КРИСТИНА ПОТУПЧИК
АННА ФЁДОРОВА

ВЛАСТЬ НАД СЕТЬЮ

КАК ГОСУДАРСТВО ДЕЙСТВУЕТ В ИНТЕРНЕТЕ

Анна Федорова
Кристина Потупчик

Власть над Сетью. Как государство действует в Интернете

Текст предоставлен издательством
http://www.litres.ru/pages/biblio_book/?art=8717302
Кристина Потупчик, Анна Федорова. Власть над Сетью. Как государство действует в Интернете: Алгоритм; Москва; 2014
ISBN 978-5-4438-0890-1

Аннотация

О роли государства в развитии современных медиа спорят многие. Одни считают, что государство приходит в интернет с единственной целью – разрушить его. Другие указывают на неизбежное поражение государственной власти в борьбе с вездесущими цифровыми структурами и активистами. Задача этой книги состоит в том, чтобы рассказать о реальном положении дел в сфере отношений между государством и интернетом. И авторы – известный общественный деятель Кристина Потупчик и политолог Анна Федорова – весьма грамотно справились с этой сложной задачей, изложив анализ в самой простой и доступной каждому читателю форме. Впервые в полном

объеме так популярно и познавательно представлен анализ опыта сосуществования и сотрудничества государства, общества и интернета. Узнай новое о сайтах, на которых сидишь ты! Учись раскручивать себя! Доноси свои идеи в массы! А хочешь – становись видным политиком! Все правила игры на интернет-пространстве – в этой книге!

Содержание

Кристина Потупчик, Анна Федорова
Власть над Сетью. Как государство действует в Интернете

Предисловие

О роли государства в развитии современных медиа спорят многие. Одни считают, что государство приходит в интернет с единственной целью – разрушить его. Другие указывают на якобы неизбежное поражение государственной власти в борьбе с вездесущими цифровыми структурами и активистами.

Задача этой книги состоит в том, чтобы рассказать о реальном положении дел в сфере отношений между государством и интернетом. Мы покажем, что, с одной стороны, все западные демократии, включая США, фактически используют те или иные техники контроля за распространением контента в интернете. Такой контроль чаще всего не только рассматривается обществом в качестве допустимой меры вмешательства в работу Сети, но и прямо поощряется общественным мнением.

С другой стороны, обсуждение взаимосвязи государства и интернета совсем не исчерпывается темой цензуры. Современное государство нуждается в интернете и активно использует его в своих целях. Интернет становится источником ярких побед для современных политиков (уже классическим примером в данном случае являются президентские кампании Обамы, во многом построенные на вовлечении активных избирателей через социальные сети).

Это, в свою очередь, означает, что любое демократическое государство должно поддерживать равный доступ кандидатов на выборные должности к сетевым ресурсам, иметь в своем составе устойчивые институты цифровой демократии.

Что еще более важно, современное государство заинтересовано в развитии инструментов общественного контроля, которые позволили бы сделать его действия более эффективными, прозрачными и легитимными. Такие инструменты также возникают из симбиоза государства и интернета, причем сегодня они также активно внедряются в повседневную практику работы бюрократических систем в развитых странах.

Основная часть книги посвящена анализу этого сложного опыта сосуществования и сотрудничества государства, общества и интернета. Говорить об этом важно именно сегодня, когда мы все еще ищем приемлемые формы ответов на новые вызовы и новые возможности, которые несет с собой интернет. Вопреки мнению скептиков и утопическим представлениям анархистов, западные государства отнюдь не спешат рухнуть под давлением новых медиа. Скорее, они перестраиваются, предоставляя своим гражданам новые гарантии безопасности и новые возможности по участию в политической жизни.

Первый раздел книги посвящен анализу механизмов регулирования интернета, распространенных сегодня в демокра-

тических странах Запада. Здесь мы расскажем, как государство защищает свои интересы в киберпространстве. Как выяснится, в действительности интересы государства чаще всего не противоречат интересам граждан. Запрос на регулирование интернета исходит от различных общественных групп и индивидов, обеспокоенных соображениями защиты частной жизни, сохранением прав интеллектуальной собственности и т. д.

Второй раздел рассказывает о том, как интернет используется политиками для побед на выборах. В отличие от многочисленных спекуляций о свержении политического режима при помощи интернета речь идет о вполне конкретном опыте проведения политических кампаний в социальных сетях.

Наконец, в третьем разделе книги представлен анализ цифровых способов контроля граждан над государством, развития прозрачности государственных услуг и гражданского участия в обеспечении такой прозрачности.

Нашу книгу можно считать своего рода путеводителем по современным формам взаимодействия власти и новых медиа, распространенным в мире. Описав их, мы постараемся показать, что государство не следует представлять в качестве монстра, мечтающего о запрете всего интернета. Однако еще более наивно было представлять его и в качестве посмешища, не способного защищать свои интересы перед лицом сетевых энтузиастов.

Раздел I. Цензура. Как государство контролирует интернет

Цензура в интернете – одна из самых болезненных и спорных проблем современного мира.

Западные демократии стремятся выглядеть защитникам неограниченной свободы слова, часто понимаемой как право человека на доступ к любой информации. Эту декларативную приверженность идеи свободы в интернете следует считать не более чем риторическим приемом, который используется для обоснования политических решений и давления на другие государства.

Реальная практика показывает, что сами западные демократии не могут обойтись без той или иной формы контроля над интернетом. Сегодня в мире практически нет государств, которые полностью отказались от регулирования Сети. Где-то это делается открыто, как в Китае. В других странах – в рамках законов о защите детей или ответственности за спам и распространение вирусного контента, как в США. В любом случае интернет подвергается активной цензуре повсеместно. Различие связано лишь со степенью вмешательства государства.

Какие формы цензура интернета принимает на Западе и, в частности, в США? Ведь там, как известно, действу-

ет Первая поправка к Конституции, запрещающая ограничение свободы слова[1]. Так что даже употребление самого слова «цензура» в данном контексте является спорным и проблематичным. Для описания интересующего нас феномена используются другие, более идеологически нейтральные слова, в первую очередь – регуляция (regulation).

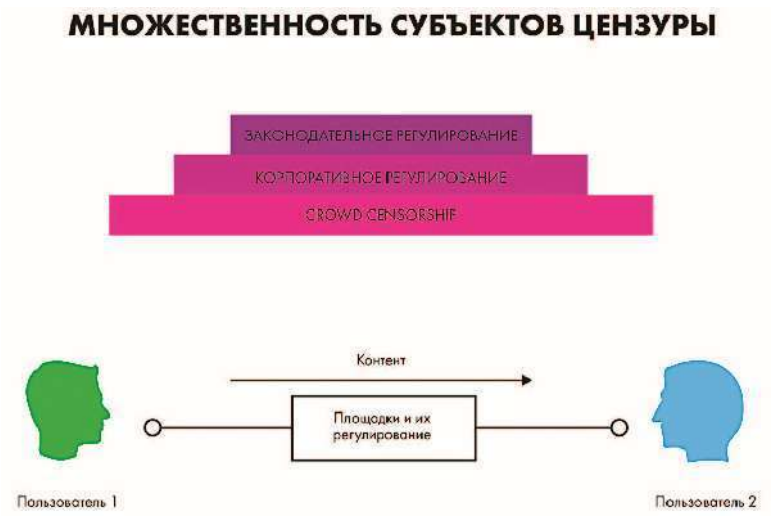
Фактически мы имеем дело с заменой излишне идеологически окрашенного слова его словарным определением. Ведь что такое «цензура»? Это именно регуляция доступа к производству, распространению и потреблению контента (информации).

