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.