

Д.С. ХАРЧЕНКО

**КОНТРОЛЬ В ИНФОРМАЦИОННОМ ОБЩЕСТВЕ:
СОЦИАЛЬНО-ФИЛОСОФСКИЕ ОСНОВАНИЯ**

Настоящая статья посвящена такой новой и малоизученной теме как правовой контроль в Интернет – сети. Автор проводит анализ сценариев установления правопорядка в Интернете по аналогии с установлением правопорядка в физическом мире, выводит особенности правового контроля в Интернете. Также в статье проводится сравнительный анализ опыта разных стран по контролю Интернет – пространства, где особое внимание отводится отечественному опыту в данном вопросе. В заключении автор дает возможные прогнозы относительно дальнейшего развития ситуации по правовому контролю Интернет – сети.

Ключевые слова: право, правовой порядок, социальная философия, контроль, Интернет, Интернет-пространство, кибербалканизация

Харченко Дмитрий Сергеевич – очный аспирант кафедры теологии и религиоведения, Саратовский национальный исследовательский государственный университет им. Н.Г. Чернышевского. E-mail: dima291189@mail.ru

D.S. HARCHENKO

**CONTROL IN INFORMATION SOCIETY:
SOCIO-PHILOSOPHICAL BASES**

The present article is devoted to such a new and poorly studied subject as legal control on the Internet. The author carries out the analysis of scenarios of establishment of law and order on the Internet by analogy with the establishment of law and order in the physical world, and thus identifies features of legal control on the Internet. The author carries out the comparative analysis of experiences of different countries in the control of the web space, where the special attention is paid to domestic experience in this regard. In conclusion, the author gives possible forecasts concerning further development of the situation with legal control of the Internet.

Keywords: law, legal order, social philosophy, control, the Internet, web space, cyberbalkanization

Dmitry S. Harchenko – postgraduate student at the Department of Theology and Religious Studies, Saratov National Research State University n.a. N.G. Chernyshevsky. E-mail: dima291189@mail.ru

Современное общество, являясь постоянно развивающейся и усложняющейся социальной структурой, зачастую требует пересмотра устоявшейся системы отношений в различных своих сферах. Одной из таких наиболее динамично развивающихся, а потому требующих максимально радикального пересмотра является сфера информации, получившая наибольшую свою реализацию в виде функционирования сети Интернет.

Концепция информационного общества уже достаточно прочно вошла в современную социальную философию, и сегодня значительное число исследований выполняется именно в рамках этой парадигмы. При этом единого определения «информационного общества» равно как и «информации» не существует. Автором концепции принято считать Д. Белла, который пытался осмыслить информационное общество как один из вариантов следующей ступени после индустриального. Если обратиться к его теории, нель-

зя не отметить, что телекоммуникации и техника занимают у него хотя и значительное место в постиндустриальном обществе, но не являются его центром. Белл наряду с технологичностью и развитием телекоммуникационных сетей атрибутирует информационному обществу ещё и экономику, выстроенную на базе сферы услуг [1]. Так, информационные технологии в трактовке Белла являются скорее средством достижения новой экономической модели, нежели тем фактором, который существенно меняет характер социальных отношений.

По мере того, как информационное общество из теоретического конструкта становится реальностью, появляются более ориентированные на технологии как самостоятельный феномен теории. Так, «Стратегия развития информационного общества в Российской Федерации» предлагает нам понимать информационное общество как общество, в котором информация и знания становятся стратеги-

ческим ресурсом общества, сопоставимым по значению с ресурсами природными, людскими и финансовыми [10]. В настоящем исследовании мы будем в целом опираться на такое понимание информационного общества с той возможной поправкой, что информация как стратегический ресурс общества не просто сопоставима с природными, людскими и финансовыми ресурсами, а, возможно, и превосходит их по значимости.

Наконец, ещё одним важным теоретическим конструктом в контексте настоящего исследования является концепция сетевого общества. Наиболее рельефно эта идея проявилась в теории Кастельса, где была представлена в качестве составной части информационного общества. Для него сетевое общество – это структура, состоящая из определённых узлов, между которыми происходит обмен информацией. Доминирующую роль при этом играет уже не столько сама информация, сколько направления её передачи и способы её использования [2]. Кастельс, таким образом, характеризовал в большей степени структуру информационного общества, нежели его сущность. Однако можно сделать предположение о том, что концепция сетевого общества может существовать и самостоятельно вне парадигмы постиндустриального общества, так как обмен информацией происходил между субъектами и до появления технических средств передачи информации.

