Организация Объединенных Наций
по вопросам образования, науки и культуры

Политика информационного общества

Ограничение и сдерживание глобальных потоков данных

UNESCO Publications for the World Summit on the Information Society

UNESCO

Politics of the Information Society: The Bordering and Restraining of Global Data Flows

Gus Hosein

Комиссия Российской Федерации по делам ЮНЕСКО
Федеральное агентство по культуре и кинематографии
Российский комитет Программы ЮНЕСКО «Информация для всех»
Межрегиональный центр библиотечного сотрудничества

ЮНЕСКО

Политика информационного общества: ограничение и сдерживание глобальных потоков данных

Гус Хосейн

Москва
2008

УДК 004.738.5:070.13
ББК 67.401.114
Х 84

Перевод с английского: *Малявская Е.В.*

Редактор русского издания: *Мурована Т.А.*

Хосейн Гус

Х 84 Ограничение и сдерживание глобальных потоков данных. – М.: МЦБС, 2008. – 68 с.

Издание на русском языке подготовлено по инициативе Российского комитета Программы ЮНЕСКО «Информация для всех» и Межрегионального центра библиотечного сотрудничества (МЦБС) при финансовой поддержке Федерального агентства по культуре и кинематографии.

Публикуется с разрешения ЮНЕСКО.

УДК 004.738.5:070.13
ББК 67.401.114

Организация Объединенных Наций
по вопросам образования, науки и культуры
7, place de Fontenoy, 75352 Paris 07 SP

CI-2004/WS/6 cld/d /15794

ISBN 978-5-91515-013-2

Содержание

Введение

В декабре 2003 г. состоялся Всемирный саммит по информационному обществу. На этом саммите были озвучены важные заявления, приняты значимые документы и определены пути развития. Время проведения саммита было выбрано удачно, особенно если учесть, что события последних лет кардинально изменили образ информационного общества, каким оно представлялось многим людям в мечтах, и придали ему реальный облик, который смогли увидеть тысячи присутствующих на саммите.

Мы когда-то мечтали об обществе, изобилующем информацией, которая должна была стать основой для знаний, увеличивающих возможности каждого человека. Границы должны были потерять свое значение, в мире должно было процветать разнообразие культур, коммуникация – привести к богатству, а истина – стать свободной. Хотя я сомневаюсь в том, что мы действительно создали «информационное общество», оно, тем не менее, естественным образом наследует многие проблемы, возможности и риски «реального общества». Независимо от того, какую инфраструктуру мы создадим, невозможно проигнорировать политику, которую проводят люди в современном мире, и людей, которые будут этот мир населять.

Политика *информационного общества* составляет главную тему настоящей работы. Особое внимание уделяется динамике событий, связанных со свободой выражения мнений и неприкосновенностью частной жизни. Многие из спорных политических вопросов в этом информационном обществе зависят от неприкосновенности частной жизни и свободы выражения мнений. Споры, которые ведутся вокруг технологий и вопросов социальной политики, включая «право на коммуникацию», «свободу участия», «стимулы для творчества», доступ и «цифровой

разрыв», охватывают вопросы неприкосновенности частной жизни и свободы выражения мнений.

Понимание путей развития политики в области введения надзора и цензуры способствует пониманию политических систем и методов руководства в существующей социально-технологической среде. Если информацию и коммуникацию в рамках своей среды мы считаем ключевыми составляющими юридической, политэкономической и социальной жизни и интересов, мы можем определять источники контроля, конфликтов и проблем, с которыми сталкиваемся.

Неприкосновенность частной жизни и свобода слова являются во многом двумя сторонами одной медали. Коллизии возможны, особенно в областях, связанных с освещением личной жизни в СМИ, или в связи с оскорблениями, которые могут содержаться в чьих-то высказываниях. В данной работе мы будем скорее говорить о несомненной взаимосвязи между этими правами человека. Мы проанализируем взаимозависимость этих прав и их ограничение: действие цензуры может наступать вследствие введения надзора, а введение разных форм цензуры может приводить к установлению надзора.

Государственные органы и различные организации вмешиваются в право на свободу выражения мнений, используя для этого различные регулятивные механизмы; подавляют свободу слова и диалога за счет усиления надзора. Ключевым элементом этих стратегий и механизмов является технология. Мы перечислим такие механизмы, чтобы показать, насколько мы ограничиваем открытое общество по причине нашей юридической, технологической и экономической «слепоты».

I.

Регулирование трансграничных потоков данных

Возникновение концепции «информационного общества» можно отнести к 60-м годам XX века. Она связана с появлением компьютеров и упадком в сельскохозяйственном и промышленном секторах экономики многих стран. Развитие сектора услуг стимулировало социальные изменения. Одновременно с этим бурный период разработки, внедрения и использования в повседневной жизни переживали информационные технологии. Наше нынешнее понимание концепции «информационного общества» связано с господством передовых информационных и коммуникационных технологий.

Сегодня «информационное общество» неотделимо от таких средств коммуникации, как Интернет, мобильная телефония и другие средства связи, обеспечивающие интерактивную коммуникацию. Эти средства связи работают на базе инфраструктур, использующих провода, кабели, оптическое стекловолокно и пластиковое волокно, спутники и антенны, которые покрывают весь мир и обеспечивают трансграничный поток данных. Применение различных протоколов связи позволяет людям легко общаться через границы. Провайдеры услуг дают возможность потребителям пользоваться электронной почтой, группами новостей, публиковать информацию на досках объявлений, размещать и поддерживать веб-сайты; позволяют пользователям *выкладывать* («push») пакеты данных на открытые ресурсы или *загружать* («pull») их из таких ресурсов, где бы те ни находились.

С некоторых пор среди различных механизмов взаимодействия с новыми технологиями стал преобладать подход «информационного общества». В настоящее время в политических программах постоянно поднимается тема приближения или наступления информационного

общества, вопросы о том, как мы должны это новое общество развивать, поддерживать и продвигать. Языковые средства описывают это общество как некое новое пространство, существующее отдельно от старого мира. Реальность же говорит о том, что это просто риторическая уловка: старый мир никогда не переставал существовать, он просто приспосабливается к новым технологиям.

Интернет и другие современные распределенные средства коммуникации заставили мир пересмотреть способы ведения бизнеса, разработки технологий и выработки политических решений. Интернет можно использовать как глобальный рынок, площадку для торговли идеями и создания приложений. Утверждалось, что новая политика должна будет учитывать рост объема информации и трудности сдерживания ее потока. Иными словами, сфера компетенции ежедневно подвергалась перераспределению и, возможно, даже определялась одним человеком – когда, например, гражданин Германии покупал книгу в книжном магазине в Америке, или программист из Австралии работал вместе с коллегой из Канады над приложениями созданного в Норвегии программного обеспечения.

Юрисдикция государственных законов и полномочий традиционно ограничивается сервисами и серверами в рамках географических границ. Более того, по традиции, провайдеры услуг отвечают за соблюдение законов в рамках юрисдикции того государства, в котором они физически находятся. Если ни серверы, ни отдельные пользователи, зависящие от их работы, не находятся в рамках тех же государственных границ, тогда государство не может контролировать ни книжные магазины, ни генерируемые коды, – так нам ранее виделась эта ситуация. Однако традиционные взгляды на юрисдикцию уступили место интерпретациям, более сложным для воплощения, как с юридической, так и с технологической точек зрения.

Некоторые страны считают, что информационный ресурс находится в их юрисдикции, если доступ к нему открыт для граждан их страны, независимо от физического местоположения сервера. Так, в соответствии с решениями судов Франции и Австралии веб-сайты США находятся в их юрисдикции и должны подчиняться, соответственно, законам Франции и Австралии. В результате провайдеры услуг по всему миру оказываются в сложной юридической ситуации, при которой они вы-

нуждены соблюдать законы нескольких юрисдикций помимо законов своей страны.

Экономические спекуляции и повышенное внимание к теме глобальной безопасности привели к появлению новой формы скептического отношения к свободе Интернета и возможностям, заложенным в ИНФОРМАЦИОННОМ ОБЩЕСТВЕ. Сегодня стало популярным развенчивать ранее существовавшие технологически-оптимистичные заявления относительно информационного общества. Заявления типа «если вы в Интернете – никто не знает, кто вы и где находитесь» или «государства бессильны контролировать глобальные сети» сейчас многими воспринимаются как нереалистичные. В последнее время стало звучать мнение, что регулирование потоков данных ничем не отличается от регулирования других видов деятельности. Скорее всего, истина находится где-то посередине.

Об юрисдикции и информационном обществе

Транснациональная деятельность создает конфликты между национальным законодательством стран и международной практикой. Это значит, что государства, как правило, имеют право принимать и применять законы в рамках своей юрисдикции; в конце концов, это их суверенное право. «Принцип суверенитета» часто определяется как исключительное право государств, осуществляемое строго в рамках государственных границ и более нигде1.

Однако возникают условия, при которых данное суверенное право подвергается сомнению, и, таким образом, возникает коллизия. В одних случаях подобная коллизия появляется при наличии большой активности зарубежом, т. е. когда деятельность, ведущаяся за пределами суверенной юрисдикции, влияет на способность этой юрисдикции применять свои законы. В других случаях коллизия возникает тогда, когда сама способность юрисдикции применять правовые нормы ослабевает вследствие сомнений в возможности применения законов по причине особенностей контекста законодательного регулирования.

---

1 Jonathan W Leeds. 1998. United States International Law Enforcement Cooperation: «A Case Study in Thailand. Journal of International Law and Practice» (Целевое исследование в Таиланде. Журнал международного права и практики) 7(1):1–14.

Подобные проблемы касаются не только информационного общества. Возьмем страну, которая решает принять закон, запрещающий разработку некоего лекарственного препарата. Эффективность этого закона сомнительна, если в другой стране аналогичного закона нет. Если первая страна не сможет предотвратить проникновение лекарства через свои контрольно-пропускные пункты, то лекарство станет доступным в нарушение духа закона. То же касается и контроля над состоянием окружающей среды: строгие ограничения на загрязнение воздуха в одном государстве не будут иметь никакого смысла, если граничащие с ним страны не примут аналогичные ограничения. В каждом случае законодательное регулирование связано с издержками и расходами без учета эффективности самого регулирования.

В случае с потоками данных в цифровых сетях и связанных с ними сервисами и продуктами подобные коллизии обостряются. Действие может быть совершено удаленно, активная деятельность конкретного индивидуума может производиться за пределами той юрисдикции, в рамках которой он физически находится. В таких ситуациях создание пограничного контроля становится еще более сложным с технологической точки зрения делом, затрагивая интересы большого количества стран, неправительственных организаций и отраслей промышленности.

Рассмотрим одну из первых политических проблем, с которой столкнулись государства: политику криптографии. Правительства различных стран были намерены регулировать использование определенного прикладного программного обеспечения, но оказались практически бессильны запретить гражданам, проживающим в открытых демократических государствах, скачивать эти приложения на свои компьютеры, получая их из других юрисдикций. Новые проблемы возникли в сфере информационного общества и электронной коммерции. Они были связаны с вполне осознанной необходимостью развивать коммуникационные сети и снижать стоимость доступа; убирать препоны на пути ведения бизнеса, наносящие вред национальным экономикам; заниматься вопросами влияния новых технологий на гражданские свободы. Время показало, что практически все попытки ввести законодательное регулирование в этих областях провалились.

Государства извлекали уроки из своих неудач. Трансграничные потоки данных представляли собой явную опасность для национальной политики. Потоки данных не подчинялись юрисдикции.

