webpublishers•ru

Ирина Левова, Глеб Шуклин, Дмитрий Винник

ПРАВА ИНТЕРНЕТ-ПОЛЬЗОВАТЕЛЕЙ: РОССИЯ И МИР, ТЕОРИЯ И ПРАКТИКА

Аналитический доклад

Ассоциация интернет-издателей
Москва 2013

ББК 67.9
УДК 342.7
Л37

Аналитический доклад подготовлен группой экспертов Ассоциации интернет-издателей при поддержке Фонда поддержки интернет и Координационного центра национального домена сети интернет.

Левова И., Шуклин Г., Винник Д.
Л37 Права интернет-пользователей: Россия и мир, теория и практика / И. Левова, Г. Шуклин, Д. Винник. М.: Ассоциация интернет-издателей; «Кабинетный учёный», 2013. — 144 с.
ISBN 978-5-7525-2831-6

Доклад экспертов посвящен актуальной проблеме регулирования интернета, в частности в отношении прав его пользователей. Авторы доклада проанализировали основные права человека в информационном обществе с точки зрения общепринятых подходов в международном праве и российском законодательстве; исследовали основные подходы к оценке прав пользователей интернета с позиций юрисдикций различных государств; провели анализ феномена «права на доступ в интернет» на основе сравнения позиции различных государств по этому вопросу, а также осветили основные тенденции регулирования правоотношений в информационной среде.

ISBN 978-5-7525-2831-6

Оглавление

Предисловие 4

Введение 5

Глава 1. Основные подходы к правам человека в информационном обществе с точки зрения международного права 29

1.1. Система международного гуманитарного права 29
1.2. Основные документы по правам человека национального и регионального уровней 34

Глава 2. Интерпретация прав человека применительно к информационной сфере и сфере интернета 36

2.1. Доступ к интернету 36
2.2. Недискриминация в обладании интернет-правами 40
2.3. Свобода и безопасность 41
2.4. Право на развитие 42
2.5. Свобода убеждений и выражения 42
2.6. Свобода собраний и объединений 46
2.7. Неприкосновенность частной жизни 47
2.8. Защита данных, в том числе персональных 49
2.9. Право на образование 50
2.10. Доступ к знаниям и культурным ценностям 51
2.11. Использование интернета детьми и защита детей в интернете 53
2.12. Право на труд 54
2.13. Участие в управлении интернетом 55
2.14. Презумпция невиновности и справедливый суд 56
2.15. Сводная таблица прав пользователей 57

Глава 3. Анализ подходов различных государств к регулированию прав пользователей интернета 59

3.1. Подходы различных государств к регулированию правоотношений в интернете 59
3.2. Информационное общество и право на доступ к информации. Нормативно-правовое регулирование в России 104
3.3. Соотношение форм и моделей государственного устройства и основных способов регулирования правоотношений в информационной среде 120

Заключение 134

Библиография 136

ПРЕДИСЛОВИЕ

Предлагаемая на суд читателей монография — плод коллективного труда известных экспертов российской интернет-отрасли, попытка осмыслить сложнейшую проблематику, в основе которой бесконечное разнообразие проявлений феномена поликультурного кода современного интернета. Координационный центр национального домена сети Интернет солидарен с авторами в том, что сегодня интернет стал больше, чем просто новой общественной средой и глобальным медиумом, — от того, по какому руслу пойдет его дальнейшее развитие, во многом зависят и траектория роста нашей страны, и наши с вами, читатель, судьбы.

Заданный авторами дискурс заключается в том, что многослойная и деликатная ткань интернета отторгает по-солдафонски прямолинейные решения и не приемлет популизма, — она нуждается в тончайшей настройке всего инструментария *public policy* для применения лучших ее образцов.

Сделать это без глубокого анализа передовой практики вряд ли возможно, и, хотя эксперты Координационного центра и находят некоторые утверждения авторов небесспорными, отраден сам факт того, что появляется ряд значимых вопросов для дискуссии. Кому-то они могут показаться слишком абстрактными и сложными в осуществлении, но… «Того, кто не задумывается о далеких трудностях, непременно поджидают близкие неприятности», — старик Конфуций, как всегда, прав.

А. В. Колесников,
директор Координационного центра национального домена сети Интернет

ВВЕДЕНИЕ

В последнее время пользователи интернета все чаще выражают недовольство нарушением их прав на доступ к информации в Сети интернет и иных прав, а в некоторых случаях даже обвиняют власти во введении цензуры.

Что имеется в виду под такими правами (содержащимися имплицитно во Всеобщей декларации прав человека, в Конституции Российской Федерации и в других нормативно-правовых актах), каковы пределы их применимости в современных условиях информационного общества — это неочевидно и требует разъяснения и всестороннего анализа, в том числе в контексте различных моделей государственного регулирования.

В настоящем исследовании изучена социальная актуальность проблематики регулирования интернета; проведена интерпретация основных прав человека в информационном обществе с точки зрения общепринятых подходов в международном праве (Всеобщая декларация прав человека ООН, Международный пакт о гражданских и политических правах, Европейская Конвенция о защите прав человека и основных свобод и др.) — и национальном законодательстве (Конституция Российской Федерации); исследованы существующие подходы к оценке прав пользователей интернета с позиций юрисдикций различных государств; проведен анализ феномена «права на доступ в интернет» и сравнены позиции различных государств по этому вопросу; выявлены основные тенденции регулирования правоотношений в информационной среде.

Развитие интернета изменяет сами основы общества, предоставляя возможности для установления равноправного, истинно демократического и процветающего мира, в котором права человека реализуются наиболее полно.

Интернет позволяет достичь недостижимого ранее уровня коммуникации и доступа к информации.

Права человека универсальны, неотчуждаемы, несомненны, неделимы и взаимозависимы. Очевидно, что права человека должны быть распространены на сферу интернета так же, как и на все остальные сферы — во всех контекстах, юрисдикциях и формах.

Интернет стал мощным инструментом для реализации и актуализации прав человека. Достаточно вспомнить «Арабскую весну» и толпы людей на площади Тахрир, организованных при помощи социальных сетей, чтобы понять, насколько глобальным и сильным средством является интернет для демократизации, проявления гражданской воли и социального прогресса.