Появление новых технических средств сегодня характеризуется понятием «Сетевая революция». Эта революция уже давно вышла за пределы интереса только специалистов в сфере высоких технологий, сегодня всё чаще к анализу сетевого общества обращаются гуманитарные науки, и социальная философия, конечно же, не является исключением. В настоящем исследовании хотелось бы обратиться к данному вопросу с позиции философии права, а конкретнее говоря – с позиции анализа сетевого общества через призму феномена правового порядка.

Особенностью сетевого общества с точки зрения социальной философии является, прежде всего, то, что сетевое общество – это один из возможных способов иерархизации и структурирования общественных отношений, то есть в определённом смысле это разновидность общественного порядка. Общественный порядок в свою очередь разворачивается в нескольких измерениях. Одним из таких измерений и является правовой порядок как та часть общественного порядка, которая находится в поле регулирования законом.

Именно обращение к этой стороне исследования сетевого общества имеет сегодня наивысшую актуальность. Первые десятилетия существования Интернет-сети, когда она ещё не воспринималась как что-либо серьёзное, существенной потребности охватывать её действием законодательства не было. Сегодня же, когда Интернет становится полноправной сферой человеческой жизни, вопрос о правовом регулировании данного пространства всё чаще ставится правительствами большинства стран. Однако существует и альтернативный полюс особой Интернет-философии, мыслящей пространство Интернета как пространство безграничной свободы. Такое понимание киберпространства получило специальное название «киберанархизма» и сформировало по сути отдельное поле философских проблем [4].

В ходе попыток определения понятия правопорядка, исследователями выделяются различные его принципы. Среди прочих принципов, таких как справедливость, иерархичность или структурность, особое место занимает принцип подконтрольности. Само понятие контроля редко определяется специально, так как до определённой степени кажется очевидным. Тем не менее, некоторые специальные виды контроля иногда находят своё определение. В частности, государственно-правовой контроль, о котором в данном контексте идёт речь обычно определяется как наблюдение за контролируемой системой со стороны государства или уполномоченными государством органами с целью проверки соблюдения закона и/или обеспечения выполнения решения государственных органов [7].

Именно в контексте правового регулирования Интернет-пространства рассмотрение вопроса о его контроле представляется наиболее интересным. Вопросы, связанные с контролем информации, блокировки тех или иных ресурсов приобрели особую актуальность в России в последние годы, в особенности вследствие принятия пакета Яровой-Озерова и запрета на различного рода анонимайзеры и обходы блокировок. Однако, прежде чем приступить к анализу актуального состояния данного вопроса в России, представляется необходимым рассмотреть накопленный зарубежный опыт.

Вопросы правового регулирования Интернет-пространства являются одними из наиболее сложных для права как такового, главным образом по той причине, что Интернет сам по себе не локали-

зован в одной стране, а, значит, не понятно, законодательством какой страны Интернет должен или, по крайней мере, может регулироваться. К разрешению данного вопроса есть два подхода: регулирование Интернета нормами международного законодательства и регулирование Интернета сегментарно нормами законодательства тех стран, которым принадлежит домен.

Говоря о контроле Интернет-пространства в контексте международного права, следует отметить, что право на свободное пользование Интернетом с недавних пор рассматривается ООН как одно из неотъемлемых прав личности [8], а, значит, любая попытка воспрепятствовать свободному доступу в Интернет может быть расценена как покушение на права человека. К сожалению, на этом фактическое международное регулирование Интернет-пространства заканчивается. Кроме того, международное сообщество настаивает на том, что ни одна из стран не должна иметь приоритета в управлении Интернет-пространством. К сожалению, на настоящий момент это пожелание международного сообщества не реализуемо, так как две важнейшие компании в области контроля Интернета – ICANN (Internet Corporation for Assigned Names and Numbers), которая создаёт новые домены верхнего (национального) уровня, и IANA (Internet Assigned Numbers Authority), которая контролирует распределение IP-адресов, на настоящий момент принадлежат США [6]. Хотя обе компании и не являются подведомственными правительству США, так или иначе, находясь в правовом поле американского законодательства.

Таким образом, система международного права в области Интернет-регулирования ещё не достаточно развита для того, чтобы полноценно осуществлять правовое регулирование Интернет-пространства. Отчасти по этой причине, а отчасти потому, что далеко не все страны устраивают международные принципы вседоступности Интернета, значительное число государств в мире применяет те или иные средства по контролю и ограничению интернет-трафика.

