
Проблемы регулирования информационного общества

«Информационное общество» – просто инструмент риторики; средство для понимания и разграничения того, что было, и того, что есть. Таким же инструментом риторики является и «киберпространство». Что мы должны понять, так это то, как информационные и коммуникационные технологии «информационного общества» влияют на системы законов, норм и практик «реального мира». На этом строилась мечта о создании нового общества; реальность же такова, что мы существуем в рамках наших обществ вместе с новыми технологиями и принятыми законами, рынками, нормами и практиками.

Интернет – это форум для взаимодействия и общения, совокупность постоянно меняющихся разнообразных телекоммуникационных протоколов и распределенных по всему миру технологий. Это также социальное явление с огромным количеством пользователей из все возрастающего числа стран. Одновременно это и интерактивный рынок, открывающий возможности для электронной коммерции, электронной торговли ценными бумагами и других форм электронных транзакций. Это еще и самая большая библиотека, самый богатый ресурс для обучения и коммуникации (и в то же время самое большое хранилище порнографической, непристойной и вредной информации). Интернет – важнейший элемент нашей повседневной жизни.

Отличается ли информационное общество от того, что было известно нам раньше? И да, и нет. Отличаются ли Интернет и транснациональный характер его деятельности от телеграфа и телефона? Во многом не очень сильно, но все же – отличаются. Наконец, изменились ли формы и функции управления благодаря появлению глобальных коммуникационных сетей? Ответ – да, до опасной степени.

Современные информационные и коммуникационные технологии действительно порождают и проблемы, и возможности для правительств. Мы уже показали, как вопрос юрисдикции превращается для государств в проблему с точки зрения регулирования; новые проблемы возникают, когда это регулирование осуществляется. Однако вызовы, связанные с регулированием, выходят за рамки трансграничных вопросов. Другая задача – определить, как вписать коммуникационные инфраструктуры, такие как Интернет, в систему законодательной практики. Проще говоря, относимся ли мы к Интернету точно так же, как к телефону, телевидению, радио или печатным СМИ?

Являются ли пользователи Интернета потенциальными «вещателями» или это просто индивидуумы, общающиеся друг с другом по принципу «точка-точка»? От ответа на этот вопрос зависит то, как мы относимся к организациям, предоставляющим услуги интернет-коммуникации. Регулирование деятельности поставщиков интернет-услуг как носителей информации, по типу телефонных компаний, снимает с них часть ответственности за контроль над контентом, но заставляет их подчиняться многочисленным регулятивным нормам в области связи. Отношение к Интернету как к широковещательной среде, подобной телевидению или радио, делает поставщиков интернет-услуг ответственными за контент, проходящий по их каналам. Иногда они, в зависимости от модели бизнеса, принимают на себя ответственность за предоставляемые услуги, однако в большинстве случаев эта ответственность определяется законом.

Обновление законов для их применения к Интернету – это, по существу, процесс поиска ответа на вопрос, является ли Интернет широковещательной средой, средой нейтральной по отношению к контенту или каналом передачи информации. Режимы ответственности компаний варьируются в зависимости от подхода к регулированию, принятого конкретным государством. Отметим, что по алжирскому законодательству все поставщики интернет-услуг должны нести ответственность за контент размещаемых сайтов; швейцарское право делает поставщиков интернет-услуг ответственными только в тех случаях, когда автора контента установить невозможно; в Венгрии провайдеры услуг свободного сетевого пространства не несут ответственности за контент, за исключением случаев, когда провайдер был осведомлен о том, что сайт нарушал закон, но ничего не предпринял в связи с этим; юридическая мысль в Великобритании превратила поставщиков интернет-

услуг почти что во «вторичных издателях», каковыми являются книжные магазины и архивы, но никак не в обычный канал передачи информации.

Определение Интернета с позиций цензуры

Государства традиционно регулируют контент теле- и радиовещания, и попытка применить существующие правила к Интернету выглядит вполне естественно.