В западных демократиях, где действуют правовые системы, ориентированные на защиту свободы слова, осуществляются и реализуются наиболее продвинутые и современные технологии регуляции доступа потребителей к контенту, т. е., называя вещи своими именами, технологии цензуры.

При этом мы исходим из предположения, что субъектом цензуры (регуляции) на Западе является не только государство с его традиционными методами правового регулирования, но и другие агенты социального действия: крупные интернет-площадки, корпорации, сообщества и даже сами потребители и производители контента.

---

[1] «Конгресс не должен издавать ни одного закона, относящегося к установлению религии или запрещающего свободное исповедание оной либо ограничивающего свободу слова или печати либо право народа мирно собираться и обращаться к правительству с петициями об удовлетворении жалоб».



Цензурирование интернета всегда является не просто репрессивным актом государства, но процессом, находящимся на пересечении противоположных социальных импульсов, предметом общественного договора.

Зыбкость и неопределенность границ между офлайном и онлайн-пространством, границ между «privacy» и «publicity» пользователя социальных сетей являются источником постоянного напряжения в обществе. Ведь в пространстве новых медиа владение технологией уже не является монополией государства, что открывает новую страницу в контроле за распространением информации.

Цензура интернета оказывается тесно связанной с двумя фундаментальными ценностями современного мира. Поми-

мо свободы слова, это также право на частную жизнь.

Обе тенденции – и свободное распространение контента, и его ограничение – связаны с потребностями пользователя, вынужденного делать постоянный выбор между свободой и безопасностью.

Некорректно считать, что контроль над информацией нужен только государству.

Сам пользователь порождает его потребностью в безопасности/усечении (privacy) и безопасности/контроле (спам-фильтр) информации.

Регулирование интернета принимается обществом в том случае, когда оно оказывается связанным с представлениями о необходимой безопасности.

Для большинства пользователей, не обладающих специальными техническими знаниями, Сеть является не только пространством возможностей, но и источником разнообразных угроз.

Также общество положительно воспринимает регулирование интернета в тот момент, когда она объясняется в терминах увеличения степеней контроля над информацией: когда человек оказывается вправе выбирать не только то, что он хочет видеть в Сети, но и то, чего не хочет.

Таким образом, цензура в интернете может быть понята и описана как регулирование передачи знания (информации) и установление своего статуса по отношению к нему основными субъектами (пользователем, сайтом, корпорацией, го-

сударством).

Отношение к интернет-цензуре меняется в момент насыщения общества информацией (окончания информационного голода), когда любая информация уже не считается благом, но начинает рассматриваться с точки зрения полезности реципиенту.

По данным проведенного Левада-центром опроса, 63 % российских респондентов считают, что в Сети существует множество опасных сайтов и материалов, доступ к которым следует ограничивать. Кроме того, 65 % респондентов заявили, что доступ в интернет необходимо ограничить и для некоторых категорий граждан[2].

---

2 http://www.levada.ru/10-10-2012/tsenzure-v-internete-obespechena-

Опрос, проведенный Фондом Открытой Новой Демократии (см. главу 6), также подтвердил: большинство граждан РФ считают, что государство должно блокировать доступ к определенным сайтам.

obshchestvennaya-podderzhka-63-grazhdan-vystupayut-za-og

Глава 1. Почему современный интернет нуждается в цензуре

Чтобы регулировать интернет, правительствам, корпорациям и обществу нужны аргументы. В этой главе мы рассмотрим основные дискуссии, которые ведутся сегодня в мире по поводу оснований, методов и последствий законодательного регулирования интернета.

Границы сообществ в интернете все более расходятся с границами государств. Все большее число пользователей вступают в коммуникацию на языке графики и мемов, уже лишь частично на английском языке. Данные об этом хранятся на серверах, разбросанных по всему миру даже в пределах одного сайта, и находятся под юрисдикцией разных стран.

Это происходит на фоне дальнейшей эволюции самого интернета, нынешний этап которой принято описывать как переход от web 2.0 к web 3.0. Большинство авторов понимают web 3.0 как профессионализацию процесса создания контента и услуг в рамках инструментов, предоставленных web 2.0. Иными словами, на нынешнем этапе развития Сети ведущую роль в ней снова начинают играть профессионалы, адаптировавшиеся к новым условиям.

Напомним, web 2.0 предоставляет пользователям возможности для свободного самовыражения. Это демократизиру-

ет медиапространство, уничтожая иерархии и делая любого блогера потенциально равным крупному СМИ (в случае вирусного эффекта). Роли «экспертов» и «профессионалов» в мире web 2.0 размываются.

В противовес этому web 3.0 отражает как раз появление экспертов, оценку информации и анализ данных. Т. е. представляет собой переход к регулированию интернет-контента как следующей стадии развития интернета[3]. Законодательство, направленное на регулирование интернета, по сути, просто фиксирует этот процесс в офлайне.

Законодатели в европейских странах видят главную задачу регулирования Сети в охране прав индивида на частную жизнь. В Европе предметом соответствующих дискуссий о цензуре в Сети является личность, тогда как для США вопрос о взаимодействии интернета и государства чаще формулируется в терминах контроля. Даже если, по сути, речь идет о тех же правах на информацию, они чаще описываются через «контроль, слежение, регулирование».

Показательный пример произошел в 2010 году, когда власти США обязали крупнейшие сайты для разработчиков свободного софта – SourceForge.net и Google Code – закрыть доступ для пользователей Кубы, Ирана, Судана, Ливии, Сирии и Северной Кореи[4]. Ограничение прав граждан других

---

[3] http://www.javajazzup.com/issue3/page59.shtml http://webtrends.about.com/od/web20/a/what-is-web-30.htm

[4] http://webplanet.ru/news/life/2010/01/25/notsoopen.html

государств не вызвало, что характерно, такой вспышки недовольства, как подобные действия в отношении американцев.

Государство и интернет в США сосуществуют в пространстве, ограниченном, с одной стороны, Первой поправкой, а с другой – целым комплексом юридических механизмов, связанных с «национальной безопасностью», угрозой детству или чужой собственности. Здесь возникает множество социальных мифов и фобий относительно того, какие необозримые возможности для контроля открывает современное состояние интернета. Характерным примером тематических публикаций в американских СМИ являются статьи вроде «Как государство использует социальные сети, следит за тобой и предсказывает твои шаги»[5].

Среди американских организаций, борющихся за цифровые права, одной из наиболее известных (и показательных с точки зрения культурных различий) является The Global Internet Freedom Task Force (GIFT, «Силы по борьбе за интернет-свободу»). Она была создана в 2006 году государственным секретарем Соединенных Штатов Кондолизой Райс «для мониторинга и реагирования на угрозы свободе выражения мнений в интернете». Внутренней задачей организации является контроль соблюдения интернет-свобод под руководством местных полицейских департаментов. Решения GIFT принимает, опираясь на междисциплинар-

---

[5] http://www.forbes.com/sites/michaelpeck/2013/02/11/social-network-software-lets-government-predict-your-movements/

ную экспертизу Департамента политики международных отношений, права человека, демократизацию, защиту бизнеса, корпоративной социальной ответственности и соответствующих особенностях стран и регионов.