Тем не менее интернет порождает и новые вызовы в области прав человека. Он может быть использован как для пользы, так и во вред. Не всегда очевидно, каким именно образом права человека приложимы к интернету, и в управлении интернетом права человека редко принимаются во внимание.

Таким образом, крайне важно установить и разъяснить, как права человека распространяются на интернет. Это необходимо и для обеспечения того, чтобы управление интернетом ориентировалось в том числе на ценности и интересы пользователей, на уважение основных ценностей человечества: человеческого достоинства, равенства и недискриминации, солидарности, разнообразия, верховенства закона и социальной справедливости.

Согласно международному праву, государства обязаны защищать, уважать и выполнять права человека граждан. Данное исследование призвано проинтерпретировать универсальные стандарты прав человека в новом контексте — в интернете.

Права и принципы, изложенные в настоящем исследовании, очерчивают круг обязанностей, которые государства имеют по отношению к интернету. При этом необходимо помнить, что интернет по определению трансграничен и

ни одна организация не имеет над ним полный контроль: ни правительства, ни бизнес, ни пользователи — у каждого есть своя роль в развитии интернет-среды, и функции управления должны быть распределены между многими субъектами. Для того чтобы права человека были соблюдены в интернет-среде, все заинтересованные стороны должны осознать смысл таких прав, потребности и возможности их реализации в виртуальной среде и предпринять действия по их обеспечению.

Социальная феноменология и актуальность проблематики регулирования интернета

Интернет в большей части мира уже стал неотъемлемой частью общественной жизни и продолжает захватывать все большие и большие сферы общественной деятельности и определять конкретные формы социальных явлений. Этот процесс вызывает определенные трудности при правоприменении существующих норм права в новых условиях, например как в ряде описываемых ниже ситуаций.

Конфликт юрисдикций

Принципы установления юрисдикции неизбежно создают ситуации, когда пересекаются юрисдикции нескольких государственных судов. Проблемы с определением юрисдикции возникают тогда, когда конфликт имеет экстерриториальную составляющую (например, в нем участвуют граждане разных государств или задействованы международные транзакции). Размещая информацию в интернете, сложно убедиться, что при этом не нарушается законодательство какой-либо страны. К любому материалу, размещенному в интернете, можно получить доступ отовсюду. В этом смысле почти каждый вид деятельности в интернете имеет международную составляющую, что может давать подвод к применению различных юрисдикций и вести к возникновению так называемого «эффекта переливания».

Одним из наиболее наглядных и часто упоминаемых судебных дел, иллюстрирующих проблему юрисдикции, является дело Yahoo!, рассматривавшееся в 2001 г. во Франции. Дело Yahoo! в очередной раз подчеркнуло значимость проблемы множественной юрисдикции. Причиной судебного разбирательства послужило нарушение веб-сайтом Yahoo! французского законодательства о нацистских реликвиях, запрещающего демонстрацию и продажу материалов подобного содержания. Сам веб-сайт был размещен в США, где распространение подобных материалов было и остается законным.

Авторское право и права интеллектуальной собственности

Авторское право защищает только выражение идей в материальной форме, например книги, компакт-диски, компьютерные файлы и т. п. Сама идея авторским правом не защищается. Однако на практике иногда сложно провести различие между идеей и ее выражением. Режим защиты авторских прав шел в ногу с технологическим прогрессом. Каждое новое изобретение: печатный станок, радио, телевидение, видеомагнитофон — влияло как на форму, так и на особенности применения авторского права. Интернет не стал исключением. Развитие интернет-технологий — от возможности «вырезать и вставить» отрывок текста до более сложных действий, таких как практически бесплатное распространение музыкальных и видеофайлов через интернет, — бросило вызов традиционной концепции авторского права. Интернет создает новые возможности и для обладателей авторских прав, обеспечивая более надежные технические средства защиты и мониторинга использования материалов. В самом крайнем случае владельцы авторских прав могут вообще запретить доступ к авторским материалам, что сделает саму концепцию авторского права бессмысленной.

Эти возможности ставят под угрозу хрупкое равновесие между правами авторов и общественными интересами, лежащее в основе концепции авторского права. На сегодняшний день обладатели авторских прав, чьи интересы представляют крупные записывающие и мультимедийные компании, защищают свои права активнее, чем рядовые пользователи. Общественные интересы пока не формулируются достаточно четко и не защищаются в нужной степени.

Показателен пример Франции, где в 2009 г. был принят так называемый закон Хадопи, названный в честь французского агентства HADOPI (Haute Autorité pour la diffusion des œuvres et la protection des droits sur internet)[1], — специального надзорного органа, ответственного за соблюдение авторских прав в интернете. Этот закон позволяет ведомству HADOPI без всякого решения суда отключать от интернета пользователей, которые вторично были пойманы на нелегальной загрузке контента, нарушающей авторские права, или при отказе защитить свои системы снова против подобных нелегальных скачиваний. В августе 2009 г. этот закон был дополнен так называемым законом Хадопи-2. Принятие этих законов вызвало крайне негативную реакцию защитников прав человека как во Франции, так и в Европейском Союзе. Закон рассматривался в парламенте ЕС, который счел, что лишение гражданина доступа в интернет без решения суда является грубым нарушением его прав. Законопроект рассматривался в Конституционном суде Франции, который 10 июня 2009 г. признал основную часть закона противоречащей Конституции Французской Республики, поскольку он нарушает Декларацию прав человека и гражданина 1789 г., а именно презумпцию невиновности, принцип разделения властей и свободу слова. Однако 22 октября 2009 г. исправленная версия закона была принята Конституционным судом. В исправленном законе была прописана судебная юридическая процедура, позволяющая

[1] http://www.hadopi.fr/

лишить гражданина доступа к интернету за нарушение авторских прав. В остальных требованиях закон сохранил свой первоначальный вид[2].

Инициативы защиты авторских прав в интернете со ссылкой на опыт Франции регулярно предпринимаются и в России. Один из последних законопроектов Министерства культуры РФ предполагает аналогичный французскому механизм уведомлений интернет-площадок правообладателями, а при отсутствии реакции со стороны информационного посредника — последующую блокировку контента операторами связи. По замыслу законотворца, пользователь не должен принимать участия в этом процессе и своевременно быть уведомленным о том, что поступила жалоба на его контент как нарушающий авторское право, его просто поставят перед фактом удаления контента. На информационных посредников предполагается возложить обязанность предоставлять персональные данные пользователей и хранить эти данные. Также со ссылкой на французский опыт, являющийся, по мнению правообладателей, позитивным, предлагается отключение от интернета пользователей, разместивших контент, нарушающий авторское право. Однако до настоящего времени руководство страны было нацелено на поиск баланса, в связи с чем в России такого рода инициативы обсуждаются и предпринимаются попытки найти разумный компромисс между обеспечением прав пользователей, правообладателей и информационных посредников.