Ситуация в Австралии может служить примером возникающих при этом проблем. Рассмотрим заявление, которое сделал заместитель председателя Австралийского управления массового вещания (Australian Broadcasting Authority, ABA) – сторонник государственного регулирования в этой области:

«Массовое вещание, а теперь и Интернет, используют государственную собственность – воздушные волны и частоту каналов связи. Массовое вещание является, а Интернет становится средством массовой коммуникации, имеющим чрезвычайно «назойливую» природу. (...)

Для должностных лиц и законодателей важно в процессе пересмотра существующих и подготовки новых правил для массового вещания и Интернета проанализировать и пересмотреть направленность общественных интересов, которые, по их мнению, следует распространить на эти области и на управление ими»⁹.

Данный сотрудник регулятивного органа трактует Интернет как «средство массовой коммуникации», подводя его тем самым под мандат АВА вместе с регулированием телевизионных услуг. В свою очередь, это управление действует в рамках своего мандата по соблюдению государственных интересов в области контроля контента.

Однако Интернет и телевидение – не одно и то же. Вот что говорит по этому поводу профессор Роджер Кларк (Roger Clarke) – критик госу-

⁹ Australian Broadcasting Authority. 1999. «Broadcasting, co-regulation and the public good» (Массовое вещание, совместное регулирование и общее благо), NR 101/1999, 29 October 1999.

дарственной политики в области цензуры национального контента и блокирования международного контента:

«Что поражает в этом заявлении, в политике государства и в законах, которые были приняты Сенатом под давлением оппозиции и Палатой представителей под управлением правительства, так это то, что они сформулированы людьми, пребывающими в счастливом неведении относительно природы технологий и, как следствие, того поведения, которое, по их представлениям, они регулируют. Это не идет на пользу предполагаемым бенефициарам и сильно вредит всем участвующим сторонам»¹⁰.

Это заявление было поддержано многими, кто не согласен с введением цензуры. Похожие высказывания звучали со стороны австралийского сообщества хакеров¹¹ (Australian hacker community), которые, помимо прочего, проинформировали пользователей о методах обхода запретительных мер, кодировании, установке соединений типа «точка-точка», прокси и многих других технических возможностях.

Сторонники цензуры часто приходят к тому, что начинают предлагать свои собственные технологические решения. На ранней стадии политических споров были предложены системы оценки контента, аналогичные рейтингам в кино и на телевидении. По этой схеме файлам и веб-сайтам должен был быть присвоен определенный рейтинг. Американский союз борьбы за гражданские свободы (American Civil Liberties Union, ACLU) ответил на это докладом, в котором изложил свое несогласие с взглядом на Интернет как на область кино- и телеиндустрии. В силу особенностей культуры, экономики и структуры Интернета подобная система рейтинга будет неосуществима, в частности, из-за

¹⁰ Roger Clarke, «Subject: Aba Demonstrates Its Ignorance to the World» (Тема: Австралийское управление массового вещания демонстрирует всему миру свое невежество), *Forwarded to the Politech Mailing List, message titled FC: More on Australian official demanding Net-regulation – demonstrating ignorance to the world*, November 3 10:42:30–0800 1999.

¹¹ Dogcow, «Evading the Broadcasting Services Amendment (Online Services) Act 1999» (Акт об уклонении от изменений услуг массового вещания (онлайн-услуг)), 2600 Australia, 1999.

международного арбитража и экономических последствий для малого бизнеса¹².

Еще одним технологическим ресурсом, предложенным сторонниками всемирной цензуры, являются клиентские фильтры, которые закрыли бы пользователям доступ к «непристойным файлам». Эта мера аналогична политике, разработанной в США в отношении V-Chip – обязательного чипа автоцензурирования, устанавливаемого во всех телевизорах с целью предотвращения просмотров непристойных передач (в соответствии с рейтингом, принятым в данной индустрии).