Решения сообщаются Генеральному секретарю через заместителя госсекретаря по вопросам экономики, бизнеса и сельского хозяйства и заместителю государственного секретаря по демократии и глобальным вопросам[6]. Целевая группа GIFT рассматривает внешнеполитические аспекты свободы в интернете, в том числе:

• Использование технологий для ограничения доступа к политическому содержанию и влияние этого на американские компании;

• Использование технологий для отслеживания и подавления диссидентов;

• Попытки изменить структуру управления использованием интернета в целях ограничения свободного потока информации.

GIFT является важным социальным маркером для американского общества и была упомянута государственным секретарем США Хиллари Клинтон в речи, посвященной свободе интернета в Вашингтоне 21 января 2010 года.

Клинтон заявила: «Мы рассматриваем GIFT в качестве форума для устранения угроз интернет-свободе во всем мире и призываем американские СМИ играть активную роль

[6] http://2001-2009.state.gov/g/drl/lbr/c26696.htm

в условиях настораживающих попыток иностранных правительств цензурировать и отслеживать интернет»[7].

Американские власти используют подобную риторику и подобные организации для того, чтобы фактически выступать в качестве главных и по возможности единственных цензоров в Сети. Дело Эдварда Сноудена ярко продемонстрировало этот статус США, которые желают цензурировать всех, оставаясь неподцензурными никому.

Публичное осуждение стран вроде Китая, регулирующих интернет-контент, на фоне постоянных попыток ввести законодательные основания для регуляции контента в самих США воспринимается чаще всего как лицемерие и вызывает общественное негодование. Требование государственной прозрачности одновременно со срочным законодательным запретом на просмотр выложенных онлайн документов Wikileaks – действие того же порядка.

Примером политики двойных стандартов может служить речь Хиллари Клинтон на конференции о свободе интернета в Гааге в 2011 году. Говоря с позиции истового борца за свободу слова в интернете, Клинтон акцентировала внимание на том, как «с каждым заблокированным разговором интернет для нас становится меньше». С идеологической точки зрения ее речь была очень близка риторике экологов: «сохранить фундаментальную свободу онлайн для будущих поколений». Большинством СМИ эти слова Клинтон были расце-

[7] http://www.foreignpolicy.com/articles/2010/01/21/internet_freedom

нены как лицемерие, а реальные действия американской администрации – как репрессивные и весьма далекие от озвученных идеалов[8].

В этом контексте нужно упомянуть и о доктрине кибербезопасности США. Соответствующий законопроект был подписан в феврале 2013, однако бурные прения по его поводу идут с весны 2011 года. Законопроект сразу встретил активное сопротивление в связи с предлагаемым ростом контроля правительства за интернетом. В числе прочего наибольшей критике подвергся пункт о том, что если США подвергается хакерской атаке, инициируемой враждебным государством, то Америка вправе считать это объявлением войны и ответить на эту атаку традиционной военной операцией. По сути, такое понимание проблемы может быть рассмотрено как попытка экспансии американской интернет-цензуры на весь мир. При этом формулировки, которыми сопровождается законопроект, апеллируют к национальной безопасности и заботе государства о гражданах. В итоге в феврале 2013 был подписан измененный вариант законопроекта, являющийся тем не менее одним из самых агрессивных на сегодняшний момент среди демократических стран.

Доступ в интернет как право человека

В ноябре 2011 года Католическая служба новостей рас-

[8] http://www.salon.com/2011/12/09/hillary_clinton_and_internet_freedom/

пространила следующую информацию: «интернет представляет собой глобальное общественное благо, которое должно быть доступным для всех», «демократическое правительство должно работать, чтобы гарантировать доступ к интернету, и принять общие принципы, описывающие использование Сети в терминах универсальных прав человека», «то, что закон разрешает или запрещает офлайн, должно также быть отражено онлайн», и даже «…мир нуждается в «Хартии прав человека в интернете»»[9].

Этот пример интересен, поскольку в нем речь идет о позиции Ватикана, что вносит в понимание «интернета как блага» для европейской культуры весьма определенные коннотации. В рамках европейского сознания интернет оказывается хорошо осмысленным явлением, вписанным в рамки религиозной жизни. В католицизме интернету покровительствует отдельный святой (выбранный на основании того, что каталогизировал данные в далеком 17 веке на тех же основаниях, на которых сегодня построены базы данных[10]), описано, когда и каким образом к этому святому следует обращаться. Более того, отношениям католической церкви и интернета посвящено немало публикаций на сайте Ватикана[11].

На данный момент понимание доступа в интернет как

---

[9] http://www.catholicnews.com/data/stories/cns/1104530.htm

[10] http://www.catholic-saints.info/patron-saints/patron-saint-of-internet.htm

[11] http://www.vatican.va/roman_curia/pontifical_councils/pccs/documents/rc_pc_pccs_doc_20020228_church-internet_en.html

права человека уже реализуется на практике. В Испании, Греции, Франции, Эстонии и Коста-Рике доступ в интернет уже является законным правом граждан. А в Финляндии даже уточнена скорость доступа, на которую имеет право гражданин (не менее 1 Mbit/s, а с 2015 года – 100 Mbit/s)[12].

Доступ в интернет как право вводится через «право на получение и распространение информации». Это не единственное существующее определение места интернета в официальных источниках. В стратегии ПАСЕ на 2012-2015 его определение через права человека соседствует с пониманием интернета как «ресурса», «пространства» или «средства»[13].

Хартия прав в интернете была принята в феврале 2001 года в Праге, на семинаре по правам в интернете, Ассоциацией прогрессивных коммуникаций (APC – www.apc.org) – общественной организацией, видящей свою цель в том, чтобы распространять доступ в интернет, а также «делать мир лучше» с помощью интернета. Хартия описывает следующие права:

- доступ в интернет для всех,
- свобода выражения мнений и ассоциаций,
- доступ к знаниям,

---

[12] http://yle.fi/uutiset/1mb_broadband_access_becomes_legal_right/ 1080940

[13] http://www.coe.int/t/informationsociety/conf2011/IG_CoEStrategy_EN.pdfhttp://www.ip-watch.org/2012/03/15/council-of-europe-passes-internet-governance-strategy/

• совместное обучение и творчество – свободное и открытое программное обеспечение и технологии,
• неприкосновенность частной жизни,
• наблюдение и шифрование, управление интернетом,
• осознание, защита и реализация прав.

APC утверждает: «Возможность обмениваться информацией и свободно общаться, используя интернет, является жизненно важной для реализации прав человека, закрепленных во Всеобщей декларации прав человека, Международном пакте об экономических, социальных и культурных правах, Международном пакте о гражданских и политических правах, Конвенции о ликвидации всех форм дискриминации в отношении женщин и Всемирной встрече на высшем уров-

не по вопросам информационного общества (WSIS)». Это мероприятие прошло в 2008 в Рио-де-Жанейро, и на нем было установлено, в частности, что целью является не разработка новых правовых оснований в отношении интернета, но реинтерпретация существующих прав человека с учетом потребностей и проблем информационного общества.

Интернет-цензура и Анонимус

Еще одним важным игроком современного интернета и попыток регулировать его являются хакерские группировки, самая известная из которых называется Anonymous (Анонимы).

Если законы защищают вполне материальных личностей, их права, границы и интеллектуальную собственность, то против цензуры зачастую протестует некоторый «коллективный цифровой разум», «анархический глобальный мозг». Существование такого «самосознания» у интернета является одним из важных современных мифов[14].