Подобного рода законодательные инициативы ставят принципиальный вопрос: «Соблюдается ли принцип соразмерности совершенного правонарушения и понесенного наказания в данном случае?» Подключение к интернету в информационном обществе является жизненно важным сервисом, без доступа к которому нормальная социальная жизнь человека становится затруднительной. По степени причиняемых человеку проблем и страданий решение об

[2] Pfanner E. France Approves Wide Crackdown on Net Piracy // New York Times. 2009. 22 October: http://goo.gl/IXkd1.

отключении от интернета сопоставимо с лишением свободы и чаще всего существенно затрудняет профессиональную деятельность.

Изначально целью защиты авторского права было поощрение творчества и изобретений. Именно по этой причине в понятие были включены два элемента: защита прав авторов и защита общественных интересов.

Основная сложность заключалась в том, что нужно было предусмотреть возможность для широкой аудитории обращаться к материалам, защищенным авторским правом, в интересах поощрения творчества, получения знаний и обеспечения всеобщего благосостояния. С точки зрения функционирования этого механизма общественные интересы защищались с помощью концепции «добросовестного использования» защищенных материалов. «Добросовестное использование» обычно понимается как использование для исследований и других некоммерческих целей. Интернет предоставляет исследователям, студентам и другим пользователям, особенно из развивающихся стран, мощный инструмент для участия в глобальном научном обмене, тем самым обеспечивая рост знаний. Ограничительный режим защиты авторских прав может вызвать негативные последствия для потенциала развивающихся стран, и чаще всего жесткие режимы охраны авторских прав в развивающихся странах являются наиболее выгодными странам развитым.

Другой аспект — рост масштабов оцифровывания предметов культуры и искусства развивающихся стран. Как ни парадоксально, развивающимся странам часто приходится платить за свое культурное и художественное наследие, когда оно уже оцифровано, помещено в новую «упаковку» и стало собственностью иностранных развлекательных компаний и медиа.

Веб 2.0: пользователи как авторы

С развитием платформ Веб 2.0: блогов, форумов, сервисов обмена документами и виртуальных миров — различия между пользователем и создателем контента стираются.

Пользователи интернета могут сами создавать значительную часть материалов: сообщения блогов, видео на YouTube, фотогалереи. Выявление, фильтрация и маркировка «неподходящих» сайтов становятся все сложнее. Несмотря на существование технологий автоматической фильтрации, автоматическое распознавание, фильтрация и категоризация изображений и видео пока недоступны.

Киберпреступность и спам

Определенное противостояние между «реальным» и «виртуальным» правом существует и в этой плоскости. Сторонники «реального» права подчеркивают, что киберпреступность аналогична преступлениям в «оффлайновом» мире, только совершается, как правило, с помощью компьютера, обычно подключенного к интернету. Преступления остаются теми же, различны только средства их совершения. В соответствии с «киберподходом» уникальные элементы киберпреступности требуют особого обращения, особенно когда речь идет о применении законов и профилактике преступности.

Составители Конвенции Совета Европы по киберпреступности[3] склонялись к «реальному» праву, подчеркивая, что единственным специфическим аспектом киберпреступности является использование коммуникационных технологий как средства совершения преступления. Конвенция вступила в силу 1 июля 2004 г. и является основным инструментом в данной области.

Конвенция о киберпреступности обострила дискуссию о равновесии между безопасностью и правами человека. Существуют опасения главным образом со стороны представителей гражданского общества, что конвенция предоставляет властям слишком много полномочий, включая право проверять компьютеры хакеров, следить за обменом информацией и т. д. Широкие полномочия могут поставить под угрозу некоторые права человека, в частности право на

[3] Европейская Конвенция по киберпреступлениям от 23 ноября 2001 г.

частную жизнь и свободу выражения убеждений. Конвенция о киберпреступности была принята Советом Европы, одной из наиболее активных международных организаций, выступающих в защиту прав человека. Это обстоятельство может способствовать нахождению необходимого равновесия между борьбой с киберпреступностью и защитой прав человека.

Одной из основных сложностей в борьбе с киберпреступностью является сбор данных для ведения судебных дел. Скорость современных коммуникаций требует быстрой реакции со стороны правоохранительных органов. Одним из возможных способов хранения улик является ведение провайдерами электронных протоколов («логов»), в которые заносится информация о том, кто и когда получал доступ к тем или иным ресурсам. Некоторые положения Конвенции о киберпреступности устанавливают обязательство хранить данные об интернет-трафике. Эта правовая норма может оказать влияние на роль интернет-провайдеров в обеспечении правопорядка в интернете.

Важно отметить, что Россия не присоединилась к указанной Конвенции, аргументируя это возможными рисками для национальной безопасности, заложенными в статье 32б, согласно которой допускается санкционированный доступ к компьютерным данным на территории другой страны для проведения следственных действий.

По мнению экспертов, это существенно препятствует расследованию трансграничных киберпреступлений.

Труд

В области трудового законодательства важным аспектом является вопрос о тайне частной жизни на рабочем месте. Имеет ли работодатель право следить за тем, как его сотрудники пользуются интернетом (проверять содержание электронных сообщений или контролировать доступ к сайтам)? Законодательство развивается и в этой области, появляется множество разнообразных новых решений. Во Франции, в Португалии и Великобритании правовые нормы

и некоторое количество судебных прецедентов защищают работника, ограничивая право работодателя следить за электронной перепиской сотрудников. Работодатель обязан предварительно предупреждать своих сотрудников о проведении подобных мероприятий. В Дании суд рассматривал дело, связанное с увольнением работника за пересылку личных электронных писем и участие в чатах сексуальной тематики. Суд постановил, что увольнение было незаконным, поскольку у работодателя не было официальной политики, запрещающей использование интернета на рабочем месте в личных целях. Другим доводом в пользу сотрудника послужил тот факт, что использование им интернета никак не повлияло на качество его работы. Трудовое законодательство традиционно относится к внутригосударственной сфере. Однако глобализация и развитие интернета привели к интернационализации вопросов, связанных с трудовым законодательством. Принимая во внимание рост количества людей, работающих в иностранных организациях и осуществляющих взаимодействие на международном уровне, следует признать, что назрела необходимость создания адекватных международных механизмов регулирования. Этот аспект был признан в Декларации WSIS, которая в § 47 призывает к уважению соответствующих международных норм на рынке труда, связанного с информационно-коммуникационными технологиями.