Интернет как самостоятельная юрисдикция

Одним из вариантов анализа сложившейся ситуации является взгляд на Интернет как на самостоятельную юрисдикцию и выработка соответствующего отношения. Традиционные понятия суверенитета и юрисдикции предполагают, что правительства придают большое значение границам, которые должны обеспечить им власть, дать силу их законодательным нормам и правилам, создать легитимность их действий и обеспечить информированность тех, на кого распространяется регулирование. Джонсон и Пост – специалисты по вопросам права и Интернета – написали в своей известной статье следующее:

> «Быстрый рост глобальной компьютерной сети разрушает связи между географическим расположением и (1) способностью местных властей установить контроль над онлайновой средой общения; (2) влиянием онлайновой среды на людей и предметы; (3) легитимностью усилий местного руководства применять местные нормы и правила в отношении явлений глобального масштаба; (4) способностью физического положения определять, какой набор правил применим в конкретном случае»[2].

Интернет и киберпространство действительно поставили суверенитет органов власти в сложное положение. Действуя на расстоянии, Интернет и трансграничные потоки данных создали эффект переизбытка. Помимо этого, говорится, что архитектура Интернета создала среду, которая вошла в противоречие с действиями органов власти. В то время, когда органы власти пытались наладить регулирование путем принятия решений, обязательных для выполнения внутри страны (например, политика криптографии), Джонсон и Пост говорили:

> «Многие из сложностей, юридические и повседневные, вызванные пересекающими границы электронными коммуникациями, можно было бы разрешить принятием одного простого принципа: нужно думать о Киберпространстве как об отдельной, с юридических позиций, «территории» по причине существования юридически значимых границ между Киберпространством и «реальным миром».

---

2 David R. Johnson and David G. Post, «Law and Borders – the Rise of Law in Cyberspace» (Закон и границы – рост влияния закона в киберпространстве), *Stanford Law Review* (1996).

Опасения властей строились не на безуспешности национальных мер или национальной политики, а на заложенных в них противоречиях в условиях новой социально-технологической среды. Вероятнее всего, применение законодательного регулирования, ограниченного географическими границами, по отношению к среде, не имеющей границ, бессмысленно. Важнее то, что регулирование силами одной юрисдикции будет иметь мгновенные последствия для другой юрисдикции именно в силу безграничности киберпространства.

Проще говоря, если бы США ввели нормы на определенную форму речи, то это бы означало регулирование речи и в других местах, поскольку большая часть Интернета приходится на США. Другим примером является решение французского суда, привлекшее Yahoo! к ответственности за содействие аукциону по продаже реликвий времен нацизма[3]. Yahoo! было предписано не допускать французских националистов к тем разделам веб-сайта, на которых были выставлены на продажу предметы времен нацизма. Важна сама по себе попытка определить «французских националистов», пусть пока только в онлайне. В итоге Yahoo! закрыл доступ всем пользователям из всех стран к аукционному разделу сайта. В первом примере принятая в США норма могла иметь фактические последствия для всего мира; во втором примере французское распоряжение распространилось на другие юрисдикции и повлияло на них.

Интернет как часть общей практики

Можно взглянуть на эту проблему и с другой точки зрения: рассматривать «информационное общество», «киберпространство» и Интернет так же как все остальные формы трансграничной деятельности. Транзакции в киберпространстве не так уж сильно отличаются от других транснациональных транзакций, поскольку задействуют людей в «реальном пространстве» в разных территориальных юрисдикциях, что приводит к «реальным» действиям и последствиям.

В этом смысле транзакции в киберпространстве по сути своей не являются основанием для большего внимания со стороны регулятивных

---

[3] Хороший обзор данного вопроса представлен у Yaman Akdeniz, «Case Analysis of League against Racism and Antisemitism (Licra), French Union of Jewish Students, v. Yahoo! Inc. (USA), Yahoo France, Tribunale De Grande Instance De Paris, Interim Court Order, 20 November 2000», *Electronic Business Law Reports* 1, no. 3 (2001).

органов отдельных стран[4]. Политика, принятая в какой-либо одной стране, всегда отразится на другой. В Интернете происходит то же самое.

Изменения в технологиях транспортировки и коммуникации, произошедшие в первой половине XX века, превратили деятельность с участием разных юрисдикций в обычное дело. Это совпало с ростом уровня регулирования и, несмотря на усилия арбитражных судов разных юрисдикций, коллизии юрисдикций стали очевидными. Даже в судебных делах по вопросам, связанным с множественными юрисдикциями, суды применяли универсальное обычное право, не имеющее привязки ни к одной конкретной суверенной власти, а именно: торговое право, морское право или международное право[5].

Сегодня международное право разрешает государствам применять их право к экстерриториальным случаям, имеющим значительные последствия для локального уровня. Один из ведущих специалистов по данному вопросу отмечает:

> «В современном мире транзакция может на законных основаниях регулироваться и в той юрисдикции, в которой она совершается, и в юрисдикциях, в которых ощущаются значительные последствия от данной транзакции, и в тех юрисдикциях, регулятивными нормами которых обременены участвующие стороны»[6].

На самом деле страны успешно справляются с регулированием потоков данных. В 1995 г. Европейский Союз принял окончательный вариант гармонизирующей директивы по защите данных, в которую вошли две статьи, регулирующие трансграничные потоки данных[7]. Такие

---

4 Jack L. Goldsmith, «Against Cyberanarchy» (Против киберанархии), *University of Chicago Law Review* 65 (1998).

5 Jack L. Goldsmith, «Symposium on the Internet and Legal Theory: Regulation of the Internet: Three Persistent Fallacies» (Симпозиум, посвященный Интернету и теории права: регулирование Интернета: три устойчивых заблуждения), *Chicago-Kent Law Review* 73 (1998).

6 Goldsmith, «Against Cyberanarchy».

7 European Union, «Directive 95/46/EC of the European Parliament and the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data» (Директива 95/46/ЕС Европейского Парламента и Совета ЕС от 24 октября 1955 г. о защите прав частных лиц применительно к обработке личных данных и о свободном движении таких данных) (1995).

совершенно разные страны, как Австралия, Китай и Саудовская Аравия, приняли законы о цензуре для контроля отправляемой, получаемой информации или того и другого; это было сделано, несмотря на предупреждения о невыполнимости и ошибочности подобных мер.

В каком-то смысле каждая новая технология нарушает существующий правовой режим. Телеграф кардинально увеличил скорость и объем коммуникации, сократив скорость коммуникации с месяцев и недель до часов и минут. Телефон сократил стоимость и увеличил частоту и приватность международной коммуникации[8]. Интернет нарушает привычную практику так же, как другая инфраструктура, но он делает это несколько более замысловатым образом.

Интернет как отдельная проблема

Сказать, что сейчас ничего не изменилось, – значит закрыть глаза на конкретные перемены, проблемы и возможности, появившиеся в связи с развитием и внедрением информационного общества. Государства часто заявляют, что просто «обновляют» свои законы с учетом новых технологических условий, стремясь сократить до минимума споры и признавая основные изменения в политике естественным и бесспорным фактом.

Транснациональные коллизии часто разрешались путем гармонизации законов. Что касается Интернета, то известны инициативы, предложенные ООН, Советом Европы, Организацией по безопасности и сотрудничеству в Европе и странами Большой восьмерки для рассмотрения таких изменений, коллизий и различий в правовых системах. Совсем недавно Всемирный саммит по информационному обществу считался центром распространения информации о том, как следует эффективно регулировать экономическое, социальное и криминальное поведение за пределами границ государств.

Проблематичными представляются попытки обращаться с потоками данных в сетевой среде так же, как мы делали это в прошлом. Возникают новые проблемы и задачи, независимо от того, насколько упорно мы делаем вид, что новые технологии похожи на своих предшествен-

---

8 Goldsmith, «Against Cyberanarchy».

ников. Новые технологии могут стать основанием для новых правовых методов, которые, в свою очередь, могут создавать новые коллизии для наших норм международного права. Наконец, различия в системах управления существовали всегда, и никакой уровень гармонизации не сможет адекватно защитить права личности.

Итак, мы возвращаемся к дискуссии об «информационном обществе» и связанной с ним политике. При обсуждении вопросов, касающихся юрисдикции и Интернета, с одной стороны, возникает опасность распространения национального законодательства за пределы конкретного государства. С другой стороны, мы рискуем обращаться с Интернетом совершенно отличным от других форм транснационального управления образом. Так в чем должна заключаться роль управления в «информационном обществе»? Отвечая на этот вопрос, мы входим в сферу технологической политики.

II.

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 издателей», 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 ABA 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 хакеров[11] (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 (онлайновых услуг)), 2600 Australia, 1999.

международного арбитража и экономических последствий для малого бизнеса[12].

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 слова[13].

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 зажарить поросенка»». Решение это было принято с учетом «самой природы Интернета» и Конституции США[14]. 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 продолжаются 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, дозволяющие 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 внедрили 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, искомых 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.

III.

Введение цензуры и ее последствия

Было время, когда высказывание типа «Интернет трактует цензуру как вред и старается ее обойти» считалось верным. Сегодня ситуация совершенно изменилась. Несмотря на то, что для отдельного национального государства установление юрисдикции над глобальными потоками данных может быть весьма опасным делом, государства разрабатывают законы, предусматривающие введение цензуры слова и надзора за поведением своих граждан. Опасность заложена и в определении Интернета как одного из видов инфраструктуры связи. И здесь государства продолжают гнуть свою линию на развитие возможностей регулирования потоков данных и введения надзора[20].

Существует несколько способов осуществления цензуры, и используются они в контрольных точках в рамках архитектуры Интернета. Эти контрольные точки включают исходное сообщение, исходящего провайдера, конечного провайдера и конечное сообщение или конечного пользователя[21]. Способы, применяемые для контроля этих параметров, включают:

- Прямые указания по контенту: что можно отправлять и к чему может быть предоставлен доступ.
- Требования по установке фильтров и других технических средств блокирования потоков данных.

---

20 Было много попыток проанализировать законы, принятые в разных странах мира для цензурирования информации или регулирования свободы выражения мнения. Основным в этой области является документ, подготовленный GreenNet Educational Trust and Privacy International: «Silenced: An International Report on Censorship and Control of the Internet», London: 2003.

21 Jonathan Zittrain, «Internet Points of Control» (Контрольные точки Интернета), *Boston College Law Review* 43, no. 1 (2003).

- Режимы лицензирования форм выражения мнения, передачи и приема информации.
- Режимы ответственности для источников сообщений и провайдеров.
- Ответственность за оскорбление и клевету.
- Режимы защиты авторского права и интеллектуальной собственности и пр.

Эти способы могут использоваться вместе или по отдельности в зависимости от ситуации.

При использовании указанных выше способов потоки данных контролируются во имя соблюдения приличий, безопасности и морали. Фильтры могут быть поставлены на уровне провайдера получателя для блокировки доступа пользователя к информации, которая считается вредной. Людей можно заставить использовать фильтры в пределах киберкафе или публичных библиотек. Желающие выразить свое мнение могут подпадать под действие законов о клевете, которые, как правило, требуют идентификации пользователя и, следовательно, некоторых форм лицензирования поставщиков интернет-услуг. Лицензирование провайдеров может сделать их ответственными за контент, хостинг которого они осуществляют. И, наконец, от провайдеров могут потребовать удаления хостируемого контента и разглашения информации о человеке, поместившем конкретный, вызывающий сомнение контент. Многие, если не все, из этих мер можно применять на основании закона об охране интеллектуальной собственности.

Кто принимает решения и осуществляет цензуру?

На пути доступа к Интернету существуют преграды, которые не всегда признаются следствием прямого влияния государственной власти. В ряде стран стоимость доступа недопустимо высока, что делает Интернет доступным только для национальной элиты. Структура рынка в ряде стран способствует созданию подобной ситуации: государственные монополии в таких странах, как Бахрейн, Бирма, Беларусь, Тунис и Либерия, выполняют двоякую задачу, ограничивая доступ к рынку и обеспечивая государственный контроль. Однако даже диверсификация рынка не обещает установления свободного от подобных проблем режима. Правительство Бангладеш отрезало от сети 60 провайдеров

услуг под тем предлогом, что они не возобновили свои лицензии; однако сами провайдеры утверждали, что принятые меры были направлены на то, чтобы заставить их прекратить предоставление услуг интернет-телефонии во имя сохранения государственной монополии на голосовую связь.