Этот «цифровой разум» является глашатаем воли децентрализованного интернет-сообщества, которое существует ровно в той мере, в которой интернет пополняется контентом. Оно не может не выступать за максимально открытое наполнение интернета, оно не может не протестовать против цензуры: так оно борется за свою жизнь.

---

[14] http://edition.cnn.com/2012/02/09/world/anonymous-explainer/index.html

Анонимы не защищают ничьих конкретных интересов, потому что не распадаются на субъектов в привычном понимании слова. «Анонимы являются группой ровно в том смысле, в котором ею является стая птиц. Откуда вы знаете, что перед вами стая? Потому что они летят в одном направлении. В любой из моментов к ним может присоединиться или улететь любое количество птиц. Каждый, кто хочет быть Анонимом, может присоединиться и работать на достижение целей. Мы координируемся, но действуем независимо» [15].

В еще не оконченном диалоге о границах и отношениях между онлайном и офлайном точка зрения Анонимов состоит в том, чтобы разграничить их полностью, исключить возможность влияния офлайн-преференций на свободу пополнения интернета контентом. Как сказал в интервью газете «Гардиан» один из представителей группировки: «Мы против корпораций и правительств, которые вмешиваются в интернет. Мы считаем, что интернет должен быть открытым и свободным для всех. Мы не забываем, мы не прощаем, имя нам – легион!»[16].

С Анонимами оказываются так или иначе связаны все основные громкие прецеденты вокруг политики и цензуры: Арабская весна, Викиликс и т. д. Представителей движения периодически пытаются поймать, но чаще всего неуспешно.

---

[15] http://www2.citypaper.com/columns/story.asp?id=15543

[16] http://audioboo.fm/boos/233905-meeting-coldblood-a-member-of-the-anonymous-community-wikileaks

Якоб Аппельбаум, связанный с Викиликс и анонимайзером Тор, был задержан, обыскан и допрошен Таможенной службой США в аэропорту Сиэтла после повторного въезда-выезда на каникулы в Исландию. Согласно твитам, которыми сопровождалось задержание, представители спецслужб были весьма огорчены отсутствием у него мобильного телефона и компьютера, явно намереваясь ознакомиться с их содержанием и называя свои действия «случайной проверкой». При этом Якоб уже подвергался аналогичной «случайной процедуре» в Ньюаркском аэропорту. Подобные эпизоды уже имели место с другими причастными к Викиликс персонами, когда их компьютеры и мобильные телефоны отбирались, а свобода их передвижения ограничивалась. Случай с Якобом заново поставил вопрос о том, каким образом распределена ответственность между онлайном и офлайном и насколько правомерно офлайн-воздействие по отношению к фигурантам, задействованным в увеличении свободного течения информации в интернете[17].

[17] http://boingboing.net/2011/01/12/wikileaks-volunteer-1.html

Каждая попытка построения нормативных границ в интернете становится для Анонимов поводом для демонстративного акта нарушения других границ, значимых и важных для «жителей офлайна». Чем выше уровень границ, которые удалось нарушить – тем более удачным считается такой акт кибертерроризма. Атака на сайты ФБР в ответ на арест владельцев хостинга с такой точки зрения – высший пилотаж. Атаке при этом подвергается не государство как таковое, а любой источник нормативного воздействия или политической воли, будь то физическое лицо или торговая корпорация.

Анонимы постепенно начинают позиционировать себя

как защитников общечеловеческих ценностей и благ офлайнового мира вообще. Доказательством тому служит одно из громких выступлений Анонимов: видеообращение января 2013, в котором участники группировки говорят, что американское правительство зовет их «террористами», потому что действительно опасается народного восстания. «Правительство Соединенных Штатов упорно лепит на нас ярлык террористов. Вопрос: кого мы терроризируем? Может быть, оно по-настоящему боится нас, народа?»

Группа призывает не к привычным для нее действиям, а к полномасштабной революции с целью свержения правительства и возвращения власти народу. «Мы не призываем коллектив нарушать работу или осуществлять DDoS-атаки сайтов государственных органов США или связанных с ними организаций. Мы не призываем народ снова оккупировать города или протестовать перед зданиями на местах: это не принесло нам каких-либо изменений в законодательстве. Это принесло нам лишь кровопролитие и лживую критику. Последние 12 лет голосование было бесполезным делом. Корпорации и лоббисты – вот кто на самом деле управляет страной и имеет власть над нашими жизнями. Чтобы перестроить наше правительство, мы должны его сначала разрушить. Пробил час нашей демократии, пробил час решения проблемы. Пробил час для Америки начать революцию. Чтобы восстановить наши конституционные права, чтобы быть поэтому свободными, Anonymous вместе с американ-

ским народом решила открыто объявить войну правительству Соединенных Штатов. Это призыв к оружию».

В видеоролике перечисляется длинный перечень злоупотреблений, которые «более недопустимы»:

• Мы отказываемся быть полицейским государством.

• Мы отказываемся терпеть бесчеловечное отношение и терять человеческий облик по воле тех самых людей, которые финансируются из наших долларов, уплаченных в виде налогов, чтобы защищать наши города и улицы.

• Мы не позволим правительству распоряжаться нашей судьбой, нашим правом строить свою собственную жизнь.

Мы требуем свободы от правительства, налогообложения, изъятия имущества за долги.

• Вам не приблизиться к нашим дверям и не забрать наше оружие, нашу собственность, вам не заставить граждан этой великой страны участвовать в беззаконии навязанного правительством здравоохранения.

• Мы, народ, отказываемся отдать в ваши руки наше здоровье, наши тела, наши умы, наши жизни.

• Мы не дадим правительству разрешения запускать беспилотники над нашими домами и населенными пунктами.

• Мы должны положить конец Федеральному Резерву. Частный центральный банк не должен выпускать нашу валюту, устанавливать процентные ставки и управлять нашей экономикой. Напротив, нам нужно возвратить контроль над нашей денежной единицей американскому народу, которому он по праву принадлежит[18].

Данная акция могла бы быть рассмотрена как настоящее политическое действие, если б не одна деталь: за последний год Анонимы совершали такие действия десятки раз против правительств разных государств, превращая традиционную форму политического протеста в «троллинг».

В пространстве новых медиа владение технологией уже не является монополией государства, а напротив, государство (как тип принятия решений) раз за разом оказывается в роли «догоняющего» по отношению к ироническим Анонимам,

[18] http://misterq.myblog.ws/tag/usa/

«аборигенам интернета», для которых возможность сохранить анонимность становится важнейшим ценностно-идеологическим конструктом и формой идентичности.

Свобода и цензура: промежуточные выводы

Несмотря на кажущееся противоречие, идея свободы слова и практика цензуры в интернете дополняют друг друга.

Пользователи интернета хотят быть свободными, но это означает, в частности, иметь возможность защищать себя от нежелательного контента. Отсюда появляется представление о регулировании контента как факторе свободы.

В зависимости от конкретной культурной ситуации могут меняться типы контента, подвергающегося такому контролю. Речь может идти о детской порнографии, противоречащей ценностям защиты детства, или о нацистских призывах, атакующих толерантность и терпимость. В рамках этой же логики возникает запрос на защиту пользователей от мошенников, аферистов и маньяков. Острым вопросом становится регулирование социальных сетей, в которых подростки доводят друг друга до самоубийств, а недобросовестные журналисты раскрывают конфиденциальную информацию.