Этот процесс уже получил название кибербалканизации (по аналогии с политической балканизацией – распада большого государства на более мелкие самостоятельные). Кибербалканизация как умозрительный конструкт предполагает под собой разделение Интернета как глобальной сети на самостоятельные локальные сети в пределах национальных

государств. С точки зрения упрощения правового регулирования сетевого пространства, процессы кибербалканизации значительно упрощают ситуацию, сводя её банально к регулированию каждой локальной сети законодательством конкретного государства. Однако, с другой стороны, кибербалканизация уничтожает Интернет как таковой, что вызывает закономерную критику с позиции глобалистов, трансгуманистов и апологетов Интернета [4]. И хотя говорить о том, что кибербалканизация произошла, ещё не представляется возможным, в последние годы всё более серьёзные меры по контролю Интернета принимаются законодательством конкретных стран. Рассмотрим такие примеры.

Одним из наиболее, казалось бы, демократичных стран в области контроля за Интернет-пространством является США. Длительное время, руководствуясь первой поправкой Конституции, которая гарантирует неприкосновенность пяти основных свобод человека, в том числе – свободу слова и печати, правительство США не вмешивалось в Интернет-пространство и, по сути, представляло провайдером в этом отношении полную свободу. Единственным исключением из этого был запрет на распространение через Интернет детской порнографии, что было продиктовано приоритетом физического и психологического благополучия детей [3].

Однако в 2010 году в законодательстве США в этом отношении произошли серьёзные перемены. Прежде всего это принятие «Исполнительного законопроекта о координации в киберпространстве», благодаря которому правительство получило право в случае возникновения чрезвычайных ситуаций, ставящих под угрозу безопасность, обрабатывать поисковые запросы, запрашивать данные пользователей, регулировать трафик вплоть до полного отключения [9]. Также важным фактором в области контроля за Интернетом стал «Закон об авторском праве в цифровую эпоху» [9], который запрещает размещение чужой интеллектуальной собственности без согласия владельца.

Аналогичное законодательство, направленное на ограничение пиратского распространения контента, работает и во Франции. Но, в отличие от США, правительство Франции гораздо жёстче контролирует содержание сайтов. МВД Франции не требуется чрезвычайная ситуация для мониторинга Интернет-пространства, а подразделения, направленные на борьбу с киберпреступностью могут блокировать сайты без санкции

суда. Когда дело касается расследования тяжких преступлений, таких как торговля наркотиками, оружием, финансовые махинации, законодательство Франции позволяет сотрудникам силовых структур даже внедряться в персональные компьютеры пользователей при помощи троянских программ [5]. При этом интересно отметить, что, если в США обязанности по удалению нежелательных материалов и вся ответственность за размещение противозаконного контента лежит на пользователе, то во Франции существенная часть ответственности возлагается на провайдера, который также обязан блокировать нежелательные сайты в соответствии со списками правительства. В случае нарушения цифрового законодательства во Франции санкции грозят пользователю, так и провайдеру, что, конечно, подталкивает последних к более тщательному анализу контента.

Таким образом, можно резюмировать, что демократическими западными странами в общем случае вмешательство в Интернет возможно либо тогда, когда Интернет способствует совершению преступлений, либо когда речь идёт о защите интеллектуальной собственности или личных данных пользователей, хищение которых, по сути, является также противозаконным действием. Однако принципиально иначе обстоит дело в ряде неевропейских и недемократических стран, где можно говорить о полноценной цензуре в Интернете.

Так, характерным примером подобной цензуры является Китай. Помимо блокировки сайтов с незаконным содержанием, в Министерстве обороны Китая существует специальное подразделение, занимающееся мониторингом социальных сетей и Интернета в целом на предмет всего, что правительство считает неприемлемым. Основным техническим проявлением такой цензуры становится система блокировки нежелательных зарубежных сайтов и особая система фильтрации поиска (т.н. Великий китайский файрвол). Системами фильтрации оснащены все китайские поисковики, в результате чего в ответ на запрос пользователь видит только цензурированные результаты.

Подобная система фильтрации поиска имеется также в ряде арабских стран и обычно согласуется с нормами Шариата. Так, в Саудовской Аравии и ОАЭ существует система фильтрации данных, при которой изымается нежелательная информация по ключевым словам. Как правило, это информация, касающаяся алкоголя, наркотиков, азартных игр, порно-

графических материалов и прочих материалов, считающихся неприемлемыми с позиции Ислама. Однако при этом ограничиваются, например, многие зарубежные, прежде всего европейские ресурсы, такие как Facebook, YouTube, сайты правозащитных организаций и т.д. Кроме того в Саудовской Аравии, например, практикуется географическая блокировка и фильтрация. Так, Теком – район Дубаи, который является интеллектуальным центром страны, имеет расширенный доступ к Интернету в отличие от всей остальной страны.