Во времена монопольной телефонной связи и государственных предприятий регулирующие органы были малочисленны, и законы проводились в жизнь самими правительствами. Теперь органы, которым поручено осуществлять надзор за процессом регулирования, могут быть самыми разными: в одних странах – это правительственные департаменты, в других – регулятивные органы, в третьих – независимые организации. Правительственные департаменты функционируют в Швейцарии (там полиция для блокировки контента, пропагандирующего расизм, направляет письма непосредственно провайдерам), в Италии (комитет национальной безопасности и министерство связи), в Лаосе (комитет, в состав которого входят несколько министерств, определяет порядок работы пользователей Интернет) и в Тунисе (Тунисское интернет-агентство, входящее в состав Министерства связи). Регулятивные органы отвечают за контент в Австралии (Австралийское управление вещания обладает правом издавать распоряжения о прекращении работы поставщиков интернет-услуг на территории Австралии), в Индии (Комиссия по связи Индии), Южной Корее (Комитет по этике информационных коммуникаций имеет право удалять контент без решения суда) и Венгрии (Национальный совет по радио и телевидению).

В состав регулятивных органов могут входить члены правительства, а сами регулятивные органы могут испытывать большое давление со стороны правительств. В числе стран с подобной моделью управления Великобритания, где действует Фонд контроля над Интернетом (Internet Watch Foundation, IWF) – организация, созданная изначально для противодействия регулированию; Венгрия, в которой существует Ассоциация контент-провайдеров (Content Providers' Association), первоначально аналогичная IWF, но ставшая более проблематичной из-за предложений по установке антипорнографических фильтров, удалению «вульгарных и агрессивных высказываний» и всего, что направлено против «хорошего вкуса», а также из-за рекомендаций в отношении потенциального нарушения авторского права. Однако проблема попрежнему в том, что все эти полномочия ограничены географическими границами.

Зачем нужна цензура?

Цели установления контроля или ограничения свободы слова могут быть самыми разными. Число различных и не всегда четко сформулированных определений «непристойных» высказываний приводит в замешательство. В качестве примера приведем наиболее яркие определения.

Цензура вводится во многих странах для защиты интересов национальной безопасности, но необходимо прояснить, что означают «интересы безопасности» в Кот-д'Ивуаре в сравнении с «государственной безопасностью и национальной гармонией» в Сингапуре. Египетские законы цензурируют контент для защиты «общественной нравственности» путем регулирования ошибочных или злонамеренных слухов или тревожных новостей, целью которых становится нарушение общественного спокойствия, вселение страха в людей или нанесение вреда государственным интересам. На законы Египта ссылаются часто[22].

В Перу наложен запрет на информацию, которая «противоречит морали или добрым традициям». Законы Марокко использовались для ареста редакторов газет за нанесение оскорбления королю и публикацию коммюнике Исламской группы[23]; в числе других «табу» – попытки поставить под сомнение претензии Марокко на Западную Африку. Тунис не признает никаких комментариев, содержащих намеки на критику политики правительства. Зимбабве регулирует все, что «способно привести в уныние», и карает подобные попытки тюремным заключением на срок до 7 лет. Австралия регулирует контент, который считается неподходящим для несовершеннолетних.

Китай подвергает цензуре информацию, нарушающую государственный порядок, раскрывающую государственные секреты и наносящую вред чести и достоинству страны; также Китай фильтрует ряд порнографических сайтов. Индия цензурирует материалы, «носящие похотливый характер» или «вызывающие похотливые желания». Закрыва-

---

22 Glenn Frankel. «Egypt Muzzles Calls for Democracy» (Египетские морды взывают к демократии). Washington Post, January 6, 2004, A01.

23 Committee to Protect Journalists, «CPJ Delegation Meets with Moroccan Ambassador: Calls for Immediate Release of Jailed Editors» (Делегация Комитета в защиту журналистов встретилась с послом Марокко и призвала его немедленно освободить задержанных редакторов), New York: 2003.

ются веб-сайты, пропагандирующие ненависть, клевету, оскорбления, азартные игры и расизм, насилие и терроризм, порнографию, включая детскую, и секс с элементами насилия. Помимо контента, описывающего инцест, педофилию, скотоложество и некрофилию, Сингапур регулирует пропаганду гомосексуализма. В Южной Корее до сих пор слушается дело о том, является ли конституционным регулирование контента, касающегося вопросов гомосексуализма.

Многие страны континентальной Европы запрещают контент, пропагандирующий расизм или ксенофобию. Совет Европы продвигает принятие гармонизирующих мер, призванных обеспечить признание всеми государствами-членами ЕС преступного характера подобных выступлений и предписывает удалять их с веб-сайтов государств-членов ЕС. Эти государства также разработали четкие законодательные нормы в отношении клеветы и оскорблений.

Пока правительство США, находясь под контролем Конституции и практики ее применения, более ограничено в вопросах регулирования свободы слова, возникают новые формы цензуры. Например, потребителей ограничивают «Условиями оказания услуг», которые принимают провайдеры, фактически ограничивая конституционные права пользователей: они разрешают им какие-то высказывания и действия, но при этом ограничивают свободу слова и доступа, которые на основании других документов являются абсолютно законными[24]. Таким образом, субъекты производства и частного сектора оказываются вовлеченными в процесс цензурирования потоков данных.

Негосударственная цензура I: интеллектуальная собственность

Практически все дискуссии о цензуре сводятся к обсуждению действий государств. Между тем беспокойство по поводу введения цензуры и контроля потоков данных должно быть направлено на механизмы, которые вводятся в действие самими источниками контроля. Индустрия, особенно когда она действует заодно с государством, может стать

---

24 Sandra Braman and Stephanie Lynch, «Advantage ISP: Terms of Service as Media Law – a Comparative Study» (Преимущество провайдеров: «Условия обслуживания» в качестве закона о СМИ – сравнительный анализ), University of Alabama, 2002.

мощным источником цензуры. Во имя защиты авторского права и интеллектуальной собственности принимаются законы и утверждается практика, вызывающая озабоченность.

Юридическая практика фактически представляет коллизии интересов разных отраслей промышленности и экономики. Так, Канада запретила потоковое видео, поскольку оно противоречило ранее введенным режимам массового вещания. Дания и Венгрия столкнулись с тонкими юридическими проблемами действия «глубинного связывания» (deep linking). Запретив интернет-порталам предоставлять выход по ссылкам на определенные статьи на других новостных сайтах, эти страны заставили их отправлять пользователей на первые страницы новостных изданий. В США индустрия контента вступила в юридический конфликт с индустрией коммуникаций в вопросе предоставления информации о пользователях «точка-точка».

При этом бывают ситуации, при которых противоборствующие стороны приходят к согласию и заключают тайные соглашения. В отличие от вышеприведенного примера с США, в Бельгии в 2000 г. впервые в мире было введено отслеживание пользователей, работающих с приложениями «точка-точка»: на основании «джентльменского соглашения» провайдеры стали предоставлять имена своих пользователей представителям музыкальной индустрии.

Гораздо дальше пошел закон об авторском праве в США. На основании «Закона об авторском праве в цифровом тысячелетии» (Digital Millenium Copyright Act, DMCA) от 1998 г. публикация информации о средствах, позволяющих обойти механизмы защиты авторского права, подлежит судебному преследованию. Закон предусматривает ответственность даже в том случае, когда люди, опубликовавшие подобный материал, находятся за пределами США. Так, в 2001 г. Дмитрий Скляров, российский программист, написавший программу, позволяющую обойти этот закон при пользовании Adobe eBooks, был арестован на собрании хакеров в Лас-Вегасе, на котором он выступал с докладом о своем изобретении. История закончилась тем, что ему лично обвинение предъявлено не было, но оно было предъявлено московской компании «Элкомсофт», сотрудником которой он являлся. Суд присяжных оправдал «Элкомсофт», частично потому, что написание программ не является в России противозаконным делом. Вот другой пример: 16-летний студент из Норвегии Йон Йоханссон написал программу DeCSS для об-

хода системы, защищающей коммерческие DVD, и был подвергнут штрафу со стороны Ассоциации американского кино опять же на основании вышеуказанного закона. Однако Ассоциация на этом не остановилась: она стала возбуждать дела против каждого, кто просто выходил по ссылке на эту программу. В числе пострадавших оказался и Эрик Корлей, редактор «2600: the Hacker Quarterly», который (наряду со многими другими пользователями Интернета) подключился к DeCSS с вебсайта своего журнала.

Все чаще в области авторского права мир следует примеру США. Европа вводит режим регулирования, аналогичный американскому «Закону об авторском праве в цифровом тысячелетии». В сочетании с принятыми в Европе режимами надзора это может иметь ужасающие последствия для свободы слова. Тем временем Австралия и Канада готовы принять как режим США по защите интеллектуальной собственности, так и европейские режимы надзора.

Негосударственная цензура II: клевета и оскорбления

Отдельные граждане и группы также могут иметь право на цензуру поведения других людей в отношении клеветы и оскорблений.

В ходе одного из исследований в Великобритании Правовая комиссия[25] обнаружила, что некоторые поставщики интернет-услуг получали более сотни жалоб в год от адвокатов и рядовых граждан на якобы оскорбительные материалы, размещаемые или распространяемые через этих провайдеров. Большая часть писем приходила от адвокатов и содержала жалобы на веб-сайты, созданные недовольными потребителями. Комиссия была вынуждена с сожалением признать, что лучшим решением для получателей этих писем было «удалить материал вне зависимости от общественных интересов и соответствия действительности». Такое решение было принято по причине неясного юридического статуса поставщиков интернет-услуг по британскому законодательству. Правовая комиссия выразила озабоченность тем, что группы

---

25 Law Commission, «Law Commission Report on Defamation and the Internet: A Preliminary Investigation» (Отчет Правовой комиссии о клевете в Интернете: предварительное расследование), London: Law Commission of England and Wales, 2002.

граждан, организующие подобные кампании, являются первой «пострадавшей стороной» в подобной ситуации. Этот правовой режим слишком близок к замораживанию свободы политического слова.

До тех пор, пока поставщики интернет-услуг воспринимаются как «вторичные издатели» или как организации, отвечающие в определенной степени за хостируемый контент, они, скорее всего, могут быть привлечены к ответственности. Правовая комиссия считает, что одним их выходов из создавшейся ситуации является полное освобождение провайдеров от ответственности, как это сделано в США. В качестве альтернативы следует подготовить более четкие инструкции по статусу поставщиков интернет-услуг как издателей, архивариусов или просто каналов передачи информации и ее носителей.

В делах, связанных с клеветой и оскорблениями, следует уделять больше внимания вопросам юрисдикций. Все чаще контент-провайдеры и поставщики интернет-услуг в разных странах мира подвергаются риску быть признанными юридически ответственными за клевету и оскорбления. Такой случай произошел в Австралии, когда суды этой страны признали, что дело о клевете против Доу Джоунса (Dow Jones), проживающего в Нью-Йорке, находится в их юрисдикции. Это дело стало прецедентом для канадского суда, который недавно принял аналогичное решение. Постановление гласило, что статья, опубликованная в Washington Post (в то время как человек жил и работал в Кении), может быть предметом слушаний в канадском суде несколько лет спустя, поскольку газета должна была «предусмотреть, что эта история будет следовать за истцом, независимо от места его проживания»[26]. Европейский Союз, работающий над разрешением коллизионного права в сфере оскорблений, считает, что любой человек, помещающий информацию в Интернете, будет отвечать по закону о клевете, принятом каждым государством-членом ЕС[27]. Недавно другой суд в Канаде признал,

---

26 See coverage of the case by Michael Geist, «Web Decision extends long arm of Ontario law» (Рассмотрение дела Майклом Гейстом – «Решение относительно Сети развязывает руки закону Онтарио), The Toronto Star, February 16, 2004.