Сторонники цензуры говорят, что оставить Сеть нерегулируемой – это все равно что отдать ее в распоряжение террористов. Они убеждены, что идея абсолютной свободы яв-

ляется лишь теоретической конструкцией, в то время как все существующие в истории человеческие сообщества, включая самые демократические и либеральные, вырабатывали определенные моральные и юридические нормы для контроля за распространением информации.

Глава 2. Какие законы используются для регулирования интернета в США и Европе

Первый законодательный акт, позволяющий правительству блокировать либо фильтровать контент, появился в Англии достаточно поздно – в 2010 году. Сразу же за этим последовало массированная общественная кампания против этой инициативы. Она выразилась, в частности, в исследовании, опубликованном OpenNetInitiative[19] (ONI) – общественной организацией на базе университетов Гарварда, Оттавы и Торонто. Проанализировав интернет-контент на предмет его вредоносности, ONI пришла к заключению, что никакой реальной опасности для жизни и здоровья людей, требующих ограничительных мер, он не представляет. Этой же организацией была разработана классификация цензуры по степе-

[19] http://opennet.net/research/profiles/united-kingdom

ни ее интенсивности и областям применения.

Согласно ONI интернет-цензура может быть введена различными способами, среди которых присутствуют как технологии фильтрации, так и иные способы регулирования контента:

• Техническое блокирование. Чаще всего используется блокировка IP, DNS-фальсификация и URL-блокирование использования прокси-сервера. Эти методы применяются для ограничения доступа к определенным страницам, доменам или IP-адресам в тех случаях, когда объект находится вне прямой юрисдикции властей.

• Исключение из поисковых результатов. Компании, предоставляющие услуги интернет-поиска и сотрудничающие с государством, могут исключать из поисковой выдачи результаты, адресующие к запрещенным или нежелательным ресурсам. Последние в таком случае не блокируются, но найти их становится значительно труднее.

• Подавление. Применяется в тех случаях, когда хозяева контента находятся в прямой юрисдикции государства.

• Инициирование самоцензуры. Предполагает комплекс мер по формированию у конечного пользователя представлений о необходимости самостоятельной фильтрации производимого и используемого контента. В самом распространенном случае осознание такой необходимости имеет в своей основе предположение о постоянном мониторинге сетевой активности со стороны государства.

В законодательстве Великобритании описано «неподобающее использование социальных сетей» (в секции 127 Communications Act 2003). Неподобающими видами использования поведения являются:

• Отправление или причастность к отправлению сообщений и других материалов грубого, оскорбительного или непристойного характера;

• Отправление или причастность к отправлению сообщений, содержащих заведомо ложные сведения.

Ответственность включает в себя штраф либо тюремное заключение сроком до 6 месяцев[20].

Основанием для блокировки интернет-ресурса в Великобритании является нарушение закона: помимо детской порнографии, это может быть пособничество террористической деятельности или нарушение авторского права.

[20] http://www.legislation.gov.uk/ukpga/2003/21

Блокировке подлежит контент, содержащий детскую порнографию. Его поиском и ручной блокировкой занимается специальная комиссия из 4 специалистов-аналитиков Internet Watch Foundation[21], частной компании, вносящей адреса подозрительных сайтов в специальный список, доступный операторам контента. Те обязаны самостоятельно уста-

[21] http://www.iwf.org.uk/

навливать системы блокировки подозрительного контента, выявленного IWF.

Одним из самых известных скандалов в деятельности IWF стало их столкновение с Википедией, в ходе которого последней удалось доказать свою правоту (детской порнографией эксперты посчитали обложку альбома музыкальной группы Scorpions), и IWF изменила решение[22].

В целом английский интернет так и остается традиционно либеральным. Однозначной фильтрации подвергается только детская порнография, сама фильтрация осуществляется частной компанией, аккредитованной правительством для ведения мониторинга интернет-контента. Государство не имеет доступа к частной переписке и не может использовать личные данные пользователей Сети во время следствия либо в суде.

В США первые законы об интернете возникли раньше, чем в Европе, – в 1990-х годах – в ответ на обилие в Сети откровенных сексуальных материалов, доступных несовершеннолетним. Попытки создания единой системы контроля над цифровым контентом в США пока не увенчались успехом, поскольку здесь в силу вступает Первая поправка, гарантирующая свободу слова.

Тем не менее на сегодняшний день в США существует 5 федеральных законов, связанных с ограничением распро-

[22] http://www.guardian.co.uk/technology/blog/2008/dec/08/internet

странения информации в интернете[23]:

1. Закон о пристойности коммуникаций (Communications Decency Act (CDA)).

2. Закон о копирайте цифрового миллениума (Digital Millennium Copyright Act (DMCA)).

3. Закон о защите детей (Children's Internet Protection Act (CIPA)).

4. Закон о защите неприкосновенности детской частной жизни (Children's Online Privacy Protection Act (COPPA)).

5. Закон о торговле с врагом (Trading with the Enemy Act).

Были внесены в Конгресс, но не прошли обсуждения следующие законопроекты:

1. Закон против онлайн-пиратства (Stop Online Piracy Act (SOPA)).

2. Закон о защите интеллектуальной собственности (Protect Intellectual Property Act (PIPA)).

3. Закон о защите свободного обмена информацией (Cyber Intelligence Sharing and Protection Act (CISPA)).

4. Закон об удалении онлайн-хищников (Deleting Online Predators Act (DOPA)).

5. Закон о защите ребенка в онлайн-среде (Child Online Protection Act (COPA)).

[23] https://opennet.net/research/regions/namerica

Также в конце марта 2013 был одобрен законопроект, который позволит представителям полиции без специального ордера читать письма электронной почты (пришедшие более 6 месяцев назад либо уже открытые)[24].

Более того, ФБР стремится следить за пользователями интернета в реальном времени.

С появлением социальных сетей и коммуникаций в режиме реального времени в интернете для ФБР возникло «слепое пятно». В отличие от архивов электронной переписки,

---

[24] http://www.guardian.co.uk/law/2013/mar/19/justice-department-police-read-email

которую не так сложно получить от провайдера (на основании Electronic Communication Privacy Act), отслеживание чатов (например, Google-чат) и Skype-переписки представляло для ФБР некоторую трудность.

В течение 2013 года ФБР планировало официально получить возможность следить за онлайн-коммуникациями, включая чаты в онлайн-играх (!), получать доступ к файлам в Dropbox, а также мониторить Gmail и Google Voice[25].

Важной особенностью развития интернета в США является то, что большая часть провайдеров являются частными. Экономически такое решение полностью оправдано: по некоторым оценкам, окончательная приватизация провайдеров позволит Америке сэкономить до $ 12 млрд из федерального бюджета в год[26].

Именно по этой причине деятельность провайдеров оказывается в значительной мере юридически защищенной от санкций в отношении контента Сети.

---

[25] http://www.salon.com/2013/03/27/fbi_pursues_greater_gmail_cloud_spying_powers/http://www.slate.com/blogs/future_tense/2013/03/26/andrew_weissmann_fbi_wants_real_time_gmail_dropbox_spying_power.html

[26] http://opennet.net/research/regions/namerica

В общем виде процесс ограничения контента выглядит следующим образом: если некто усматривает в контенте запрещенное содержание, он обращается к автору публикации либо сразу подает в суд.

