* Free culture. How Big Media Uses Technologies and the Law to Lock Down Culture and Control Creativity (translation from English) — M., 2007.
8. *Tedeev A. A.* Theoretical fundamentals of legal regulation of information relations being formed in global computer networks. — M. — 2007.
9. A Handbook on Media Self-Regulation. Fedotov M.A. (ed.) — M., 2009.
10. Topical problems of information law. Proceedings of a scientific-theoretical conference. Moscow, January 27, 2000, MSAL. Papers on intellectual property. Vol. 2, 2000.
11. *Barber B.* The Logic and Limits of Trust. — New Brunswick, NJ: Rutgers University Press, 1983.
12. *Lessig L.* Code and Other Laws of Cyberspace. — NY. Basic Books. 1999.
13. *Lessig L.* Code. Version 2.0. — NY. Basic Books. 1999.
14. *Putnam Robert D., Feldstein Lewis M. and Cohen Don* Better Together: Restoring the American Community. — NY.: Simon & Schuster Paperbacks. 2004.
15. *Sztompka P.* Trust: a Sociological Theory. — Cambridge: Cambridge University Press, 1999.