27 Article 19, Press Release: «ARTICLE 19 concerned that proposed Rome II regulations pose threat to Internet publishers' freedom of expression» (Article 19, пресс-релиз : ARTICLE 19 выражает озабоченность тем, что решения, предлагаемые проектом «Рим II», представляют угрозу для интернет-издателей в части свободы выражения мнения), January 14, 2004.

что анонимная клевета «носит более рискованный характер, т. к. в нее легче поверить», и, следовательно, тот, кто клевещет на других с использованием Интернета, должен нести большую ответственность за причиненный ущерб[28].

Недостаточно корректное рассмотрение данной ситуации может привести к тому, что цензура будет введена как орудие правового устрашения. Это может произойти в результате запугивания поставщиков интернет-услуг или отдельных людей, лимитируя их право на свободу слова.

Законы о клевете используются также и правительствами. В некоторых странах клевета является преступлением. Правительство Сингапура боролось со своими оппонентами, подавая на них в суд за клевету. Закон о клевете в Джорджии используется как щит против расследований СМИ и имеет в своем арсенале гражданские и уголовные наказания, а правительство предлагает ввести более продолжительные сроки наказания за клевету на государственных официальных лиц. Согласно Article 19, Глобальной кампании за свободу выражения мнений[29]:

- клевета должна быть исключена из числа уголовно наказуемых преступлений;
- государственным органам, включая органы законодательной, исполнительной или судебной власти, должно быть запрещено подавать иски о клевете;
- высказывание мнения, в отличие от фактических обвинений, не должно служить основанием для обвинений в клевете;
- провайдеры интернет-услуг и другие организации, выполняющие аналогичные функции, должны быть ограждены от ответственности;

---

28 Patrick Brethour, «Net Libel Open to Higher Damages: Judge says anonymous Web postings can magnify impact of defamatory comments» (Клевета в Сети чревата тяжелыми последствиями: Судья говорит, что анонимные объявления в Сети могут усилить клеветнические заявления), Globe and Mail, February 11, 2004.

29 Article 19, «Harsh Georgian Defamation Laws Must Be Amended» (Суровые законы Джорджии о клевете должны быть изменены), London: The Global Campaign for Free Expression, 2004.

- должны быть предусмотрены меры защиты обоснованных публикаций;
- наказание должно быть адекватно нанесенному ущербу, а за нанесение нематериального ущерба должен быть установлен верхний предел наказания.

Цензура не должна быть включена в своды законов; простой факт того, что книги, содержащие законы, могут быть восприняты обывателем как индикатор ошибок и неточностей, может привести к цензуре.

Политика фильтрации и блокирования

Сеть, по сравнению с другими приложениями, скорее всего, представляет собой простейший объект для цензурирования, т. к. обычно веб-сайты создаются вполне идентифицируемым лицом и размещаются на коммерческом сервере. Вероятный цензор может использовать несколько вариантов действий: он может связаться с провайдером и попросить удалить сайт; он может арестовать создателя сайта или подать на него в суд; он может включить адрес веб-сайта в базу данных сайтов, запрещенных для доступа гражданам и/или потребителям. Все эти методы не новы. В первых двух случаях существует один общий риск: удаление сомнительного веб-сайта иногда воспринимается остальной частью Сети как «cause celebre» (вопрос, вызывающий жаркие общественные дебаты), а граждане стран за пределами сферы действия цензора могут в знак протеста открыть зеркальные закрытому сайты.

Технология блокирования используется довольно часто, но для того, чтобы стать по-настоящему эффективной, она должна применяться постоянно. Риск заключается в том, что пользователи могут научиться обходить блоки с помощью анонимных (прокси) сайтов или получения доступа к контенту через другие действующие прокси-сайты, такие как кэш в поисковике Google. Оба варианта действуют как связующее звено: они получают доступ к веб-сайту и отображают его для пользователя. Так создается виртуальный эквивалент ситуации, при которой ваш помощник отправляется в книжный магазин, чтобы купить для вас книгу, читать которую вам запрещено.

Технологии и методы блокировки и мониторинга развиваются в рамках политики, с учетом конкретных целей; их возможности огра-

ничиваются техническими средствами. Источник блокировки может быть установлен на уровне провайдера или на компьютере конечного пользователя.

Фильтрация на уровне провайдера

Блокирование отдельных веб-сайтов можно осуществлять на уровне государства. В идеале осуществить эту процедуру можно в странах с ограниченным числом поставщиков интернет-услуг. В этом случае доступ в Интернет осуществляется не с децентрализованного компьютера, а через контролируемую государством фирму, которая отвечает за мониторинг и блокировку доступа.

Китай «прославился» созданием своего «Золотого щита», ограничивающего доступ гражданам страны к информации с серверов, находящихся за пределами Китая. Как показали исследования, проведенные Центром Беркмана по Интернету и обществу Гарвардского университета (Harvard University Berkman Center for Internet & Society), метод фильтрации предполагает фильтрацию на пакетном уровне, встроенную в маршрутизаторы на границе. Существует также фильтрация по ключевым словам, в результате которой файл, загружаемый с сервера, может быть либо отфильтрован, либо сделан недоступным. В ходе исследования специалисты с помощью Google осуществляли в Китае поиск по словам «правосудие Китай» и «диссиденты Китай». Полученные данные показали, что чуть менее половины найденного контента оказалось заблокированным. При этом заблокированы были серверы BBC, CNN, Time, PBS и другие крупные новостные сайты. Однако блокировка не является явлением постоянным, и специалисты обнаружили, что Reuters блокировали периодически, а потом открывали, и то же самое происходило с Washington Post[30].

Специалисты из Центра Беркмана провели аналогичное исследование блокирования в Саудовской Аравии[31]. В этой стране весь сетевой трафик направляется через государственную организацию под названи-

---

30 Jonathan Zittrain and Benjamin Edelman, «Internet Filtering in China» (Фильтрация Интернета в Китае), IEEE Internet Computing, March-April (2003).

31 Jonathan Zittrain and Benjamin Edelman, «Documentation of Internet Filtering in Saudi Arabia» (Саудовская Аравия фильтрует документацию в Интернете), Berkman Center for Internet and Society, 2002.

ем «Internet Services Unit», в которой фильтрация данных осуществляется с целью сохранения «исламских ценностей». Это предполагает блокировку контента сексуальной направленности и страниц с описанием наркотиков, бомб, алкоголя, азартных игр, а также страниц, содержащих оскорбительные высказывания об исламе. Специалисты обнаружили блокировку сайтов, касающихся вопросов религии, а также музыкальных сайтов, сайтов с художественными фильмами и сайтов гомосексуальной направленности. Заблокированными оказались страницы, посвященные вопросам здоровья и образования, такие как раздел «Женщины в истории Америки» в онлайновой версии Британской энциклопедии, Музей Анны Франк и сайты по вопросам ближневосточной политики.

Последним «образцом для подражания» в отношении фильтрации на уровне провайдеров стал штат Пенсильвания. В этом штате действует закон, по которому фильтр на уровне интернет-протокола должен определять веб-сайты, распространяющие детскую порнографию. Специалисты из Центра Беркмана[32] открыли, что сделать это крайне сложно, поскольку 87,3 % действующих веб-сайтов в доменах .com, .net и .org имеют общие IP-адреса. Это означает, что любой IP-адрес, заблокированный на основании закона штата Пенсильвания, приведет к блокировке неопределенного числа других, не связанных с ним сайтов. Помимо этого, возникает еще одна проблема: поскольку поставщики интернет-услуг, находящиеся в США и обслуживающие пользователей штата Пенсильвания, не могут отличить их от пользователей других штатов, то запрет выходит за пределы штата. В сентябре 2002 г. WorldCom объявил, что собирается заблокировать доступ к обозначенным IP-адресам для всех своих абонентов в Северной Америке из желания соответствовать требованиям закона Пенсильвании[33].

Фильтрация на уровне конечного пользователя

Для уровня конечного пользователя разработаны коммерческие программы фильтрации. Во многих странах эти программные приложения

---

32 Benjamin Edelman, «Web Sites Sharing IP Addresses: Prevalence and Significance» (Веб-сайты с общими IP-адресами: широко распространенное явление и его значение), Berkman Center for Internet and Society, 2003.

33 Lisa Bowman and Declan McCullagh. «WorldCom blocks access to child porn» (WorldCom блокирует доступ к информации о детской порнографии). CNet News.com, September 23, 2002.

продаются родителям, которые опасаются, что их дети выйдут в Сети на нежелательный материал; компаниям и другим организациям, которые не хотят, чтобы их сотрудники в рабочее время использовали доступ к Интернету для просмотра порнографических сайтов.

Использование таких фильтров часто является обязательным по закону. Законодательство США увязывает вопросы установки программ блокировки на компьютеры в библиотеках и школах с вопросами финансирования. Законы Австралии, Китая и Аргентины требуют использования разных видов фильтров. В ряде стран, например Дании, Южной Корее и Афганистане, школы, библиотеки и интернет-кафе обязаны устанавливать программы фильтрации для защиты детей. Все эти формы цензуры оказывают непропорционально сильное влияние на людей с ограниченными возможностями – ведь они вынуждены использовать эти средства для любого выхода в Интернет.

Как правило, основу программного обеспечения для блокировки составляет некая внутренняя база, включающая нежелательные для посещения сайты, которые иногда сопровождаются поясняющими словами или фразами, появление которых на экране приводит к блокировке этих сайтов. Коммерческие организации, производящие подобные программы, как правило, держат в секрете точное содержание своих баз. Государственные регулирующие органы поступают точно так же. Когда на основании закона о свободе информации к Австралийскому управлению массового вещания обратились с просьбой назвать сайты, занесенные в «черный список», оно отказалось это сделать. В том и другом случае, предполагается, что заблокированный контент включает сайты выше того предела и шире тех классификаций, которые устанавливаются для блокировки.

Еще одна проблема состоит в том, что любая попытка цензурировать Интернет путем блокирования материала по ключевым словам способна, пусть даже и ненамеренно, блокировать совершенно независимый материал. Так, AOL (America online) вынуждена была просить британских пользователей из городка Scunthorpe писать название их родного города с ошибкой, потому что город пал жертвой программного цензора из-за неудачного сочетания четырех букв в середине слова. Попытки фильтров блокировать дискуссии на сексуальные темы, используя слово «грудь» в качестве ключевого слова, поставит блок на пути к нужным сайтам людям, больным раком груди. В 2003 г. чле-

ны Британского Парламента сочли невозможным проводить электронные дискуссии по законопроекту о сексуальных насилиях после того, как Парламент внедрил новую систему блокировки рекламной электронной рассылки порнографической информации.

Коммерческие программы блокировки продемонстрировали наличие и других, уже не только технических проблем. Производители программного обеспечения стали блокировать статьи и аналитические материалы, содержащие критику созданного ими программного обеспечения. Было установлено, что фильтры могут действовать, исходя из определенных интересов, например, блокируя сайты, рекламирующие безопасный секс, аборты, и даже сайты правозащитных организаций, несмотря на то, что эти ресурсы вовсе не находятся в состоянии конфликта с законодательными режимами, в рамках которых они созданы.

Специалисты потратили очень много времени на изучение списков блокируемых объектов для того, чтобы привлечь внимание к проблемам фильтрации. Они указали на множество случаев избыточного блокирования, когда оставались заблокированными сайты, не содержащие никакого непристойного контента. Также были обнаружены случаи недостаточной блокировки, когда программы не смогли отфильтровать тот контент, который должны были отфильтровать[34].