Защита персональных данных и тайна частной жизни

Криминальный сыск, политический сыск, контрразведывательная деятельность, разведка прошлые времена были специфическим видом деятельности, основанной на работе с доверенными лицами, агентами и прочими личностями, сообщающими разные сведения в личных или публичных беседах. Такая работа всегда занимала очень большое количество времени, сил и средств. В прошлом установление персональных данных, дружеских и товарищеских связей конкретного человека, круга его общения было весьма трудоемкой задачей. Появление социальных сетей стало бес-

ценным подарком не только для служб сыска и надзора, но и для всяческих коммерческих агентств: детективных, подбора персонала, финансово-кредитного анализа и т.п. Если ранее задача выявления друзей конкретного человека была пусть и выполнимой, но в большинстве случаев экономически невыгодной; то с появлением социальных сетей она стала технически элементарной.

В 2006 г. в ЕС была принята Европейская хартия хранения данных[4]. Директива была инкорпорирована в национальное законодательство большинства государств-членов ЕС. Согласно этому документу интернет-провайдеры на местном уровне обязаны сохранять конкретные данные, относящиеся к электронным сообщениям, чтобы помочь в расследовании преступлений, а также в качестве доказательств для возможных судебных разбирательств. Данные должны храниться не менее шести месяцев, но не более двух лет.

Целью архивации данных была объявлена трассировка незаконного контента, выявление источников атак на информационные системы, установление лиц, использующих сети электронных коммуникаций для террористической деятельности и организованной преступности. Директива вызвала острую критику во многих государствах — членах ЕС и была оспорена в немецком Конституционном суде[5].

Тем не менее некоторые страны пошли еще дальше в своих надзорных инициативах и вышли за пределы дозволенного законодательством ЕС.

В марте 2007 г. шведское правительство разрешило Агентству национальной военной разведки (МУСТ) поставить под контроль трансграничные телефонные переговоры

[4] Directive 2006/24/EC of the European Parliament and of the Council of March 15, 2006, on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC.

[5] Heise Online. Data Retention: ISPs Rely on Constitutional Appeals and Exception Rules. 2008. January 10 // http://www.heise.de/english/newsticker/news/101624

и трафик электронной почты без необходимости запрашивать ордер. Кроме того, государственному агентству было предоставлено право разрабатывать план мониторинга ключевых слов в пересылаемых сообщениях, а также мониторинг контента на серверах за пределами страны[6]. НКО предъявили иск к правительству Швеции в ЕСПЧ[7]. Некоторые крупные международные компании в области информационно-коммуникационных технологий (ИКТ) выразили недовольство этими правилами и заявили, что прекратят значительные инвестиции в страну, если спорная норма не будет отменена[8].

В Финляндии — стране, в которой право доступа интернет признано правом человека[9], ассоциация работодателей (включая компанию Nokia) лоббировали закон, позволяющий работодателю отслеживать электронную почту сотрудников с целью предотвращения промышленного шпионажа. Закон не разрешает читать содержание писем, но разрешает отслеживать атрибуты писем: адрес, время отправки, факт прочтения, наличие вложений.

В Германии также активно усиливается государственный онлайн-надзор. Новые поправки в национальное законодательство требует, чтобы провайдеры сохраняли личные данные, такие как сообщения электронной почты и их параметры, IP-адреса каждого абонента интернета, а также уникальный идентификатор каждого клиента, позволяющий отслеживать онлайн-активность.

Еще более сомнительным выглядят так называемые онлайн-рейды, осуществляемые криминальной полицией Германии (Bundeskriminalamt)[10]. Смысл этих рейдов заключается в заражении персонального компьютера троян-

---

[6] European Digital Rights. Cross-Border Wiretapping Proposed by the Swedish Government. 2007. March 14 // http://goo.gl/vOKhq

[7] David Landes. Norwegian Group Joins Case against Sweden's Wiretapping Law. The Local. 2009. February 13 // http://goo.gl/woLGE

[8] Ibid.

[9] http://www.point.ru/news/stories/21007/

[10] Wikipedia, Online-Durchsuchung // http://goo.gl/1jjME

ской программой для полного отслеживания активности пользователя. В марте 2008 г. Федеральный конституционный суд Германии вынес решение, согласно которому онлайн-рейды могут применяться только в исключительных случаях.

Во Франции аналогичная практика стала нормой. В 2011 г. Конституционный совет Франции ратифицировал ст. 4 закона Loppsi-2[11], позволяющей фильтровать интернет без всякого судебного решения. Согласно этому закону, черный список сайтов находится под контролем Министерства внутренних дел. 21 апреля 2011 г. агентство HADOP I сообщило о планах интегрировать скрытое программное обеспечение в модемы и маршрутизаторы французских провайдеров с целью отслеживать весь трафик, включая частную переписку и мгновенные сообщения. Этот софт также содержит утилиту, с помощью которой можно следить за тем, что пользователь набирает на клавиатуре (кейлоггер), а также собирать эти данные в свою базу. Согласно закону, кейлоггеры могут быть инсталлированы на конкретный компьютер до четырех месяцев. Согласно решению суда этот срок может быть продлен еще на четыре месяца. Кроме того, Loppsi-2 предписывает интернет-провайдерам тесное сотрудничество с государственными ведомствами. В случае необходимости провайдеры должны подчиниться требованиям властей и блокировать доступ к конкретным сайтам. Кроме того, в предварительный вариант законопроекта включено положение о создании глобальной базы данных Pericles (по иронии, она названа именем Перикла, знаменитого правителя эпохи расцвета афинской демократии), которые будут содержать супердосье с информацией о французских гражданах. Досье будут включать любые сведения, какие только можно будет собрать в автоматическом режиме — вроде номеров водительских удостоверений и мобильных идентификаторов IMEI.