Вопрос о содержании контента не формализован, и, в случае если контент напрямую не попадает под определения, описанные выше, а фигуранты не могут прийти к согласию самостоятельно, дело решается в каждом случае индивидуально, в суде. Итогом может стать либо удаление контента, либо прекращение деятельности сайта, либо прекращение

доступа в интернет для признанного виновным[27].

Регулируемые типы контента

Со всей определенностью удалению в абсолютном большинстве стран подлежат следующие типы контента:

1. Содержащий детское порно.

2. Содержащий чужие личные данные, попадающие под понятие «privacy».

3. Содержащий данные, являющие корпоративной собственностью.

4. Попадающий под определение «вредоносного».

[27] http://russeca.kent.edu/USAeconomy/Lecture02.html

5. Являющийся объектом авторского права.

6. Связанный с террористической деятельностью.

7. Не соответствующий правилам сайта, на котором размещен.

Рассмотрим теперь подробнее законодательство стран США и Евросоюза по отношению к каждому из перечисленных типов интернет-контента. Исключение составит рассмотрение корпоративных правил работы с информацией, которые станут предметом обсуждения в главе 4, а также рассмотрение правил, которыми руководствуются при фильтрации контента сами площадки, что тоже станет предметом отдельного обсуждения в главе 3.

Прежде всего, говоря о типах контента, подлежащих ограничению, необходимо уточнить, где заканчивается свобода слова и начинается регулирование. Ведь даже принцип свободы слова как один из базовых конституционных принципов США действует не безгранично. Существует определенная категория высказываний, не подпадающих под его защиту (unprotected speech). Определенные высказывания могут быть в некоторых случаях частично или полностью запрещены законодательно. К таким высказываниям относятся [28]:

- непристойные высказывания,
- намеренное введение в заблуждение,
- провокация насилия,
- пропаганда противоправного поведения,

[28] http://www.wneclaw.com/medialaw/unprotectedcategories.html

• диффамация, угрозы,
• детская порнография.

Основной проблемой юридического использования категории незащищенной речи являются трудности, которые возникают почти в каждом конкретном случае ее идентификации. А по отношению к интернет-высказываниям дополнительно стали возникать вопросы, всякая ли социальная активность может быть названа речью.

С другой стороны, в регуляции интернет-контента возникает термин «overbreadth» (чрезвычайного расширения), использующийся для описания законов, противоречащих друг другу, когда зоны влияния одного начинают расширяться излишне по отношению к другому. Классический пример overbreadth связан с Первой поправкой к Конституции в США и существованием незащищенных высказываний. Здесь гарантии свободы слова сталкиваются с практикой запрета ряда высказываний. Это область постоянного социального напряжения, которое возникает в связи с неоднозначной трактовкой и множеством возможных интерпретаций противоречащих друг другу законов.

Тем не менее абсолютное большинство стран все же считают подлежащими ограничению следующие типы интернет-контента.

Контент, содержащий детское порно

Этот тип интернет-контента запрещают в любой стране. При этом он же является наиболее острым вопросом в дискуссиях об overbreadth. Ведь сентенции на тему защиты детства являются чуть ли не единственным основанием для прямого воздействия на интернет в виде отслеживания, фильтров и цензуры, а не просто однократного удаления материалов. Именно в рамках законов о детском порно впервые было обосновано, что фильтрация трафика допустима. Иначе говоря, было обосновано, что существуют прецеденты, для которых недостаточно просто однократного удаления контента, а нужно системное отслеживание информации на аппаратном и организационном уровне. Как только этот принцип утвердился, его сразу стали пытаться расширить и на другие области, такие как, например, нелегальный файлообмен.

Блюстители интернет-свободы в связи с этим опасаются, что постепенно цензура в интернете будет принята как принцип. И субъекты цензуры смогут принципиально усложнить попытки ее обойти (ведь на сегодняшний момент фильтры и запреты американских и европейских законов легко обходятся большинством пользователей, и на это, по сути, предпочитают закрывать глаза)[29].

Показателен пример 2007 года, когда Йоганн Шлютер,

[29] http://www.bbc.co.uk/news/technology-13116796

представитель датской антипиратской группы, лоббирующей интересы кино и музыкальной индустрии, с трибуны произнес: «Детская порнография – это прекрасно. Это прекрасно, потому что детская порнография понятна для политиков. Разыграв этот козырь, мы можем заставить их действовать и начать блокировать сайты. И как только это произойдет, мы сделаем так, чтобы они начали блокировать и сайты файлообмена… Однажды у нас будет гигантский фильтр, который мы разработаем вместе с IFPI и MPA. Мы постоянно отслеживаем детскую порнографию в Сети, чтобы показать политикам, что фильтр работает. Детская порнография – это проблема, которая им понятна»[30].

Отметим, что данное мнение разделяют большинство интернет-игроков. Крупным медиакомпаниям нужна цензура интернета, и они хотят использовать детскую порнографию как повод. На данный момент общим для США и стран Евросоюза является наличие законов, строго запрещающих постинг материалов, которые могут быть рассмотрены как детское порно.

Еще в марте 2010 года еврокомиссар по внутренней политике Сесилия Мальстрем представила Евросоюзу Директиву, вводящую фильтрацию Сети. Как было сказано в проекте этой Директивы, страны-участники должны были ввести блокирование сайтов, где предположительно содержится детская порнография. Благодаря упорной работе членов

[30] http://habrahabr.ru/post/155295/

Европарламента из нескольких разных политических групп, входящих в Комитет по Фундаментальным Правам (LIBE), попытка комиссии ввести обязательную блокировку была отвергнута. Европарламент изменил Директиву, указав, что участники «могут», а не «должны» вводить блокирование, а если они это делают, они должны убедиться, что процедура соответствует хотя бы минимально юридическим стандартам, и что лицо, чей сайт блокируется, имеет право на апелляцию[31].

Реакция интернет-общественности на данный законопроект была однозначной: блоги запестрили сообщениями о том, что индустрия копирайта будет продолжать использовать козырь детской порнографии везде. К тому же рейды против детского порно в интернете не раз давали сбои.

5 марта 2012 года датские пользователи, попытавшиеся зайти на сайты Google и Facebook, были шокированы тем,

[31] http://www.meldpunt-kinderporno.nl/files/Biblio/Speech-Malmstrom-Combating-sexual-abuse06_05_2010.pdf

что, залогинившись, они увидели сообщение: «Национальный центр High Tech преступности Датской полиции, помогающий в расследовании интернет-преступлений, сообщает, что интернет-страница, с которой вы пытались связаться, может содержать детскую порнографию». Такая же информация появилась еще примерно на 8000 сайтов. Судя по всему, ошибка произошла на уровне «человеческого фактора» датской полиции. По словам главы Института технического образования Джонни Лундберга, такие вещи легко объяснимы. «Видимо, это случилось, когда какой-то сотрудник полиции поместил список вполне законных сайтов не в ту папку… Прежде чем стало известно об ошибке, два провайдера получили список сайтов». Несколько неверных щелчков мыши моментально отправили в черный список более 8000 сайтов.