Наконец, пожалуй, образцом тоталитаризма в области контроля над Интернетом является ситуация в КНДР. В определённом смысле, можно сказать, что доступа в Интернет в КНДР нет вообще, по крайней мере, для простых пользователей. Фактически подключение к Интернету там имеет крайне ограниченное число правительственных организаций, занимающихся контактами с зарубежными странами, и несколько ведущих университетов. Даже в этих организациях доступ к Интернету осуществляется только по спецпропускам, а компьютеры, подключенные к Интернету, стоят в специальных охраняемых комнатах. При этом для обычного населения в КНДР существует внутренняя сеть Кванмён, наполнение которой жёстко контролируется правительством. В основном содержание сети Кванмён представляет собой сгружаемые Корейским компьютерным центром из Интернета страницы научного и технического содержания, прошедшие предварительную цензуру. По этой причине Кванмён в основном используется как образовательный ресурс.

Таким образом, подводя итоги опыта зарубежных стран по контролю Интернет-пространства, мы видим два основных уровня выстраивания порядка в сети Интернет. Первый – это приведение контента в соответствие с оффлайн законодательством и борьба с Интернет-ресурсами, способствующими совершению преступлений, а также борьба с киберпреступностью как таковой – в частности с хищением персональных данных пользователей или киберпиратством. Второй уровень контроля – это установление системы цензуры во избежание широкого распространения «нежелательного» контента. Перечень нежелательного контента регламентируется каждым государством самостоятельно и может варьироваться, но так или иначе основанием для вынесения решения о «нежелательности» той или иной информации явля-

ются соображение безопасности, противодействия экстремизму и терроризму.

На первый взгляд может показаться, что оба типа контроля Интернет-контента в целом направлены на поддержания правопорядка в сети и приведение в соответствие онлайн- и офлайн-законодательства. Меры, предпринимаемые тем же Китаем, насколько бы они ни казались недемократичными европейскому человеку, тем не менее, продолжают находиться в рамках действующего китайского законодательства. Однако принципиальная разница заключается в юридическом подходе к системе правового регулирования в сети. Первый сценарий, назовём его условно европейским (хотя он характерен не только для европейских стран), направлен на пресечение конкретных преступных действий, нарушающих существующее законодательство. Второй же сценарий, назовём его условно азиатским, направлен, в том числе, и на предотвращение возможных преступных действий, которые ещё не случились, и нет никакой гарантии, что случатся когда-либо. Таким образом, такой подход нарушает один из базовых юридических принципов – презумпцию невиновности. Пользователю, ещё не совершившему преступление, но совершающему действия, которые, по мнению правительства, могут в дальнейшем привести или подстрекать других к тем или иным преступлениям, уже вменяется вина до того, как противоправное действие будет совершено.

Теперь же имеет смысл обратиться к анализу ситуации с контролем Интернет-пространства в России. Одним из первых мер по правовому регулированию Интернета, а вернее – регулированию правопорядка, в том числе посредством Интернета, стал пункт в Федеральном законе «О связи» [14], обязывающий операторов, в том числе Интернет-провайдеров, предоставлять правоохранительным органам, ведущим оперативно-розыскную деятельность, информацию о пользователях. Тем не менее, несмотря на то, что данный закон был принят ещё в 2003 году, далеко не все сегменты Интернет-сети были открыты для правоохранительных органов. Следующим значимым законом в этом отношении стал Федеральный закон «О противодействии экстремистской деятельности» [13], который среди прочего включил в себя Федеральный список экстремистских материалов, в соответствии с которым российские провайдеры начали блокировку сайтов, где были размещены соответствующие материалы.

Вслед за экстремистскими материалами под запрет попала информация, содержащая детскую порнографию, пропагандирующая наркотики и суицид [12], а позже началась борьба с нелегальным цифровым пиратством. Также с 2014 года Роскомнадзор получил возможность блокировать сайты, содержащие призывы к экстремизму без решения суда [11], а с 2015 года – ту же возможность в отношении сайтов с пиратскими материалами.