---

[11] Франция: тоталитарный закон Loopsi 2 // http://goo.gl/RhogW

В 2005 г. итальянское правительство приняло решение усилить надзор за интернетом и телефонными сетями. По постановлению правительства хозяева интернет-кафе обязаны требовать у клиентов паспорт, делать и сохранять его ксерокопию, регулярно предоставлять полиции лог-файлы посещаемых сайтов[12]. Постановление также усложняет процедуру лицензирования интернет-провайдеров, делая существенным условием наличие удовлетворительных систем мониторинга и хранения данных.

Анонимность

Отношение к анонимным сообщениям в различных культурах и эпохах различно. В одних случаях анонимные жалобы рассматриваются государственными и общественными органами, в других случаях на это налагается запрет. Право журналистов и писателей на псевдоним защищено законом в России и многих странах мира, также защищены личные данные штатных и внештатных сотрудников спецслужб, действующих под оперативными псевдонимами. В интернете феномен Анонимуса получил новое звучание. Есть страны, в которых практика запрещения анонимности применяется до сих пор. В 2011 г. правительство Саудовской Аравии ввело новые правила и регулятивные нормы для онлайн-газет и блогеров, требующие специальной лицензии от министерства культуры и информации[13]. Согласно новым правилам, все авторы в Сети, включая авторов на форумах и даже авторов коротких сообщений вроде Твиттера, должны получить эту лицензию, срок действия которой составляет три года.

Правительство объяснило нововведение тем, что должно защитить общество от тлетворных влияний, и отметило, что в любом случае уже давно осуществляет политику цензурирования контента.

---

[12] Sofia Celeste. Want to Check Your e-Mail in Italy? Bring Your Passport. Christian Science Monitor. 2005. October 4 // http://goo.gl/V1w1j

[13] http://goo.gl/fJLn7

Актуальность ограничения права на анонимность демонстрирует судебное дело в Европейском суде по правам человека в связи с возможным нарушением статьи 8 Конвенции о защите прав человека и основных свобод. Это дело известно как «дело К. У. против Финляндии»[14]. Гражданин Финляндии К. У., подлинное имя которого не раскрывается из этических соображений, обнаружил в интернете объявление, написанное от имени его 12-летнего сына анонимным автором. Объявление содержало предложение вступить в интимную связь. Сам мальчик узнал об этом, когда получил отклик на объявление от взрослого мужчины. Отец ребенка подал заявление в полицию с целью установить личность автора объявления, однако интернет-провайдер отказал заявителю, считая себя связанным правилами конфиденциальности пользовательского соглашения. Полиция обратилась в окружной суд с просьбой обязать провайдера раскрыть указанную информацию в соответствии с уголовно-процессуальным правом. Суд не обнаружил в законе прямого указания, позволяющего ему это сделать при совершении преступления, не относящегося к тяжким. После неудачных апелляций в национальных инстанциях отец ребенка обратился с заявлением против Финляндии в Европейский суд по правам человека. ЕСПЧ удовлетворил требования истца и указал в своем вердикте, что свобода выражения мнения и конфиденциальность связи должны соблюдаться, а пользователи телекоммуникаций и интернет-услуг должны иметь гарантии конфиденциальности и тайны личной жизни, такие гарантии не могут быть абсолютными. Европейский суд указал, что эти гарантии при необходимости должны отступать перед иными законодательными императивами, такими как поддержание общественного порядка и предотвращение преступлений, защита прав и свобод других лиц. После этого случая государство-ответчик было вынуждено изменить свое законодательст-

[14] Case Of K.U. v. Finland // http://goo.gl/q9KGO

во, которое обязывало теперь в подобных ситуациях раскрывать имя нарушителя.

Ответственность информационных посредников

Поставщики интернет-услуг (провайдеры) подключают конечных пользователей к интернету. Поэтому с точки зрения многих правительств они являются самым простым и очевидным механизмом обеспечения соблюдения правовых норм в интернете. По мере возрастания коммерческой значимости интернета и актуализации вопросов кибербезопасности многие государства начинают использовать провайдеров как инструмент правоприменения.

Большинство правовых систем признает, что провайдер не может нести ответственности за использование предоставляемых им услуг для размещения нарушающих авторское право материалов, если не знает об этом. Основное отличие заключается в том, какие юридические действия предпринимаются после того, как провайдер проинформирован о нарушении авторских прав, связанном с размещенным на его сервере материалом.

Подход, ограничивающий ответственность провайдеров, в целом поддерживается судебной практикой. Вот некоторые наиболее значимые судебные прецеденты, в которых с провайдеров была снята ответственность за размещение материалов, нарушающих права интеллектуальной собственности: дело сайентологов (Нидерланды), дело «RIAA vs Verizon» (США), «SOCAN vs CAIP» (Канада) и «Sabam vs Tiscali» (Бельгия).

Под давлением общественного мнения интернет-провайдеры постепенно, хоть и неохотно, вовлекаются в регулирование материалов интернета. При этом у них есть два варианта поведения. Первый — обеспечивать следование нормам, выработанным органами власти. Второй, основанный на саморегулировании, — самим определять, какие материалы подходят для размещения. Этот вариант связан с риском «приватизации» политики в отношении содержа-

ния интернет-ресурсов, когда провайдеры будут брать на себя функции правительства.

Защита детей в интернете

Защита детей от информации, могущей нанести им вред, — одна из самых острых и актуальных тем, особенно в приложении к интернету. Наиболее наглядно тема защиты детей может быть проиллюстрирована на примере порнографии. Если до интернет-эпохи порнографические материалы можно было получить только в специальных магазинах, по почте и из рук в руки, то в настоящее время они стали более доступны. Характерно, что качественное увеличение степени доступности изменило характер самой порноиндустрии – она диверсифицировалась, колоссально выросла ее спецификация. Государственный контроль оборота порнографических материалов в новых условиях стал намного более сложной задачей. Однако самым неприятным феноменом стал не рост порноиндустрии как отрасли, а легкость доступности материалов для несовершеннолетних.