В феврале 2011 года в США по ошибке закрыли 84 тысячи веб-сайтов по обвинению в публикации детской порнографии. Операция под названием «Защитим наших детей» была проведена в ходе совместной акции департамента Национальной Безопасности США и Министерства юстиции. В ходе операции они получили ордера на арест десяти доменных имен сайтов, предположительно связанных с распространением детского порно. Однако вследствие допущенной ошибки был захвачен большой DNS-сервис, обслуживающий 84 000 сайтов, ни один из которых не был связан с детской порнографией. В ходе захвата департамент на-

циональной безопасности отключил сайты, заменив главные страницы баннером «Реклама, распространение, транспортировка, получение и хранение детской порнографии являются федеральными преступлениями и караются сроком до 30 лет в федеральной тюрьме, 250 000 $ штрафа, конфискацией и реституцией». Восстановление работы сайтов заняло 3 дня, которые, естественно, самым плачевным образом отразились на бизнесе как с точки зрения ущерба от трех дней остановки, так и с точки зрения репутационных издержек [32].

А вот в Исландии попытка правительства ограничить порнографию в интернете (февраль 2013 года) встретила сопротивление со стороны Международного института современных медиа. Многие гражданские активисты утверждали, что это вступает в противоречие с нормами свободы слова и «приближает ситуацию в Исландии к ситуации в Китае и Северной Корее». Противники этой инициативы утверждали, что она несовместима с либеральной политической культурой Исландии.

Никто, однако, не оспаривал необходимость отслеживать и предотвращать сексуальное насилие, в частности защищать детей от демонстрации откровенных и содержащих сцены насилия сексуальных материалов. Основная претензия исландцев в целом сводилась к тому, что невозможно принимать решение об удалении контента в автоматическом режиме: машина не в состоянии в действительности оценить

[32] http://digitaljournal.com/article/320602

контент. В итоге система не была одобрена[33].

В США соответствующий закон Child online protection Act (COPA) был принят еще в 90-х и стал предметом обширной общественной дискуссии.

Вступив в силу, закон практически сразу стал подвергаться критике со стороны судебных инстанций разного уровня, ведомых Союзом по Защите Гражданских прав. Основания для критики были такими:

1) «формулировки закона о «стандартах коммуникации» являются чрезмерно широкими»;

2) «травмирующая информация для детей трех и шестнадцати лет не является одинаковой»;

3) «само определение тех, кто попадает под защиту закона, продиктовано коммерческими целями и не является достаточно узким и точным ни для эффективной защиты этих групп, ни для обоснования жесткого контроля».

Закон подразумевал ограничение доступа детей к порноконтенту в интернете и предусматривал наказание для интернет-провайдеров, которые размещают в Сети порнографические материалы, не заботясь об обеспечении защиты несовершеннолетних от подобного контента. Закон последовательно был назван антиконституционным многими инстанциями. Против него выступил Американский союз гражданских свобод, посчитавший его нарушением Первой поправки к Конституции США. Сразу после принятия закон

[33] http://www.guardian.co.uk/world/2013/feb/28/iceland-porn-ban-free-society

получил отвод в Федеральном суде, поскольку был признан неконституционным. Суд указал на то, что закон способствует размыванию норм защиты свободы слова, а также на то, что для решения поставленных задач есть более эффективные, чем COPA, способы, например программная фильтрация контента (программы родительского контроля). Итогом нескольких лет разбирательств, однако, стало то, что COPA так и не вступил в силу.

Вредоносный контент

Точное определение вредоносного контента зависит от конкретной страны. Например, нацистская пропаганда запрещена во Франции и Германии, но не запрещена в Великобритании. Зато в Великобритании имеется «Кодекс работы ассоциации интернет-провайдеров», где указано, что они должны прилагать разумные усилия для того, чтоб материалы не содержали жестокости, садизма или расовой ненависти[34].

В целом понятие «вредоносный контент» может быть предельно широким. К нему может быть причислен «любой контент, могущий обидеть ценности, предрассудки, религиозные традиции любого из меньшинств» и т. д.[35]

---

[34] http://www.ispa.org.uk/

[35] http://www.publications.parliament.uk/pa/cm200708/cmselect/cmcumeds/353/353.pdf

Проблема заключается в том, что в интернете увидеть «вредоносный» контент могут жители всех стран. В январе 2013 французский суд предписал компании Twitter идентифицировать людей, разместивших антисемитские и нацистские высказывания. По мнению суда, указанные посты нарушили французский закон о расистских высказываниях. Администрация Twitter, в свою очередь, возразила, что, согласно ее правилам, личности пользователей не разглашаются, за исключением предписания суда США, где расположены серверы. Однако Twitter уже удалил спорные твиты, согласно своему правилу об удалении материалов, которые нарушают законы конкретных стран. Остается неясным, станет ли французская прокуратура добиваться своего через Атлантический океан в американском суде в русле договора о взаимной правовой помощи. Это дело затронуло важный вопрос о том, в чьей юрисдикции находится контент в интернете.

Все большее количество информации хранится в «облаках», доступных через интернет в любом месте, в любое время. Европейских законодателей очень занимает вопрос о том, какие данные граждан ЕС могут стать доступны американскому правительству, которое вправе наблюдать за иностранными гражданами согласно законодательству. Американский адвокат Крис Вульф, прибывший в Брюссель для обсуждения законов о защите данных, отметил сложности в интерпретации законов в цифровую эпоху, а также предложил бумажную аналогию для решения подобных конфлик-

тов. Если французским властям понадобится доступ к файлам, хранящимся в парижском офисе американской компании, они вправе прийти и физически получить их для использования в суде[36].

В некотором смысле ситуация с вредоносным контентом все же несколько проще, чем с другими видами онлайн-правонарушений. Чаще всего он представляет собой запрещенные и к устному изъявлению утверждения и находится в этой связи под юрисдикцией обычных законов о клевете, запрете пропаганды расизма и т. д., не требуя новых типов решений.

В США пользователей от вредоносного контента защищает «Закон о пристойности коммуникаций», однако конкретные виды вредоносного контента разнятся также от штата к штату.

В общем виде вредоносными и подлежащими ограничению в большинстве случаев являются следующие виды контента:

- направленные на подстрекательство к преступлениям,
- разжигающие военные действия,
- противоречащие закону страны, к которой принадлежит пользователь,
- высказывания, призывающие к насилию или угрожающие любыми другими противоправными действиями,
- высказывания, приводящие к незаконным сговорам. В

[36] http://www.nytimes.com/2013/01/25/technology/twitter-ordered-to-help-reveal-sources-of-anti-semitic-posts.html?_r=1&

целом к данному пункту относится и террористическая активность, однако в силу ее особенного положения по отношению к национальной безопасности данный вид активности чаще всего упоминается отдельно[37].

Защита приватности

Защита приватности понимается как отражение базовых для европейской культуры ценностей: ценности личности, ее автономии и закрепленных за ней фундаментальных прав. Прежде всего, права на неприкосновенность частной жизни, которое переносится в пространство web 2.0 с помощью ряда последовательно принимавшихся в ЕС с 2002 года «Директив о конфиденциальности и электронных коммуникациях».

Здесь возникает известное противоречие. Если неприкосновенность личной жизни – право личности, то свободное движение информации предстает как право и неотъемлемый атрибут самого цифрового пространства коммуникации[38].

«Директивы» обязывают сервисы удалять «не нужные более данные» и сохранять их лишь в целях «оплаты счетов», информировать пользователя обо всех операциях, которые могут быть совершены с внесенными им данными. А

---

[37] http://www.marshallcomputer.com/files/Speech%20&%20the%20Law%2012%2012.pdf

[38] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0058:EN: NOT

также утверждают право пользователя отказаться от получения нежелательной информации (как, например, сообщения по электронной почте, которые могут быть получены только с предварительного согласия пользователя).