В качестве примера можно привести поисковую машину Google. Google SafeSearch – это фильтр, исключающий из результатов поиска информацию, имеющую сексуальный характер, или нежелательную информацию. Списки с результатами поиска автоматически сканируются для фильтрации порнографии и контента явно сексуального содержания в целях защиты, в первую очередь, детей. При этом исследование, проведенное в Центре Беркмана, показало значительное число неверно классифицированных результатов поиска[35].

---

34 Benjamin Edelman, *Sites Blocked by Internet Filtering Programs: Edelman Expert Report for Multnomah County Public Library Et Al., Vs. United States of America, Et Al.* (Сайты, заблокированные программами, фильтрующими Интернет), 2003 [cited February 24, 2004]; http://cyber.law.hatvard.edu/people/Edelman/mul-v-us/.

35 Benjamin Edelman, Empirical Analysis of Google Safesearch (Эмпирический анализ Google Safesearch), Berkman Center for Internet & Society, April 14, 2003 [cited February 12, 2004]; http://cyber.law.harvard.edu/people/eledman/google-safesearch/.

В числе исключенных страниц оказались сайты правительства США (congress.gov, Thomas.loc.gov, shuttle.nasa.gov); сайты, находящиеся в ведении правительств других стран (Министерства юстиции Гонконга, Министра юстиции северо-западных территорий Канады, Администрации Премьер-министра Израиля, Малайзийского национального совета по профессиональному образованию); политические сайты (Республиканской партии Вермонта, геев-демократов Остина, штат Техас); новости (включая статьи из New York Times о блогах, дефляции и военной стратегии США, а также статьи, публикуемые BBC, CNet news.com, the Washington Post и Wired), сайты образовательных учреждений (класс по химии в Колледже Миддлбери, материалы о войне во Вьетнаме в Беркли, юридическая школа Университета Балтимора, Северо-западный университет) и религиозные сайты (Фонд изучения Библии, современная дословная Библия, кошерная пища для пасхи). Среди исключенных сайтов, не содержащих очевидного сексуального контента, есть несколько, причиной блокировки которых стали двусмысленные слова в их названиях (например, Hardcore Visual Basic Programming); однако большая часть сайтов не дает никаких оснований предполагать разумную причину их исключения.

Исключенными оказались даже сайты, предназначенные для детей и полезные детям, включая материалы энциклопедии Grolier. Заблокированы были сайты, содержащие информацию по сексуальным вопросам, а также сайты по контролю над наркотиками. При этом открытыми остаются сайты с явно нежелательной информацией.

Другие исследования, которые были посвящены ряду ведущих программных приложений для фильтрации контента, обнаружили интересные данные. В одном из таких исследований, проведенном Национальной коалицией против цензуры (National Coalition Against Censorship), говорится, что продавцы ведущих программ фильтрации регулярно осуществляют избыточное блокирование[36]. Вот список наиболее спорных сайтов, оказавшихся заблокированными одним или несколькими ведущими программными приложениями:

---

36 Marjorie Heins and Christina Cho, «Internet Filters: A Public Policy Report» (Интернет-фильтры: отчет по государственной политике), Free Expression Policy Project, National Coalition Against Censorship, 2001.

- Домашние страницы Коалиции по сохранению традиционных ценностей (Traditional Values Coalition) и члена Конгресса США;
- Сайт Лиги за свободу программирования Массачусетского технологического института (MIT's League for Programming Freedom); часть сайта города Хиросима; сайты, посвященные Джорджии О'Кифи (Georgia O'Keeffe) и Винсенту Ван Гогу; сайт общества в поддержку моногамии Society for the Promotion of Unconditional Relationships;
- Практически все сайты геев и лесбиянок, а после обнаружения словосочетания «не менее 21»* – раздел новостей сайта Amnesty International (предложение, которое посчитали оскорбительным, звучало так: «Из Ириан Джайя поступают сообщения о перестрелках, в результате которых число убитых и раненых в Индонезии и Восточном Тиморе составляет не менее 21 человека»);
- эссе на тему «Непристойность в Интернете: уроки из мира живописи» (Indecency on the Internet: Lessons from the Art World), доклад ООН «ВИЧ/СПИД: глобальная эпидемия» (HIV/AIDS: The Global Epidemic) и домашние страницы четырех фотогалерей;
- официальный веб-сайт тогдашнего лидера большинства в Палате представителей Ричарда (Дика) Армея – по причине обнаружения слова «Дик» (dick – половой член);
- домашние страницы Союза за гражданские свободы штата Висконсин и Национальной коалиции против цензуры;
- Декларация Независимости; полное собрание пьес Шекспира; «Моби Дик» и «Марихуана: что нужно знать детям и подросткам» – брошюра, изданная Национальным институтом по вопросам злоупотребления наркотиками (National Institute on Drug Abuse), отделением Национальных институтов здоровья (National Institutes of Health);
- Сайты по правам человека – Комиссара Совета по делам стран Балтии (Commissioner of the Council of the Baltic Sea States); «Algeria Watch»; Медицинской библиотеки Арчи Дайка Канзасского университета (University of Kansas's Archie R. Dykes

* Прим. пер.: в данном случае «least 21» должно означать «не моложе 21 года».

Medical Library) – по причине присутствия слова «dykes» (лесбиянка);

- Страничка для еврейских детей и проект исследований молекулярной генетики собак Университета штата Мичиган («Canine Molecular Genetics Project at Michigan State University»);
- «Национальный журнал Закона о сексуальной ориентации» (The National Journal of Sexual Orientation Law); запрещенные книги Университета Карнеги-Меллон (Carnegie Mellon University's Banned Books); сайт компании по поставке продуктов питания «Давайте заведем роман» («Let's Have an Affair»); а также – по причине наличия грубых слов – не разрешен поиск «Мерзавцы вон из Каролины» («Bastard Out of Carolina») и «Сова и киска» («The Owl and the Pussy Cat»).

Фильтры также блокируют сайты, «обходящие закон», т. е. сайты, предлагающие анонимные, частные услуги, переводы на разные языки, юмористические тексты и даже услуги проверки функциональных возможностей веб-сайтов. По мнению одного из экспертов:

> «Чтобы цензура выполнила порученную ей задачу (контроля над информацией), ничто не должно ускользнуть от этого контроля. Поэтому следует закрыть любой сайт, который оставляет впечатление, что человек может получать информацию без ее предварительной проверки соответствующей программой цензуры. С этих позиций следует запретить сайты, обеспечивающие конфиденциальность, анонимность и даже переводы на другие языки»[37].

Итак, фильтры не разрешают пользователям обращаться к сервисам, которые способствуют укреплению их права на неприкосновенность частной жизни, и причина этого проста: частная жизнь предполагает свободу выражения мнения и доступа к информации. Надзор за частной жизнью и ее ограничение открывают дорогу цензуре и способствуют ее установлению.

---

[37] Seth Finkelstein, «Bess's Secret Loophole (Censorware Vs. Privacy & Anonymity)» (Секретный ход Бесс (Программное обеспечение с целью надзора против неприкосновенности частной жизни и анонимности), Anticensorware Investigations, 2002.

IV.

Угроза неприкосновенности частной жизни: надзор как первое ограничение

Свобода выражения мнения и неприкосновенность частной жизни связаны друг с другом так же, как цензура и надзор. В этой главе мы расскажем, как инициативы по усилению надзора влияют на цензуру, оказывая парализующее воздействие на свободу слова. Точно так же инициативы в области цензуры все больше зависят от механизмов надзора.

Знаменитое решение окружного суда США, отменяющее действие Акта о пристойности в сфере связи (Communications Decency Act), настаивало на том, что основным недостатком этого закона является разрешение проверки идентичности и возраста в онлайновом режиме.

> «Не существует эффективного способа определения идентичности или возраста пользователя, получающего доступ к материалам через электронную почту, программы-рассылки, телеконференции или чаты. Адрес электронной почты не предоставляет надежной информации об адресате, который может пользоваться почтовым псевдонимом или анонимной пересылкой почты. Не существует также полного или надежного списка электронных адресов и соответствующих имен и номеров телефонов, и любой подобный список либо является неполным в момент своего появления, либо быстро становится таковым. По этим причинам у отправителя нет никакой достаточно убедительной возможности узнать, кем является получатель сообщения – взрослым человеком или подростком. Проверка возраста становится еще более сложной задачей, когда программы-рассылки обрабатывают списки автоматической рассылки. Эксперт правительства [...] согласен с тем, что на сегодняшний день нет такой технологии, которая

могла бы с уверенностью обеспечить присутствие в списке для программ-рассылок только взрослых абонентов»[38].

Любой закон, который попытается ограничить доступ определенной группе населения к определенной информации, столкнется с этой проблемой. В противном случае начнет действовать эффект переизбытка. Взрослые люди не смогут получить доступ к контенту, на который они имеют полное право. Неспособность идентифицировать интернет-пользователя из Пенсильвании приведет к тому, что все пользователи поставщиков интернет-услуг на территории Северной Америки не получат выхода на определенные веб-сайты. Решение французского суда отразится на всех пользователях аукционных сайтов Yahoo!.

Нет простых решений, обеспечивающих идентификацию людей, работающих в онлайновом режиме, как нет гарантий идеальности таких решений, даже если бы они и существовали. Право людей на анонимное общение – одно из прав, столь же уважаемое обществом и заложенное в законе, сколь и попираемое.

Право оставаться неидентифицированным в процессе коммуникации

В странах совещательной демократии существует богатая традиция защиты анонимности слова. В 1776 г. Томас Пейн опубликовал свой «Здравый смысл» (Common Sense) и подписал: «Написано англичанином». Одно из наиболее почитаемых произведений в истории США – «Записки федералиста» (Federalist Papers) – вышло в свет в 1787–1788 гг. под псевдонимом. Его автором был объявлен некий «Публий» (Publius), пытавшийся склонить граждан Нью-Йорка к ратификации Конституции.

Право на анонимное участие защищено законом США, а Первая поправка защищает свободу слова. Первая поправка к Конституции США гласит:

---

38 *Chief Judge Sloviter. 1996. American Civil Liberties Union et al. v. Janet Reno, Attorney General of the United States: United States District Court for the Eastern District of Pennsylvania (Американский Союз в защиту гражданских свобод и др. против Джэнет Рено, Главного прокурора США).*

> «Конгресс не должен издавать законов, устанавливающих какую-либо религию или запрещающих ее свободное исповедание, ограничивающих свободу слова или печати или право народа мирно собираться и обращаться к Правительству с петициями о прекращении злоупотреблений».

Любая попытка государства ограничить свободу слова может быть объявлена незаконной как противоречащая Конституции. Ограничения свободы слова могут быть незаконными в силу размытости своих формулировок, что способно оказать парализующее воздействие на свободу слова; из-за широкого толкования законов, запрещающих как защищаемую, так и не защищаемую свободу слова; установления априорных ограничений на свободу слова; регулирования содержания слова при отсутствии узкоспециальной задачи, стоящей перед государством, и менее суровой ограничительной альтернативы; при этом постановления, принуждающие к слову, не разрешены. Запрет на принуждение к слову был использован для отмены законов, обязывающих людей раскрывать свою идентичность[39].

Один из первых юридических случаев, связанных с анонимностью слова в США, фактически предшествовал принятию Конституции. В 1735 г. состоялся суд над издателем Джоном Питером Ценгером (John Peter Zenger). Его обвиняли в отказе раскрыть имена анонимных авторов, выступавших с нападками на губернатора Нью-Йорка. В свою очередь, губернатор и его Совет обвиняли Ценгера в создании пасквилей, подстрекающих к мятежу. Многие подтверждали, что именно в ответ на эти события была подготовлена Первая поправка к Конституции США.