Всё это – борьба с распространением детской порнографии, пропагандой наркотиков, призывов к незаконной деятельности, борьба с пиратством – вполне укладывается в «европейский» сценарий контроля Интернет-пространства. Тем не менее, установление порядка в Интернете только этими мерами не ограничивается. Основной упор Роскомнадзором в настоящее время делается на возможность как такового контроля активности пользователей в сети для возможности выяснения трафика при необходимости в последующее время. Эти меры как таковые трудно назвать составляющей правопорядка в Интернет-пространстве, но состояние подконтрольности пользователей правоохранительным органом оно предоставляет.

Таким образом, можно подвести некоторые итоги касательно становления правопорядка в Интернет-пространстве. С тех пор, как пользование Интернетом приобрело относительно массовый характер, и он перестал рассматриваться как что-то несерьёзное, начались определённые попытки правового регулирования данного пространства. В области правового контроля Интернет-пространства существует два основных сценария – приведение Интернет-пространства в соответствие с реальным позитивным правом той или иной страны, т.е. запрет на фактическое нарушение закона Интернет-пространств; и упредительный контроль, запрещающий в Интернете всё, что гипотетически может привести к нарушению закона. Это порождает интересный феномен: вне правового порядка оказываются действия, не противоречащие естественному праву и не покрывающие преступные действия, но просто препятствующие контролю за киберпространством. Так, например, использование криптовалют или оверлейных сетей само по себе не наносит ущерба обществу, но, являясь тем фактором, который затрудняет контроль в Интернете для правоохранительных органов, оказывается также разрушающим правовой порядок.

Тем не менее, в вопросе правового регулирования Интернет-среды на данном этапе остаётся больше вопросов, чем отве-

тов. Тот факт, что Интернет является глобальным феноменом, и, значит, не может быть сведён к правовой системе одного конкретного государства, требует существенного развития международного законодательства в этом отношении. В противном случае киберпространство и социум ждут крайне интересные трансформации от распада Интернета на локальные сети до формирования субинтернет-сети, которая вовсе окажется вне возможности всякого правового регулирования.

Список литературы

1. Белл Д. Социальные рамки информационного общества / Сокращ, перев. Ю.В. Никуличева // Новая технократическая волна на Западе. Под ред. П.С. Гуревича. – М., 1988. – 330 с.
2. Кастельс М. Становление общества сетевых структур // Новая постиндустриальная волна на Западе. Антология / Под ред. В.Л. Иноземцева. – М.: Academia, 1999. – 640 с.
3. Коуэн Г. Свобода слова и печати: исключения из Первой поправки // Институт проблем информационного права. Серия «Журналистика и право». – 2005. – Вып. 53. – С. 144-193.
4. Ладлоу П. Криптоанархии, кибергосударства и пиратские утопии. – Екатеринбург: Изд. Ультра. Культура, 2005 – 600 с.
5. Люди-пауки. Как контролируют Интернет-паутину в разных странах // Российская газета. Федеральный выпуск №5591 (215). – 27.09.2011 (дата). – С. 11.
6. Международное право и Интернет: движение навстречу или противостояние? // Центральный научно-исследовательский институт связи, 27.03.2014 [Электронный ресурс]. – URL: <https://zniis.ru/actual/news-industry/internet/548> (Дата обращения: 30.08.2017).
7. Мельник М.В., Пантелеев А.С., Звездин А.Л. Ревизия и контроль: учебник. – М.: КНОРУС, 2006. – 640 с.
8. ООН признала доступ в интернет базовым правом человека // Лента.ру, 07.06.2011 [Электронный ресурс]. – URL: <https://lenta.ru/news/2011/06/07/basicright/> (Дата обращения: 25.08.2017).
9. Паламарчук А.В. Регулирование правоотношений в сети Интернет в зарубежных странах // Вестник Академии Генеральной прокуратуры Российской Федерации. – 2012. – № 6(32). – С. 24-32.
10. Стратегия развития информационного общества в Российской Федерации от 07 февраля 2008 г. №Пр-212 // Федеральный выпуск №4591. – 16.02.2008. – С. 5.
11. Федеральный закон «О внесении изменений в Федеральный закон «Об информации, информационных технологиях и о защите информации» от 28 декабря 2013 г. № 398-ФЗ.
12. Федеральный закон «О защите детей от информации, причиняющей вред здоровью и развитию» от 29 декабря 2010 г. № 436-ФЗ.
13. Федеральный закон «О противодействии экстремистской деятельности» от 25 июля 2002 г. № 114-ФЗ.
14. Федеральный закон «О связи» от 07 июля 2003 г. № 126-ФЗ.