Отдельно обсуждается сохранение «cookies», которое также ограничивается Директивами. «Cookies» рассматриваются как «важные и полезные для функционирования современного интернета» и одновременно «представляющие опасность с точки зрения приватности».

Cookie – это небольшая порция текстовой информации, которую сервер передает браузеру. Браузер хранит эту информацию и передает ее серверу с каждым запросом как часть HTTP-заголовка. Одни значения cookie могут храниться только в течение одной сессии, они удаляются после закрытия браузера. Другие, установленные на некоторый период времени, записываются в файл. Обычно этот файл называется 'cookies.txt' и лежит в рабочей директории установленного на компьютер браузера[39].

С 2009 года в ЕС согласие на сохранение cookies не требуется лишь там, где они считаются «строго необходимыми для доставки услуг, запрашиваемых пользователем». Пример «строго необходимых» cookies: когда вы нажимаете «добавить в корзину» или «продолжить заказ», делая покупки онлайн. Важно, что браузер запоминает информацию из предыдущей веб-страницы, чтобы завершить сделку. При

[39] http://citforum.ru/internet/html/cookie.shtml

этом в формулировке Директив не называются никакие конкретные технические средства, которые могут быть использованы для хранения данных, Директива относится и обращается к самой информации, которая хранится в браузере пользователя. Это на уровне идеологии отражает «стремление ЕС оставить режимы Директивы открытыми для будущих технологических разработок».

Законодательство Великобритании подразумевает наличие возможности дать свое согласие на принятие cookies единожды для указанного списка сайтов. Однако показательно, что, несмотря на такую публичную позицию, выставление опции «не принимать cookies» по умолчанию в новой версии браузера Mozilla привело к внушительному недовольству со стороны субъектов цензуры, ведь более 80 % пользователей никогда не изменяют опции, установленные по умолчанию[40].

В отличие от Соединенных Штатов и Канады законодательство ЕС оставляет за своими гражданами право на доступ ко всей полноте информации, которая есть у компаний и сайтов о них. Например, европейский пользователь Facebook может потребовать предоставить все данные, которые есть о нем, и Facebook обязан их предоставить[41].

Огласку получил эпизод, случившийся в 2011 году, когда

---

[40] http://www.fastcompany.com/1739058/mozilla-ceo-firefox-faced-advertiser-backlash-over-do-not-track-feature

[41] http://www.europe-v-facebook.org/EN/Get_your_Data_/get_your_data_.html

австрийский студент попросил Facebook предоставить ему все данные о нем. Получив 1222 страницы данных, он все равно обвинил сайт в укрытии части из них и использовании их в рекламных целях[42].

Это послужило причиной провокационной акции пользователей сайта Reddit, направивших тысячи запросов о предоставлении персональных данных в Facebook 4 ноября 2011 года, вызвав у сайта серьезные технологические затруднения[43].

В 2012 году были внесены важные изменения в европейское законодательство относительно приватности в интернете: Евросоюз усилил контроль пользователей над своими данными.

25 января было внесено предложение об изменении правил защиты данных, существовавших с 1995 года, с целью «усилить право на онлайн-приватность и повысить возможности европейской цифровой экономики»[44]. Единый закон должен покончить с текущей фрагментацией ответственности и огромными административными расходами и позволит предприятиям экономить около € 2,3 млрд в год. Также,

---

[42] http://www.telegraph.co.uk/technology/facebook/8917836/Facebook-faces-EU-curbs-on-selling-users-interests-to-advertisers.html

[43] http://www.damnlol.com/watermarked/ea83e08059fd271293365560edd6d795.jpghttp://www.reddit.com/r/funny/comments/ktc16/how_to_annoy_facebook/http://yro.slashdot.org/story/11/09/28/1344218/european-users-overwhelm-facebook-with-data-requests

[44] http://europa.eu/rapid/press-release_IP-12-46_en.htm?locale=en

по мнению создателей, эта инициатива будет способствовать укреплению доверия потребителей к онлайн-сервисам, обеспечивающим столь необходимый импульс для экономического роста, занятости и инноваций в Европе. Изменения вступят в силу до конца 2014 года. Основные изменения в рамках данной реформы:

• Единый набор правил о защите данных, действительный на всей территории ЕС (в числе которых, например, требование о том, что компании и организации должны уведомлять национальный контролирующий орган о нарушениях в данной области настолько быстро, насколько представляется реальным, если это возможно, то в течение 24 часов).

• Организации имеют дело только с одной национальной институцией по защите данных.

• Для пользователей облегчен доступ к собственным данным; также теперь они могут передавать персональные данные от одного поставщика услуг к другому (право на переносимость данных).

• «Право быть забытым» помогает людям лучше управлять рисками и защищать свои данные на сайте: теперь люди могут удалить свои данные, если нет законных оснований для их сохранения.

• Данные правила по отношению к персональным данным распространяются и на компании, действующие за рубежом, но предлагающие свои услуги гражданам ЕС.

• Данные правила распространяются также и на случаи со-

трудничества с полицией или судебное делопроизводство.

• Право на защиту персональных данных прямо признается в статье 8 Устава ЕС об основных правах и в Лиссабонском договоре. Договор создает правовую основу для правил о защите данных для всех видов деятельности в рамках законодательства ЕС в соответствии со статьей 16 Договора о функционировании Европейского Союза.

В феврале 2012 года администрация президента Обамы также вносит изменения в представления об интернет-приватности – 23 февраля появляется «Билль о правах неприкосновенности пользовательской частной жизни». Упор в данном законе делается на соглашение Белого дома, коммерческих организаций и рекламных сетей о принципе «Неот-

слеживания» («Do not track» technology) в большинстве браузеров с целью облегчения для пользователя контроля своего онлайн-треккинга. Большинство компаний, представляющих до 90 % контекстной рекламы в интернете, – в том числе Google, Yahoo! Microsoft, AOL – согласились отдать пользователю право выбирать режимы управления онлайн-слежением[45].

Клевета

Особым видом вторжения в privacy становится клевета как вид высказывания. В США широко применяется гражданско-правовая ответственность за клевету. Уголовно-правовая ответственность де-юре существует в законодательстве некоторых штатов, однако не применяется уже многие годы, поскольку признана неконституционной. Доказательство факта клеветы – задача истца, причем, в зависимости от категории истца и ряда других условий, набор критериев для определения клеветы может сильно разниться. В частности, если истец является публичной фигурой, то он должен в суде доказать факт злого умысла, ставшего причиной клеветы.

Случай с блогером Кристалл Кокс из США продемонстрировал, насколько избирательно может работать система определения клеветы. Блогер был осужден за клевету, по-

[45] http://www. whitehouse.gov/the-press-office/2012/02/23/we-can-t-wait-obama-administration-unveils-blueprint-privacy-bill-rights

скольку его онлайн-активность не была рассмотрена в качестве журналистской деятельности, что, в свою очередь, не позволило ответчику воспользоваться программой защиты журналистов, дающей им возможность ссылаться на анонимные источники при доказательстве правдивости написанного. Помимо всего прочего, принятое судебное решение создало прецедент отрицания блога как элемента средств массовой коммуникации[46]

[46] https://www.eff.org/deeplinks/2011/12/crystal-cox-and-bloggers-as-journalists

Конец ознакомительного фрагмента.