Право на анонимное участие в политической жизни было поддержано Верховным Судом США и в XX веке. В 1938 г. в деле «Ловелл против Гриффина» (*Lovell v. Griffin*) Верховный Суд признал недействительным решение, накладывающее всесторонний запрет на безлицензионное распространение литературы в любое время и в любом месте в Гриффине, штат Джорджия. В принятом решении говорилось, что памфлеты и листовки «всегда были оружием защиты свободы», и что

---

39 Electronic Privacy Information Center (Электронный центр защиты информации), «Free Speech» (Свобода слова), EPIC, April 8, 2002 [cited February 2004]; http://www.epic.org/free_speech/.

применение постановления по Гриффину «способно восстановить систему лицензий и цензуры в своей наиболее неприглядной форме». Постановления подобного рода действовали в то время во многих районах США. Несмотря на то, что целью принятия таких постановлений было предотвращение подделок, беспорядков или замусоривания территории, суд отказался поддержать их, отметив, что «существуют другие способы действия ради достижения этих законных целей, и нет необходимости вводить для этого ограничения на свободу слова и печати».

В 1958 г. Верховный Суд поддержал право Национальной ассоциации содействия прогрессу цветного населения (NAACP) не раскрывать списки членов недружественному ей правительству штата Алабама[40].

В этот же период в деле «Тэлли против штата Калифорния» (*Talley v. California*) Верховный Суд поддержал право на анонимность выступлений. Суть дела состояла в том, что правительство города Лос-Анджелес приняло решение, ограничивающее распространение рекламных листовок. Решение города требовало указывать в листовке имя ее автора и распространителя. Истец по фамилии Тэлли был арестован и предстал перед судом за нарушение этого решения. Его рекламные листовки касались организации «Мобилизация национальных потребителей» и призывали читателей оказать содействие этой организации в бойкотировании торговцев и бизнесменов, чьи имена были указаны в листовке, по той причине, что они торговали изделиями тех производителей, «которые отказывались предоставлять равные возможности по трудоустройству неграм, мексиканцам и выходцам из стран Востока».

В своем решении по делу «Тэлли против штата Калифорния»[41] судейская коллегия записала:

> «Анонимные памфлеты, листовки, брошюры и даже книги сыграли важную роль в прогрессивном развитии человечества. Группы и секты, подвергавшиеся преследованиям в разные периоды истории человечества, имели возможность анонимно критиковать за насилие законы и методы их осуществления. Принятый Англией предосуди-

---

40 *NAACP v. Alabama* (*NAACP против штата Алабама),* ex rel. Patterson, 357 US 449 (1958) and upheld in *NAACP v. Alabama*, 377 US 228 (1964).

41 *Talley V. California: the Supreme Court of the United States* (Тэлли против штата Калифорния: Верховный Суд США), 362 U.S. 60, decided March 7, 1960.

тельный закон лицензирования печати, который применили также и в колониях, можно частично объяснить тем, что объявление имен издателей, писателей и распространителей способно привести к сокращению числа изданий, содержащих критику правительства. Старые дела о мятежниках, оскорбляющих правительство Англии, показывают, как далеко могут зайти власть предержащие, чтобы найти ответственных за книги, звучащие для них оскорбительно. Джона Лилбурна высекли, пригвоздили к позорному столбу и оштрафовали за отказ ответить на вопросы, которые послужили бы основанием для признания его или кого-то другого виновным в тайном распространении книг в Англии. Два священника-пуританина, Джон Пери и Джон Удал, были приговорены к смерти по обвинению в написании и издании книг. До начала Войны за независимость патриоты-колонисты вынуждены были часто скрывать свое авторство или участие в распространении книг, поскольку могли с легкостью подвергнуться преследованиям со стороны контролируемых Англией судов. Примерно в это же время были написаны «Письма Джуниуса», автор которых неизвестен по сей день. Даже «Записки федералиста», написанные в поддержку принятия нашей Конституции, были опубликованы под вымышленными именами. Совершенно ясно, что анонимность использовалась порой в самых конструктивных целях».

В своем решении Верховный Суд пояснял, что «Письма Джуниуса» включали одно письмо, написанное 28 мая 1770 года, в котором был задан следующий вопрос относительно обложения США чайным налогом: «Что это как не одиозное, невыгодное проявление спекулятивного права и порабощение американцев, которое не может послужить на пользу их хозяевам?» В решении говорится, что «автор вряд ли осмелился бы задать этот вопрос, если бы у него не было возможности сделать это анонимно».

Еще одним делом, связанным с анонимностью высказываний, было дело «МакИнтайр против Комитета по выборам штата Огайо» (McIntyre v. Ohio Elections Committee). Это дело поставило под сомнение закон штата Огайо, запрещающий распространение анонимной литературы в период проведения избирательных кампаний. Закон предписывал, чтобы вся распространяемая литература содержала указание имени и адреса человека или чтобы в период кампании распространялась только официально изданная литература.

Маргарет МакИнтайр (скончавшаяся ко времени принятия решения) распространяла в 1988 г. листовки среди участников обществен-

ного митинга в одной из школ Огайо. На некоторых листовках ее имя было указано, но на многих вместо подписи было написано «Озабоченные родители и налогоплательщики». Сотрудник школы подал жалобу в Комиссию по выборам штата Огайо, и Комиссия оштрафовала г-жу МакИнтайр на 100 долларов.

В этом случае решение Верховного Суда гласило, что нет оснований считать, что текст сообщения содержал ложную, вводящую в заблуждение или клеветническую информацию. В решении Суда[42] говорилось:

> «Заинтересованность в появлении анонимной литературы на рынке идей, бесспорно, перевешивает любую заинтересованность государства в раскрытии авторства как обязательного условия появления этой литературы. Следовательно, решение автора сохранить свою анонимность, как и другие решения, касающиеся включения в публикацию или исключения из нее какой-то информации, является аспектом свободы слова и защищено Первой поправкой».

Соглашаясь с решением суда в целом, судья Томас предложил посмотреть на это дело с другой точки зрения. Вместо того чтобы задаваться вопросом, имеет ли анонимное слово историческую ценность, «нам следует определить, защищало ли словосочетание «свобода слова и печати» в его изначальном понимании анонимность политических взглядов, выраженных в форме листовок. Уверен, что защищало».

Несогласный с ним судья Скалиа при поддержке председателя Верховного Суда сказал, что составление анонимных обращений является разрушительным и жульническим делом.

> «Оно наносит вред, потому что освобождает от ответственности, а именно это и составляет саму цель анонимности. Конечно, бывают исключения, и в тех случаях, когда анонимность нужна, чтобы избежать угроз, оскорблений или репрессалий, Первая поправка потребует освобождения от действия Закона Огайо. Однако отменять Закон Огайо в его общем применении и аналогичные законы 48 других штатов Федерации по причине того, что все анонимные сообщения в нашем обществе являются «святая святых», представляется мне искажением прошлого, которое может привести к огрублению будущего».

---

42 McIntyre V. Ohio Elections Commission: the Supreme Court of the United States (МакИнтайр против комиссии по выборам штата Огайо: Верховный Суд США), No. 93–986, Decided April 19, 1995.

Аргументы «за» и «против» повторяются из дела в дело, позволяя предполагать, что анонимность – это ценность свободного и открытого будущего.

Самым последним по времени судебным решением на данную тему стало решение по делу «Сторожевая башня Библии против Страттона» (Watchtower Bible v. Stratton) в июне 2002 г. Суд вынес следующее постановление[43]:

> «Анонимность – это щит, защищающий от тирании большинства [...]. Он иллюстрирует цель, ради которой были приняты Билль о правах и в особенности Первая поправка: защитить от возмездия нетолерантного общества неугодных ему индивидов, а их идеи – от запрета».

Суд постановил, что требование для каждого индивида получать именное разрешение на участие в поквартирной (широкой) пропаганде политических взглядов является неконституционным.

Что касается Интернета, то правительства часто пытались требовать от граждан идентификации личности для предоставления им права высказывать свое мнение. В 1996 г. органы законодательной власти штата Джорджия приняли закон, запрещающий анонимные и псевдонимные высказывания в онлайновом режиме. ACLU предупредил о неконституционном характере данного закона, поскольку он накладывал ограничения на контент в части выражения мнения в компьютерных сетях[44]. Суды согласились, что закон чрезмерно широко и нечетко трактовал этот вопрос и накладывал ограничения на контент в нарушение Конституции.

Законодатели штата Джорджия утверждали, что целью законодательного акта было оказание противодействия мошенничеству, и Суд согласился с тем, что эта цель может представлять для штата интерес. Однако законодательный акт не полностью соответствует этой цели и затрагивает выступления, не содержащие ничего предосудительного и защищаемые законом. Суть в том, что формулировка запрета позволяет применять его к любому выступлению, независимо от того, имеет ли выступающий

---

43 *Watchtower Bible & Tract Society of New York, Inc. et al. v. Village of Stratton et al.: the Supreme Court of the United States, No. 00–1737*, Decided June 17, 2002.

44 ACLU, «Fahrenheit 451.2: Is Cyberspace Burning? How Rating and Blocking Proposals May Torch Free Speech on the Internet».

намерение обмануть или обман уже имел место. Поэтому этот законодательный акт можно применять к широкому спектру случаев передачи информации, которые «ложно идентифицируют» отправителя, но при этом не являются «мошенническими» в значении уголовного кодекса[45].

Это было важное решение, т. к. в то время ряд штатов и стран рассматривали возможность принятия подобных юридических документов.

Поддержка права анонимного доступа и отход от него

Растущая необходимость как можно быстрее решить вопрос обращения с непристойным материалом в онлайновом режиме привела к тому, что в 1996 г. Конгресс США принял Акт о нормах приличия в коммуникациях (Communications Decency Act, CDA). Стороны, участвующие в обсуждении положений этого закона, говорили, что решение по делу МакИнтайр можно с еще большим основанием применить к Интернету. Дэвид Собел (David Sobel), ведущий эксперт по данному вопросу, сказал:

> «Независимо от того, что ищут посетители интернет-сайтов – информацию по беременности несовершеннолетних, СПИД или другим болезням, передающимся половым путем, по классическим литературным произведениям или поэзии авангарда, они осуществляют свое конституционное право на выполнение этих действий анонимно и конфиденциально. А CDA хочет это право нарушить»[46].

Те же идеи стояли за решением суда:

> «Анонимность важна для тех пользователей Интернета, которые ищут в нем деликатную информацию, например, для посетителей веб-сайтов Critical Path AIDS Project или Queer Resources Directory – ведь эти веб-сайты посещают в основном молодые люди нетрадиционной ориентации, или для пользователей Stop Prisoner Rape. Многие из людей,

---

45 *American Civil Liberties Union of Georgia V. Miller (Американский Союз в защиту гражданских свобод штата Джорджия против Миллера).* 977 F. Supp. 1228 (1997).

46 Electronic Privacy Information Center, «Internet «Indecency» Legislation: An Unconstitutional Assault of Free Speech and Privacy Rights» (Электронный центр защиты информации. Законодательство о непристойности в Интернете: неконституционные нападки на права на свободу слова и неприкосновенность частной жизни), (Washington DC: 1996).

входящих в список рассылки последнего сайта, попросили сохранить их анонимность из-за лежащего на них позорного пятна тюремного изнасилования».

Действие Акта было опротестовано на основании действия положений об идентификации, анонимности и свободы слова.

Однако анонимность пользователей не идет дальше провайдеров интернет-услуг. Неудивительно, что режим Мои (Moi) в Кении регулярно требовал от провайдеров предоставлять списки своих абонентов; что пользователи интернет-кафе в Бирме должны регистрироваться и указывать свои паспортные данные и адреса; что Южная Корея предложила установить порядок, по которому национальные паспортные данные должны быть предоставлены до того, как человек получит право размещать свои сообщения на «досках объявлений» общественных организаций; что пользователи в Италии должны безо всяких оснований предъявлять паспорта в интернет-кафе; что растущее беспокойство вызывает закон, требующий установки систем наблюдения в интернет-кафе одного из городков Калифорнии[47]. Полиция Индии требует от властей штата Махараштра установить порядок, по которому Интернет-кафе могут получить лицензии только после установки фильтров на программном обеспечении; помимо этого, все посетители должны будут в обязательном порядке заполнять длинные анкеты с указанием своих адресов, номеров телефонов и других данных, а также предъявлять удостоверения личности с фотографией[48]. Установление идентичности пользователей услуг интернет-провайдеров и разглашение этой информации вызывает все больше и больше вопросов.