Феномен порнографии онлайн является распространенным аргументом сторонников введения способов и процедур ограничения доступа к интернет-контенту и к самому интернету. Эти способы включают: 1) добровольную инсталляцию самими пользователями на собственных машинах программ контент-фильтрации; 2) юридическое принуждение интернет-провайдеров инсталлировать программы или специальное оборудование («железо») для фильтрации на различных узлах обработки данных; 3) классическую меру воздействия — административное и/или уголовное преследование хозяев порнопорталов, открытых в нарушении закона, регулирующего оборот порнографической продукции; 4) юридически закрепленную процедуру верификации возраста пользователя в публичных местах (интернет-кафе и публичных Wi-Fi-зонах) с целью выбора профиля фильтрации; 5) создание и пропаганду общественной системы жалоб на порнографические сайты с целью их добавления в «черные списки»; 6) глубокую фильтрацию

порнографического контента на узлах сопряжения национального интернета и глобальной Сети с целью изоляции национальной Сети от зарубежного антиморального контента на основании нормативно-правовых актов различного уровня.

Использование методов (2) и (6) сопряжено с негативными эффектами, связанными с несовершенством систем фильтрации, вследствие которых неизбежны технические ошибки, из-за которых в «черные списки» попадают сайты, не содержащие порнографии. Вот как охарактеризовал работу таких систем журналу «Компьютерра» Рафал Рогозинский (Rafal Rohozinski), директор группы перспективных исследований сетевой безопасности Кембриджского университета:

> «Практически всегда используются коммерческие системы уровня предприятия. У этих систем, надо сказать, есть серьезные недостатки. Например, их очень трудно точно настроить на тот контент, который вы желаете блокировать. Поэтому иногда блокируется заодно и безобидная информация — Рон Диберт в своем докладе приводил пример, как в одной из стран стал вдруг недоступен веб-сайт американского посольства, так как в слове „usembassy“ система отреагировала на порнографическую, по ее мнению, строку „ass“. С другой стороны, не так трудно обойти блокировку, которую обеспечивают эти системы»[15].

В Саудовской Аравии система действует не на уровне отдельных провайдеров, а через единственное «бутылочное горлышко». Дело в том, что сегмент саудовского интернета сообщается с глобальной Сетью через прокси-ферму, расположенную в Королевском технополисе (KACST)[16]. Еще в 2001 г., согласно статье в «Нью-Йорк Таймс»[17], более семи тысяч сайтов добавлялось в «черный список» ежемесяч-

---

[15] Между киберземлей и кибернебом: цензура в Сети рухнет 1 декабря // http://goo.gl/eQ47r

[16] http://www.kacst.edu.sa/en/Pages/default.aspx

[17] Companies Compete to Provide Saudi Internet Veil // New-York Times. 19.11.2001.

но. Контрольный центр получал каждый месяц более ста запросов с просьбой исключить сайт из «черного списка», включенных в него в большинстве случаев по причине технической ошибки коммерческого программного обеспечения для фильтрации производства американской фирмы Secure Computing. Характерной особенностью данной системы цензуры является то, что она в принципе направлена на сотрудничество с подданными: на сайте подразделения существует специальная форма, с помощью которой можно написать заявление с предложением блокировать тот или иной ресурс. И как сообщается, сотни заявлений приходят каждый день от обеспокоенных моралью подданных королевства. Также можно написать заявление об ошибочном внесении своего сайта в «черный список», рассчитывать на разблокирование и получение весомой компенсации.

Кроме того, сторонники защиты свободы информации говорят о том, что внедрение обязательных систем фильтрации контента на уровне провайдеров может привести к тому, что программы фильтрации будут использоваться не только надлежащим образом, но будут нацелены и на политическую цензуру.

Известно распространенное мнение, что почти половину интернет-трафика занимает порнография. В действительности это не так. Согласно подсчетам, сделанным в 2011 г., только 4% из сайтов топ-миллиона являются порнографическими и только 13% запросов на поисковых машинах касаются порнографического контента[18]. По мере развития интернета доля порнографического контента падает.

Детская порнография

Детская порнография, несомненно, подпадает под более общее понятие порнографии, однако выделение ее в самостоятельный социальный феномен вполне оправданно. Если отношение к «взрослой» порнографии в разных обществах существенно различается, то на уровне как отдельных стран,

[18] http://goo.gl/QMc4r

так и на международном уровне в этом вопросе существует абсолютный общественный консенсус, доступность и само существование феномена детской порнографии полностью неприемлемы.

Характерно, что американо-канадский исследовательский проект Open Net Initiative (ONI)[19], изучающий режимы цензуры и фильтрации данных в различных странах, воздерживается от оценки, действительно ли существует в конкретной стране режим фильтрации детской порнографии и насколько он эффективен, по причине того, что для такой оценки требуется пересылать и размещать противозаконный контент.

Однако правовые режимы против детской порнографии и мнения о допустимых мерах борьбы с таким контентом расходятся. В некоторых странах, например в США, действует предельно строгий режим: уголовно наказуемо простое владение материалами детской порнографии и преступление, «совершаемое с помощью компьютера», т.е. криминальна осознанная попытка получить к ним доступ (скачать файл)[20]. Это означает, что противозаконно не только распространение контента, но и сама попытка получить доступ к контенту.

В России попытка получить доступ к такому контенту пока не является уголовно наказуемой. В 2012 г. группа депутатов Государственной думы из всех фракций предложила дополнить ст. 242.1 УК РФ (изготовление и оборот материалов или предметов с порнографическим изображением несовершеннолетних) пунктом о приобретении и хранении детского порно и наказывать за него лишением свободы до четырех лет: «…в РФ нет никакой ответственности за детское порно в личных целях, тогда как в 55 странах это считается преступлением»[21], — поясняют депутаты в поясни-

[19] https://opennet.net/about-oni

[20] Десткая порнография: модель законодательства и всемирный обзор. 2010 // http://goo.gl/Q3gGo.

[21] Цит. по: http://goo.gl/vZW5j.

тельной записке. В том же году на заседании Общественной палаты РФ глава Следственного комитета РФ А. Бастрыкин заявил: «Исполнение Факультативного протокола и Конвенции Совета Европы потребует от России введения законодательного определения понятия детской порнографии, установления уголовной ответственности за владение и получение детской порнографии без цели ее распространения»[22]. Более того, А. Бастрыкин утверждал, что в УК РФ должны быть введены санкции за умышленную загрузку или просмотр детской порнографии в интернете и так называемый груминг (grooming — вхождение посредством интернета в доверие к ребенку с целью его сексуальной эксплуатации).