Однако установка фильтров в Интернет – отдельный вопрос. В ряде докладов, подготовленных академическими и неправительственными организациями, возможности фильтров были подвергнуты сомнению. Было показано, что сама *природа Интернета*, его распределенный характер и проблематичность создания инструментов автоматической проверки на «пристойность» могут привести к блокированию вполне адекватного контента. Кроме того, определенный объем непристойного материала все равно остается неотфильтрованным. В ряде докладов говорилось о *необъективности* имеющихся фильтров, о том, что они блокируют веб-сайты вопреки интересам их разработчиков, таких как организации, отстаивающие свободу слова¹³.

Интересные вопросы обсуждались на первом формальном процессе в США по регулированию интернет-контента. В 90-е годы XX века Конгресс США принял закон, предписывающий установку средств проверки возраста людей, заходящих на «непристойные» веб-сайты. Когда действие Акта о нормах приличия в сфере связи (Communications Decency Act, CDA) было отменено решением суда по делу «ACLU против Reno», то аргументом послужила сложность определения понятия «не-

¹² ACLU, «Fahrenheit 451.2: Is Cyberspace Burning? How Rating and Blocking Proposals May Torch Free Speech on the Internet» (451,2 градуса по Фаренгейту: Пожар в киберпространстве? Как предложения по установлению рейтинга и блокированию могут уничтожить свободу слова в Интернете), American Civil Liberties Union, 1997.

¹³ Electronic Privacy Information Center, «Faulty Filters: How Content Filters Block Access to Kid-Friendly Information on the Internet» (Неправильные фильтры: как фильтры контента блокируют доступ к дружественной детям информации в Интернете), 1997.

пристойная информация», притом, что ограничение доступа по возрасту также было технологически сложной и дорогостоящей задачей. Суд постановил, что «любое регулирование контента Интернета, независимо от степени добродетельности цели, с которой это регулирование будет осуществляться, способно «спалить город ради того, чтобы зажать поросенка»». Решение это было принято с учетом «самой природы Интернета» и Конституции США¹⁴. Суд признал, что Интернет отличается от всех ранее созданных коммуникационных инфраструктур и что он способен стать для людей развивающей силой. Все усилия по регулированию должны предприниматься с осторожностью, и CDA – совсем не тот случай.

Для многих стран процесс, начатый Конгрессом США, послужил примером, и они стали принимать свои собственные законы, регулирующие контент. Стратегии и механизмы регулирования стали включать попытки определения ответственности поставщиков интернет-услуг, выработки мер аутентификации непристойных слов и установки фильтров на уровне провайдеров и шлюзов, поддержки использования потребителями программного обеспечения для фильтрации данных. Тем не менее, в США продолжают споры о недостатках и опасностях цензуры, ставшие очевидными еще на ранних стадиях ее введения. Однако это не остановило международные правительственные организации от выступлений в поддержку изменений законов с целью недопущения появления непристойной или вредной информации.

Определение Интернета с позиций надзора

Принятие законов о надзоре в средствах коммуникации является обычной практикой государств. XX век, начавшийся с перехвата почтовых, телеграфных и радиотелеграфных сообщений, стал свидетелем появления законов, разрешающих такой перехват. Сегодня предпринимается довольно большое количество попыток «реанимировать» законы, позволяющие надзор в сфере связи, и распространить их на Интернет. Проще говоря, государства пытаются регулировать Интернет как телефонную систему.

¹⁴ «ACLU v. Reno» (ACLU против Reno). United States District Court for the Eastern District of Pennsylvania, 1996.