Самым известным делом, связанным с раскрытием информации об идентичности в Интернете, стало дело anon.penet.fi. Управлял этим анонимным римейлерным сервисом Йохан Хельсингиус (Johan Helsingius) из Финляндии. После трех лет работы, когда общее число

---

47 Anita Ramasastry, «Can a City Require Surveillance Cameras in Cybercafes without Violating the First Amendment? A California Court Rules on the Issue» (Может ли город требовать установки камер слежения в интернет-кафе, не нарушая при этом Первую поправку? Один из судов Калифорнии выносит решение по данному вопросу), *Findlaw's Writ Legal Commentary*, February 19, 2004.

48 Zubair Ahmed, «Bombay Plans Cyber Café Controls» (Бомбей планирует установить средства контроля в интернет-кафе), *BBC News Online*, January 27, 2004.

пользователей достигло 500 000, а в день обрабатывалось более 7000 сообщений, сервис был закрыт[49]. Полиция Финляндии предъявила Хельсингиусу ордер на обыск в связи с расследованием заявления, поступившего от Церкви сайентологов, обвинявшей Хельсингиуса в использовании anon.penet.fi для разглашения частной информации, взятой из компьютеров церкви, и размещении ее на сайте alt.religion.scientology в USENET.

22 августа 1996 г. окружной суд г. Хельсинки вынес постановление, обязывающее г-на Хельсингиуса передать полиции электронный адрес отправителя[50]. В качестве обоснования причины вынесения данного постановления суд привел пример, что свидетель не имеет права уклоняться от предоставления информации в ходе судебного заседания, что сообщения, о которых идет речь, были направлены в общедоступную сеть, и что публичные сообщения не защищены законом. Хельсингиус отверг данное требование, заявив, что конфиденциальность почтовых отправлений, телефонных разговоров и других личных сообщений защищена Конституцией Финляндии и не может быть нарушена в ходе предварительного расследования мелкого правонарушения, коим являлось выдвинутое против него обвинение в нарушении авторского права. На основании решения окружного суда, после пяти обысков, которые проводила полиция в связи с поступлением новых обвинений в нарушении авторских прав и сообщений, содержащих оскорбления в адрес официальных лиц других стран, Хельсингиус был вынужден закрыть свой сервис[51].

Определенную роль в этом решении сыграл страх быть обвиненным в преступлении. The London Observer цитировала консультанта ФБР, который сказал, что до 90% детской порнографии, которую он нашел в Интернете, проходила через римейлер Хельсингиуса[52]. После

---

49 Daniel Akst, «Postcard from Cyberspace: The Helsinki Incident and the Right to Anonymity» (Открытка из киберпространства: случай в Хельсинки и право на анонимность), *Los Angeles Times*, February 22, 1995.

50 Johan Helsingius, «Press Release: Johan Helsingius Closes His Internet Remailer» (Пресс-релиз: Йохан Хельсингиус закрывает свой римейлер), Penet.fi, 1996.

51 Johan Helsingius, «Press Release: Johan Helsingius Closes His Internet Remailer», (Penet.fi, 1996).

52 CNET Staff, «Remailer» Service Shut Down» (Служба римейлера закрыта), CNET *News.com*, August 31, 1996, 2:00pm, PT 1996.

расследования, проведенного финской полицией, обвинение Observer оказалось беспочвенным – за год до статьи в Observer полиция подтвердила, что деятельность римейлера была ограничена, и передача изображений была запрещена. Римейлер также обвиняли в том, что им часто пользовались криминальные лица из России[53]. Под натиском всех этих обвинений сервер был закрыт, несмотря на то, что он использовался одной британской организацией для предотвращения суицида отчаявшихся людей, не желающих раскрывать свои имена[54].

Ограничение свободы слова за счет введения массового надзора

Личность пользователей раскрывается все чаще. Во многих странах мира суды выносили постановления, обязывающие раскрывать личность людей, помещающих объявления в Интернете, людей, осуществляющих электронные рассылки, и рядовых пользователей. Авторское право, предписывающее предоставлять информацию о предполагаемых пользователях файлов, усугубляет ситуацию в сфере защиты неприкосновенности частной жизни человека. На сегодняшний день музыкальная и звукозаписывающая отрасль в США выдала более 2400 повесток[55].

Одним из наиболее актуальных дел, находящихся на рассмотрении Окружного суда США по Восточному округу Пенсильвании, является дело между BMG Music и 203 анонимными и не связанными друг с другом людьми. Звукозаписывающая компания обвиняет ответчиков в предоставлении другим пользователям Интернета защищенных авторским правом музыкальных записей. Таким образом, ответчиков об-

---

53 Paul A. Strassman and William Marlow, «Risk Free Access into the Global Information Infrastructure Via Anonymous Re-Mailers» (Устойчивый доступ к глобальной информационной инфраструктуре через анонимные римейлеры. Доклад, представленный на симпозиуме по Глобальной информационной инфраструктуре). Information, Policy & International Infrastructure, Cambridge, MA, January 28–30, 1996.

54 CNET Staff, «Remailer» Service Shut Down».

55 Electronic Frontier Foundation, *Subpoena Database Query Tool* (Организация по защите свободы слова в электронных коммуникациях, «Средство запроса информации из БД о повестках в суд»). EFF, December 1, 2003 [cited February 2004].

виняют в участии в незаконном анонимном общении в Интернете. Особенность ситуации в том, что, поскольку анонимное слово находится под защитой конституции, повестка в суд по поводу выдачи информации об абоненте подпадает под иммунитет при условии соответствия установленным требованиям. Возможно, что установление личности этих людей плохо скажется на анонимности общения: интернет-пользователи будут знать, что их смогут идентифицировать люди, способные ложно обвинить их в нарушении закона, даже не имея намерения затевать судебный процесс[56].

Раскрытие персональной информации имеет все шансы превратиться в актуальнейшую проблему. Ход развития государственной политики заставляет провайдеров услуг раскрывать правоохранительным органам идентичность людей, пользующихся их коммуникационными услугами. Такое раскрытие не заканчивается информацией об абонентах; оно затрагивает также данные о трафике.

Доступ к данным о трафике представляется проблематичным с позиций защиты неприкосновенности частной жизни. По мнению группы экспертов Еврокомиссии по неприкосновенности частной жизни и защите данных[57], информация о трафике и современные коммуникационные инфраструктуры становятся все более деликатной сферой.

Особенностью телекоммуникационных сетей и Интернета в особенности является их способность генерировать огромные объемы переменных данных (данных, созданных с целью обеспечения правильных соединений). Возможности для интерактивного использования сетей (определяющая характеристика многих интернет-сервисов) еще больше увеличивают объем таких данных. Обращаясь к онлайновой газете, пользователь «взаимодействует» с ней путем выбора страниц, которые он хочет прочитать. Эти выборы создают «кликовый поток» переменных данных. В отличие от него, более традиционные новости и информационные услуги используются значительно пассивнее (телевиде-

---

56 Public Citizen et al., «Memorandum in Response to Motion for Expedited Discovery in BMG Music, Et A., V. Does 1–203» (Меморандум в ответ на ходатайство на ускоренное расследование по BMG Music, Et A., против Дуес 1–203), United States District Court for the Eastern District of Pennsylvania, 2004.

57 Article 29 Working Party, «Recommendation 3/97: Anonimity on the Internet» (Рекомендация 3/97: Анонимность в Интернете), Brussels: European Commission, 1997.

ние, например), интерактивность которых ограничена офлайновым миром газетных киосков и библиотек. Несмотря на то, что в ряде юрисдикций переменные данные получают некоторую степень защиты в соответствии с законом, защищающим конфиденциальность переписки, колоссальный рост объемов этих данных представляет собой, тем не менее, законное основание для беспокойства.

Этот рост данных фактически усугубляется по причине принятия определенных законов.

В 90-е годы XX века две международные организации работали над соглашениями по международному сотрудничеству в области изучения и предотвращения высокотехнологичных преступлений или «киберпреступности». Практически с 1995 г. «Большая восьмерка» промышленно развитых стран проводит регулярные совещания по методам гармонизации, создания новых возможностей для исследований и способов сотрудничества. Одновременно с этим в 1997 г. Совет Европы (СЕ) – международное объединение 43 государств-членов для выработки соглашений – работал над «Конвенцией по киберпреступлениям» (Convention on Cybercrime), которую завершил и представил для подписания в ноябре 2001 г. Результат работы этих двух организаций имеет большое значение для раскрытия персональной информации провайдерами интернет-услуг.

Европейская конвенция по киберпреступлениям требует от ратифицировавших ее государств вынуждать провайдеров раскрывать информацию о своих абонентах, хранить данные о трафике и предоставлять их в случае расследования какого-либо преступления. Сложность ситуации усугубляется тем, что эти права могут стать основой для обмена разведывательными данными между странами: когда одна страна обращается к другой с просьбой предоставить те или иные данные, а вторая страна должна выполнить эту просьбу, запросив соответствующую информацию у действующего в этой стране поставщика услуг. На страны оказывается давление по принятию данной конвенции. Возможно, эта конвенция будет способствовать международному распространению американской системы защиты авторских прав, в частности, в предоставлении доступа к информации о пользователях и к иным данным в других странах даже в тех случаях, когда подобная информация не может быть получена в США.

Доступ к данным о трафике становится еще более противоречивым делом, когда провайдеры интернет-услуг вынуждены в силу закона архивировать на длительный срок разные виды данных о трафике, что противоречит самому духу закона о неприкосновенности частной жизни. «Большая восьмерка» постоянно поддерживала идею сохранности данных о трафике. Идея эта возникла в США в 90-е годы XX века. Тогдашний директор ФБР говорил:

> «Мы будем побуждать интернет-провайдеров к тому, чтобы они поддерживали абонентов и хранили информацию об осуществляемых ими поисках в течение определенного периода времени; сегодня, в отличие от телефонных компаний, они уничтожают ее слишком быстро. Эти записи могут быть очень важны для идентификации и даже отслеживания дел [по детской порнографии]. Это будет очень полезная вещь, и мы надеемся, что она заработает, пусть даже на добровольной основе. Мы надеемся, что определение и сохранение интернет-провайдерами информации о личности абонента будет другой добровольной мерой, которая должна помочь нам, и мы в настоящее время проводим встречи с провайдерами, чтобы убедиться, что они готовы помогать нам»[58].

Позднее США стали продвигать эту политику в ЕС и «Большой восьмерке». В октябре 2001 г. Президент Джордж Буш обратился с письмом к Президенту Еврокомиссии, в котором рекомендовал принять изменения в европейской политике, «рассмотреть вопросы защиты данных в контексте применения законодательства и антитеррористического императива» и, в конечном итоге, «пересмотреть проект директив по неприкосновенности частной жизни, призывающих к обязательному уничтожению данных, в направлении разрешения сохранения подобной информации в течение целесообразного периода»[59]. В основе этого предложения лежали рекомендации Департамента юстиции США Еврокомиссии, гласящие, что «процедуры защиты данных при об-

---

58 Louis Freeh, «Hearing of the Commerce, Justice, State and the Judiciary Committee – Subject: FY '99 Appropriations for Proposal to Prevent Child Exploitation on the Internet» (Ассигнования на предложение по предотвращению эксплуатации детей в Интернете), Washington DC: Federal Bureau of Investigation, 1998.