Противники внесения ответственности за хранение материалов и за попытку доступа к материалам аргументируют свою точку зрения тем, что сфабриковать уголовное дело под такую норму не составляет особого труда.

Политика в отношении фильтрации этого типа контента также вызывает нарекания.

Иногда это приводит к острой полемике и судебным разбирательствам. Например, в 2005 г. датская полиция инсталлировала так называемый Фильтр детской порнографии совместно с НКО «Спаси ребенка». Когда «Спаси ребенка» и полиция обнаруживают сайт, содержащий детскую порнографию, полиция информирует провайдера и просит его блокировать доступ к этому сайту без всякого предварительного оповещения хозяев сайта. Эти сайты блокируются фильтром, который держится полицией в секрете. В 2008 г. утечки Викиликс показали, что среди заблокированных сайтов некоторые сайты были неактивны или содержали материалы, которые не имели никакого отношения к детской порнографии[23].

Заместитель министр внутренних дел Германии Бригитта Зиприс, отвечающая за интернет-безопасность в стране, ответила в интервью Рейтер, что «нереалистично

[22] http://goo.gl/mLcp3.

[23] http://goo.gl/8QpO.

пытаться экранировать Германию от иностранных сайтов, даже если полиция имеет своей целью пресечь деятельность доморощенных нацистов. Настолько же нереалистично бороться с другими угрожающими материалами, такими как детская порнография»[24].

Феномен детской порнографии в интернете является мощным аргументом для введения цензурных режимов, криминализации интернет-серфинга (не исключен вероятный заход на запрещенный ресурс и скачивание запрещенного файла), что в конечном счете может привести к ограничению прав человека на получение информации. Следует отметить, что подобные строгие режимы действуют в странах, которые считаются эталонами демократии и свободы слова.

Защита чести и репутации

Проявление радикализма в высказываниях (личных, политических, религиозных, национальных, культурных, эстетических, научных и т. п.), использование оскорблений и выражение своего крайне негативного отношения к личности оппонента с использованием аргументов столь же древнее, как сам человеческий язык. В исторические периоды острых социальных конфликтов такая риторика по тем или иным причинам популярна, вытесняет спокойные и трезвые формы аргументации, порой даже используется службой официальной пропаганды. С появлением интернета такая риторика характерна и для тематических интернет-форумов, в чатов, блогов и групп в социальных сетях.

Общества и политические режимы относятся к «риторике ненависти» по-разному. Одни полагают, что это нормальное, более того, полезное явление, позволяющее людям выместить свою агрессию в интернете, а не в реальной жизни и бороться с ним не стоит. Другие считают, что интернет есть продолжение реальной общественной жизни, поэтому

[24] Source: Adam Tanner, Silicon Valley Germany won't block access to foreign Nazi sites // News, 25 Jul 2000.

обществу и государству следует принимать меры по сохранению правил приличия на дискуссионных площадках в социальных сетях. Например, в Германии риторика ненависти (Volksverhetzung) определяется как «разжигание ненависти в отношении меньшинств при определенных условиях», строго запрещена и уголовно наказуема[25].

Наиболее наглядным, впрочем неудачным, прецедентом борьбы с феноменом риторики ненависти на государственном уровне стал пример Южной Кореи. Согласно статистике, количество издевательств и угроз составляло 13,9% от общего числа сообщений, написанных гражданами Южной Кореи[26]. Корейские власти вполне разумно посчитали, что главной причиной массового распространения риторики ненависти является возможность действовать в интернете анонимно. Поэтому в 2008 г. незадолго до президентских выборов в Южной Корее был введен в действие скандально известный среди интернет-общественности закон «Система действительных имен в интернете»[27] (Internet Real-Name System), который требовал, чтобы все крупные интернет-порталы проверяли личность пользователей. Это относилось ко всем пользователям, которые выкладывали контент в открытом доступе. Например, чтобы добавить комментарий к новостной статье, требовались регистрация и указание идентификационного номера гражданина. Иностранцы, которые не имели такого номера, должны были отправлять по факсу копию паспорта. Хотя общественность изначально протестовала против этого закона, большинство крупных порталов, в том числе Daum, Naver, Nate и Yahoo Korea, такие проверки осуществляли[28]. YouTube отказался подчиниться закону и просто отключил функцию

[25] Strafgesetzbuch [GermanCriminalCode], Section 130, http://goo.gl/EVaFC.

[26] https://opennet.net/research/profiles/south-korea.

[27] http://koreanlii.or.kr/w/index.php/Real_name_system.

[28] Kim Hyung-eun. Do new Internet regulations curb free speech? // Korea JoongAng Daily. 2008. 13 August. http://goo.gl/j4kxw.

комментирования на корейском сайте[29]. Закон был принят в целях борьбы с киберпреступностью и уменьшением количества клеветы и оскорбительных комментариев в южнокорейском интернете. Новый закон предписывал системным администраторам раскрывать данные пользователей, публиковавших комментарии с угрозами или раскрывающие тайну личной жизни других участников дискуссии.

В течение пяти лет южнокорейские пользователи интернета не могли анонимно оставлять комментарии на местных сайтах. Однако сделать интернет-пространство более дружелюбным властям так и не удалось. Южнокорейские интернет-пользователи, чтобы сохранить свою анонимность, просто перешли на зарубежные веб-ресурсы, популярность же отечественных сайтов значительно упала. При этом количество оскорбительных комментариев уменьшилось лишь на 0,9%[30]. Двадцать четвертого августа 2012 г. Конституционный суд Южной Кореи отменил закон о раскрытии данных, по мнению остальных стран, нарушающий свободу слова в стране, гарантированную конституцией. Согласно судебному постановлению, отмененный закон препятствовал формированию плюрализма, который является основой демократии. Интернет-ассоциация Южной Кореи горячо поддержало решение Конституционного суда.

[29] Martyn Williams. Google Disables Uploads, Comments on YouTube Korea // IDG News. 2009. 13 April. http://goo.gl/f7pGt.