Так, в 2000 г. в Великобритании был принят законопроект о регулировании прав на ведение следственных действий (Regulation of Investigatory Powers Act), который распространял свое действие на перехват интернет-коммуникаций. Правительство, стоявшее тогда у власти, говорило, что искомые полномочия не представляют собой ничего нового. Законопроект распространялся на всех поставщиков услуг связи, чтобы «все отрасли находились в равных условиях и закреплялся действующий принцип, по которому поставщики услуг обязаны поддерживать функционирование *разумного средства перехвата*»¹⁵. Индустрия интернет-услуг должна была регулироваться по той же схеме, по которой регулируется телефония, из намерения гармонизировать законодательную среду для всех отраслей деятельности.

Согласно современной политике США все телефонные компании обязаны иметь устройства наблюдения, но на провайдеров интернет-услуг это требование пока не распространяется. В период подготовки данного доклада были предприняты попытки включить голосовую связь по IP-протоколу (VoIP) в число услуг, которые на основании законов США обязаны иметь встроенные возможности перехвата.

Корни этой политики уходят в более ранние инициативы правительства США. В 1999 г. Министерство юстиции обратилось в Открытое международное сообщество проектировщиков, учёных, сетевых операторов и провайдеров (Internet Engineering Task Force, IETF) с просьбой разработать для Интернета протокол, позволяющий осуществлять перехват и прослушивание. По своей природе IETF – демократичная организация, все члены которой имеют право голоса, и членом которой может стать каждый желающий. После долгих споров IETF приняла решение отказаться от работ над подобным протоколом. Некоторые возражали против такого решения, поскольку считали, что IETF могла (и должна была) создать детерминированный протокол для перехвата и прослушивания, который можно было использовать во всем мире; однако детерминированным он должен был быть потому, что требовал использования режима санкционированного доступа с высокой степенью технологической защиты. Некоторые посчитали, что возмож-

¹⁵ House of Commons. 2000. «Second Reading of the Regulation of Investigatory Powers Bill» (Второе чтение законопроекта по регулированию прав на ведение следственных действий), Jack Straw, Home Secretary, 6 March, 2000.

ность была упущена. Вот что сказал по этому поводу Стюарт Бейкер (Stewart Baker) – бывший Генеральный советник Управления национальной безопасности:

«В то время отказ IETF рассмотреть этот вопрос был воспринят с одобрением как победа гражданских свобод. На самом деле, по иронии судьбы, он привел к тому, что методы прослушивания стали конфиденциальными и разрабатываются по тихому сговору с ФБР. Вывод таков: ближайшее десятилетие будет очень непростым для Сети, противостоящей по своей природе контролю со стороны государства»¹⁶.

В итоге решения были изъяты из открытого форума, и были разработаны альтернативные методики. США внедриli Carnivore (DCS 1000) – программу, устанавливаемую на узле провайдера и регистрирующую трафик.

Отношение к Интернету как к телефонной системе позволяет также осуществлять надзор за «данными о трафике». Во времена старой доброй телефонной системы, после долгих юридических споров содержание коммуникации было признано секретным, и поэтому любое нарушение конфиденциальности требовало силовых действий, разрешенных законом. Такие «силовые действия» предполагают, как правило, выдачу ордера – судебного ордера в США или ордера, выдаваемого государственным лицом в Великобритании. Подобное правило не применялось к данным о трафике, включающим информацию о вызываемых и вызывающих номерах и времени коммуникации. Сбор и разглашение данных о трафике считалось мелким вмешательством. Особенно помогало то, что данные о трафике сохранялись телефонными компаниями и были доступны правоохранительным органам. Содержания разговоров, как правило, не хранились телефонными компаниями, и это частично снимало с компаний груз ответственности за соблюдение закона: данные о трафике имелись, они были юридически не такими конфиденциальными и потому доступными для государственных органов.

¹⁶ Stewart Baker, «Re: Metaswitch Embeds Police Spy Features in New Net-Phone Switch», (Компания Metaswitch встраивает шпионские средства для полицейской слежки в новый коммутационный пакет интернет-телефонии). Politech Mailing List, 2003.