59 President Bush, «Letter to President of the European Commission: Proposals for US-EU Counter-Terrorism Cooperation» (Президент Буш, Письмо к Президенту Еврокомиссии: предложения по сотрудничеству между США и ЕС в борьбе с терроризмом), Brussels: 2001.

мене правоприменительной информацией должны быть сформулированы так, чтобы не подрывать международное сотрудничество»[60], и что

> «Любой режим защиты данных должен устанавливать баланс между защитой неприкосновенности частной жизни, законными потребностями провайдеров услуг по обеспечению безопасности своих сетей и предотвращением мошенничества и развитием общественной безопасности»[61].

Очень похожая формулировка появилась в документах «Большой восьмерки» после проведенного в мае 2002 г. саммита по вопросам сохранения данных.

> «Сделать так, чтобы законодательство по защите данных, в том виде, в котором оно вступило в силу, принимало во внимание общественную безопасность и другие общественные ценности, в частности, за счет разрешения удерживать и хранить данные, необходимые для обеспечения безопасности сети, расследований или судебных преследований, в особенности применительно к Интернету и другим новейшим технологиям»[62].

Понимая, что хранение данных о трафике является критически важным делом в борьбе с терроризмом, ряд стран принял политику хранения этих данных. В декабре 2001 г. меры по хранению данных были представлены и приняты в рамках антитеррористического закона Великобритании, примеру которой последовала Франция и многие другие страны ЕС, а за ними – и другие страны, включая Южную Африку и Аргентину. Все эти страны требуют теперь от интернет-провайдеров и телефонных компаний хранить в течение длительного времени данные о трафике их клиентов, если эти данные могут представлять

---

60 United States Government, «Comments of the United States Government on the European Commission Communication on Combating Computer Crime» (Правительство США, Комментарии Правительства США о докладе Еврокомиссии по борьбе с киберпреступлениями), Brussels: 2001.

61 United States Government, «Prepared Statement of the United States of America, Presented at European Union Forum on Cybercrime» (Правительство США, «Подготовленный доклад США, представленный на Форуме ЕС по киберпреступлениям»), Brussels: 2001.

62 G8 Justice and Interior Ministers, «G8 Statement on Data Protection Regimes» (Министры юстиции и внутренних дел «Большой восьмерки», «Доклад Б8 о режимах защиты данных»), Mont-Tremblant: G8 Summit, 2002.

ценность для расследования любого вида преступлений. В Алжире предлагалось регистрировать имена, адреса и логи клиентов поставщиков интернет-услуг, но затем эта практика была приостановлена. США пока подобных решений не приняли.

Новая политика позволяет осуществлять массовый надзор и совместное использование полученной персональной информации разными странами. Данными с мобильных телефонов теперь могут обмениваться государственные органы Франции и США, занимающиеся расследованием уголовных преступлений. Список IP-адресов, которые связывались с сервером в Великобритании, систематически сохраняется провайдерами интернет-услуг и передается местным властям с минимальными ограничениями; они также могут стать предметом обмена с иностранными государственными органами на основании еще более нечетко прописанной правовой процедуры.

Создается впечатление, что широкая общественность практически ничего не знает об этих режимах массового надзора. Всю тяжесть ситуации мы осознаем только тогда, когда появятся дела о нарушении авторского права, в суде обнародуют данные о том, как какой-то человек на протяжении нескольких лет пользовался Интернетом, пересылая песни пользователям в других странах мира, и когда данными расследования будут обмениваться с истцами в США.

Возможно, только тогда мы начнем задавать вопрос, действительно ли Интернет и информационное общество существуют в соответствии с принципами свободы. Скорее всего, такой путь может привести к замораживанию свободы выражения мнения: мы будем менее склонны получать доступ к материалам, зная, что наш провайдер интернет-услуг должен хранить запись наших контактов в течение срока, установленного государством, и что эта информация может быть передана местным властям и даже в другие страны. Мы будем менее склонны публиковать информацию, поскольку это может привести к тому, что власти иностранных государств потребуют наши данные и дополнительную информацию, которую хранит наш провайдер, а затем привлекут нас к суду в иностранных юрисдикциях. Мы будем менее склонны участвовать в жизни информационного общества из-за политики, разработанной с целью «сохранения» этого общества за счет «обновления» ранее принятых законов и разработки новых, для участия в сегодняшних войнах и удовлетворения интересов вчерашнего дня.

V.

Рекомендации для политики завтрашнего дня и предстоящих всемирных саммитов по информационному обществу

Наш мир чрезвычайно разнообразен. Разные страны по-своему трактуют свободу слова и неприкосновенность частной жизни и используют разные способы их регулирования с разными намерениями, целями и результатами. А ясного представления о последствиях этой политики явно не хватает. Нельзя сказать, что действия стран четко направлены на разрушение свободы выражения мнения, однако нельзя и утверждать, что Интернет – самый главный освободитель и источник сопротивления цензуре (как уже было показано выше). Форма и природа цензуры в Интернете претерпели за последние годы удивительно большие изменения, однако, сочетаясь с новыми методами надзора, они рождают удивление, которое сменяется тревогой.

«Информационное общество» как инструмент риторики провалилось. Термин использовался тогда, когда речь заходила о надежде создания нового мира с передовыми коммуникационными технологиями, способствующими нашему процветанию, развитию знаний и способностей к коллективному участию в делах. Этой мечте никогда не суждено сбыться, как невозможно избавиться от старых административных структур и методов работы.

В число таких структур входят правительства и индустрия, а методы работы включают цензуру «непристойного» и «наносящего вред» материала и контента, охраняемого авторским правом, а также – обвинения в клевете и диффамации. Используя эти методы и новые технологии, государственные органы сумели трансформировать инфраструк-

туру связи, которая в течение определенного времени приводила нас всех в восторг.

Нас с самого начала предупреждали, что невозможно регулировать такую структуру, как Интернет, которая не может не быть транснациональной по своей юрисдикции. Государства не последовали этому совету и принимали законы, устанавливающие в своих юрисдикциях цензуру слова. Тогда появились предупреждения о том, что правила, введенные в одной юрисдикции, могут иметь побочный эффект для других юрисдикций и принести вред не только Интернету, но и демократическим правам граждан. Этот совет также был проигнорирован. В конце концов, пришлось признать, что Интернет не представляет собой нечто уникальное, что транснациональная деятельность всегда имела место и всегда подвергалась регулированию.

За этим последовали новые инициативы. Появились попытки регулировать Интернет как средство массового вещания и применять уже известные методы контроля телевидения к этой новой среде, требуя установки далеких от совершенства фильтров, которые осуществляли избыточную блокировку политических высказываний и пропускали то содержание, которое призваны были блокировать. По собственному усмотрению государственные организации регулировали Интернет и как телефонную систему, в попытке расширить действие ранее принятых правил в отношении установки систем слежки. Они также «актуализировали» режимы авторского права, законы о клевете и диффамации и распространили их действие на новые коммуникационные инфраструктуры.

В результате инфраструктура, которая должна была стать основой для нового глобального общества, превратилась в хаотично и избыточно регулируемую и контролируемую среду. Методы и формы регулирования могут быть различными в зависимости от города, штата, провинции, страны, государственной системы и области деятельности. Контроль осуществляется через инфраструктуру в точках, позволяющих контролировать поток данных. Устанавливаются фильтры и определяется ответственность.

Там, где эффективные методы контроля установить нельзя, остается возможность надзора. Сегодня люди могут обмениваться файлами и высказывать свое мнение, но после того, как их взгляды и привычки будут раскрыты вместе со всей информацией по транзакциям за меся-

цы и годы, как того требует антитеррористическая политика, они могут укрепиться в своем нежелании продолжать обмен. Когда их обяжут предъявлять документы или будут фиксировать на видео во время работы за общественным терминалом или в интернет-кафе, они, скорее всего, будут вести себя по-другому. То, что сначала было заявлено как инфраструктура, стимулирующая разнообразие, стало частью общества, обладающего эффективными средствами управления поведением человека.

Всемирные саммиты по информационному обществу должны были бы приложить все усилия для исправления этой ситуации. Вместо этого, они становятся рупором глав государств, которые, сидя на важных международных совещаниях по установлению режимов надзора, заявляют о своей поддержке национальных «информационных обществ». Нужно проделать серьезную работу, чтобы восстановить свободу в новом обществе, строительством которого мы занимаемся. Серьезная работа уже делается и много сил вкладывается в борьбу с терроризмом и в защиту авторского права. Мы же никак не научимся серьезно относиться к собственным правам.

Еще многое предстоит сделать. Правильность политики следует поставить под сомнение, а законы аннулировать и составить заново. Надо признать, что еще один саммит, который будет проведен под руководством одного из самых репрессивных режимов мира, не станет идеальным форумом для подобной повестки дня. Однако серьезную работу можно начинать уже сейчас, и начинать, пожалуй, нужно с тех мест, в которых сложилась самая тяжелая ситуация. Мы можем возродить мечту об «информационном обществе» в такой форме, чтобы она поддерживала идеи оптимизма и добра, и перестала быть воплощением цинизма. Мы можем убрать границы на пути потоков данных и в области юридической ответственности, снять бремя с наших прав, освободиться от предварительных запретов и вернуться к тому, чтобы мечтать вслух.

Об авторе

Гус Хосейн – сотрудник правозащитной организации Privacy International, консультант Американского союза борьбы за гражданские свободы и сотрудник Лондонской школы экономики и политических наук. Имеет степень бакалавра математических наук в области прикладной математики (Университет Ватерлоо) и докторскую степень в области информационных систем (Лондонская школа экономики). В настоящее время область его научных интересов охватывает вопросы развития международной политики, разработки антитеррористической политики и общих тенденций в сфере неприкосновенности частной жизни и защиты данных. Дополнительная информация: http://is.lse.ac.uk/staff/hosein

Благодарности

Автор выражает благодарность коллегам по Privacy International и особенно Дэвиду Банисару, Саймону Дэвису и Венди Гроссман, также коллегам по GreenNet Education Trust, в том числе Карен Бэнкс и Хитер Форд. Я также хотел бы поблагодарить Институт «Открытое общество» за помощь, оказанную на стадии исследования, и Совет по исследованиям в области общественных наук за поддержку при составлении концептуальной основы данной работы. Я также хотел бы поблагодарить ЮНЕСКО за оценку вклада в данной области, включая и мой собственный.

ПОЛИТИКА ИНФОРМАЦИОННОГО ОБЩЕСТВА:

ОГРАНИЧЕНИЕ И СДЕРЖИВАНИЕ ГЛОБАЛЬНЫХ ПОТОКОВ ДАННЫХ

Гус Хосейн

Редактор *Т.А. Мурована*

Ответственные за выпуск *С. Д. Бакейкин, Е.И. Кузьмин*

Технический редактор *Ю.Ю. Таранова*

Корректор *Т.М. Малинкина*

Издатель:

Межрегиональный центр библиотечного сотрудничества (МЦБС)

105066, г. Москва, 1-й Басманный пер., д. 2а, стр. 1

Тел.: (495) 267 33 34, факс: (495) 657 96 20

www.mcbs.ru

Художественное оформление:
Издательство «Права человека»
119992, Москва, Зубовский бульвар, 17
веб-сайт: www.hrpublishers.org

ИД № 02184 от 30.06.2000. Подписано в печать 27.03.2008.
Формат 60x90 $^{1}/_{16}$. Бумага офсетная. Гарнитура FranklinGothicBook.
Печ. л. 3,0. Печать офсетная. Тираж 1000 экз. Заказ №

Отпечатано на Фабрике офсетной печати,
249039, г. Обнинск, ул. Королева, 6

Политика информационного общества

Full texts of the studies at:
http://www.unesco.org/wsis

Полный текст книги на русском языке
размещен на сайте Российского комитета
Программы ЮНЕСКО «Информация для всех»
http://www.ifapcom.ru