Ставя Интернет на одну доску с телефонными компаниями, государства получили возможность доступа к данным об Интернет-трафике, сбор которых осуществляет провайдер. На юридическом языке эта информация относится к категории «данные о трафике», однако информация из Интернета коренным образом отличается от данных, предоставляемых телефонными компаниями: она включает все адреса, на которые вы отправляли электронную почту, все серверы, к которым вы подключались, всех людей, с которыми вы общались в чате, и, возможно, все веб-сайты, на которые вы заходили, страницы, которые вы просматривали, и темы, которыми вы интересовались. Совет Европы отмечал:

«Сбор этих данных в определенных случаях представляет возможность составить досье на человека, в котором будут указаны его интересы, круг общения и социальный контекст. Участвующие стороны должны помнить об этом при определении мер соответствующей защиты и формулировке юридических предпосылок для принятия таких мер»¹⁷.

Невзирая на это, большинство законов предоставляют государствам неограниченный доступ к этим «данным о трафике», независимо от того, насколько конфиденциальными могут быть эти данные и насколько они отличаются от данных телефонного трафика.

Правительство США применило более комплексный подход под контролем последовательно сменяющих друг друга администраций Белого дома. Сначала Администрация Клинтона объявила о своем намерении обновить право законного доступа с включением в него кабельных интернет-соединений, предложив «поправки, которые обновят устаревшие формулировки закона, связанные с техническими средствами, и сделают их технологически нейтральными»¹⁸. Эти «устаревшие» формулировки содержались в Законе о кабельном телевидении (Cable Act) от 1984 г., который поставил защиту данных о кабельном

¹⁷ Council of Europe, «Explanatory Report to the Convention on Cybercrime, ETS No. 185» (Совет Европы, «Пояснительный доклад к конвенции о киберпреступлениях»). Strasbourg: 2001.

¹⁸ John Podesta, «Speech by the White House Chief of Staff on Cybersecurity» (Речь руководителя аппарата Белого Дома о кибербезопасности). Washington, D.C.: National Press Club, 2000.

трафике или защиту данных о предпочтениях в области телевизионных программ на уровень выше даже защиты коммуникационного контента. Администрации Клинтона не удалось добиться изменений в законе в отношении данных об интернет-трафике, предоставляемом кабельными компаниями, но Администрация Буша оказалась более успешной и приняла в октябре 2001 г. USA-PATRIOT Act (Закон США об объединении и укреплении Америки путем предоставления необходимых инструментов для пресечения и препятствования терроризму). Этот документ настолько изменил Закон о кабельном телевидении, что заставил кабельные компании, предоставляющие интернет-услуги, передавать правоохранительным органам данные о трафике по той же методике, которая используется при предоставлении данных о телефонном трафике, т. е. при значительно более низком уровне защиты. Генеральный прокурор объявил об этом в следующей форме:

«Агентам будет поручено использовать преимущества новых технологически нейтральных стандартов для сбора сведений. (...) Следователям будет поручено активно преследовать террористов в Интернете. Новые положения в законодательстве позволяют использовать устройства, фиксирующие адреса отправителей и получателей, связанных через Интернет»¹⁹.

Закон разрешает доступ к значительно более обширной сфере информации, чем даже данные о любимых телевизионных программах. Эта информация включает данные о электронных адресах, номерах телефонов, просматриваемых веб-сайтов, искомым терминах, местоположении, копируемых файлах.

Таким образом, Интернет определяется как среда массового вещания, когда это отвечает интересам государства по введению цензуры; Интернет определяется как инфраструктура телефонных коммуникаций, когда это отвечает интересам государства по установлению надзора с минимальными ограничениями. Ни одно из этих определений не отражает технических реалий или инвазионного характера контроля.

¹⁹ Senate Committee on the Judiciary, *Testimony of the Attorney General* (Юридический комитет Сената Конгресса США, Показания Генерального Прокурора), September 25, 2001.