[30] https://opennet.net/research/profiles/south-korea

ГЛАВА 1
Основные подходы к правам человека в информационном обществе с точки зрения международного права

1.1. Система международного гуманитарного права

Права человека в теории международного права и его соотношении с внутригосударственным правом имеют следующие уровни регулирования:

— международные стандарты прав человека (закреплены в ключевых международных соглашениях ООН, конвенциях и документах региональных международных организаций Совета Европы, ОБСЕ, учредительных договорах Евросоюза);

— правовые механизмы защиты прав человека на международном уровне (Совет по правам человека ООН, советы и комиссии ООН, практика Европейского суда по правам человека и Суда Европейского Союза);

— конституционное регулирование и закрепление права человека в национальном законодательстве (судебные и административные механизмы защиты прав человека, включая деятельность уполномоченного по правам человека).

Специфика информационного общества и изменение характера правового регулирования реализации прав человека учитываются в концепции трех поколений прав человека: закрепление личных и политических прав в Новое время (XVII–XVIII вв.), социальных и экономических прав в результате деятельности профсоюзных движений (XIX в.), экологических прав, прав национальных групп

и меньшинств, прав человека в информационной сфере включая регулирование интернет-ресурсов (XX–XXI вв.).

Бурное развитие международных стандартов прав человека и их влияние на законодательства стран в послевоенную эпоху привело к тому, что современные конституции и национальное законодательство предусматривают перечни гарантируемых прав человека в связи с ратификацией и необходимостью исполнения международных договоров.

Важнейшие документы в области прав человека:

— Всеобщая декларация прав человека (ООН, 1948), сокращенно ВДПЧ (наряду с Декларацией прав ребенка — ДПР) и Декларация права на развитие (ДПРЗ);

— Конвенция Совета Европы о защите прав человека и основных свобод (Совет Европы, 1950), сокращенно ЕКПЧ;

— Международный пакт о гражданских и политических правах (ООН, 1966), сокращенно МПГПП (наряду с Международным пактом об экономических, социальных и культурных правах);

— Хартия Евросоюза об основных правах (2000), включенная в качестве юридически обязательного документа на основании Лиссабонского договора (2007), сокращенно ХЕСОП;

— Хартия европейской безопасности ОБСЕ (ОБСЕ, 1999), сокращенно ХЕБОБСЕ.

Эти документы на международном уровне гарантируют свободу поиска и передачи информации любым не запрещенным законом способом, включая использование электронных средств связи.

В частности в ст. 19 Международного пакта о гражданских и политических правах предусмотрены следующие положения:

1. Каждый человек имеет право беспрепятственно придерживаться своих мнений.

2. Каждый человек имеет право на свободное выражение своего мнения; это право включает свободу искать, получать и распространять всякого рода информацию и идеи, независимо от государственных границ, устно, письменно

или посредством печати или художественных форм выражения или иными способами по своему выбору.

3. Пользование правами, предусмотренными в п. 2 настоящей статьи, налагает особые обязанности и особую ответственность. Оно может быть сопряжено с некоторыми ограничениями, которые, однако, должны быть установлены законом и являться необходимыми:

а) для уважения прав и репутации других лиц;

б) для охраны государственной безопасности, общественного порядка, здоровья или нравственности населения.

Отсюда следует, что право каждого на свободу выражения мнения включает свободу информации и гарантируется независимо от государственных границ и способа реализации. В современных условиях широкого использования информационных технологий и интернета положения Международного пакта о гражданских и политических правах применяются в полном объеме и не могут служить основанием для чрезмерного ограничения прав человека вне зависимости от установленных законом целей (принцип пропорциональности в международном праве — соразмерность ограничения прав закрепленным законом целям).

В 2012 г. Советом по правам человека при ООН принята специальная резолюция, в которой предусмотрено, что «права, которые человек имеет в оффлайновой среде, должны защищаться и в онлайновой среде, в частности право на свободу выражения мнений, которое, в соответствии со ст. 19 Всеобщей декларации прав человека и Международного пакта о гражданских и политических правах, не зависит от границ и любых выбираемых человеком средств массовой информации»[31]. Тем самым уровень регулирования прав человека не ставится в зависимость от того, в какой среде они реализуются.

Исходя из положений Международного пакта о гражданских и политических правах необходимо отметить,

---

[31] Поощрение, защита и осуществление прав человека в интернете. Резолюция Совета по правам человека № A/HRC/RES/20/8 от 16 июля 2012 г. См.: http://goo.gl/1gygk.

что права человека не могут ограничиваться в силу соображений, не установленных законом.

Конвенция о защите прав человека и основных свобод была открыта для подписания Комитетом министров Совета Европы 4 ноября 1950 г.[32] За время ее существования она пополнилась четырнадцатью протоколами, которые расширили список гарантируемых прав человека и усовершенствовали ее контрольный механизм. Данная конвенция коренным образом изменила представления о допустимых пределах вмешательства во внутренние дела государств и распространила международно-правовое регулирование на некоторые области внутригосударственных отношений, находившиеся прежде под исключительным контролем национальных властей. В частности, она существенно ограничила меру свободы национальных властей в обращении с лицами, находящимися под их юрисдикцией, как с собственными гражданами, так и с иностранцами и лицами без гражданства[33]. Конвенция одна из первых в международном праве признала процессуальную правосубъектность личности (ст. 34). После вступления в силу протокола № 11 Конвенции единственным органом, который осуществляет контроль за выполнением ее положений, является Европейский суд по правам человека. Благодаря решениям Европейского суда, разъясняющим, в чем заключаются права и свободы, признаваемые Конвенцией, ее текст перестал быть самодостаточным и превратился в один из элементов особой системы права, часто называемой «правом Конвенции». Строго говоря, решения Европейского суда обязательны только для государств-ответчиков, которые должны обеспечить их выполнение на национальном уровне. Поскольку Европейский суд рассматривает дела после того, как были

[32] См. подробнее: Ромер Ф.Б., Клебес Х. Право Совета Европы. На пути к общеевропейскому правовому пространству. М., 2007.

[33] Обязательства государств-участников Европейской конвенции о защите прав человека по исполнению постановлений Европейского Суда. Екатеринбург, 2005. (Серия «Международная защита прав человека». Вып. 5).

исчерпаны внутригосударственные средства правовой защиты, на национальном уровне необходимы юридические основания пересмотра судебных решений (в России установлено ГПК РФ, АПК РФ, УПК РФ), чаще путем принятия законодательных актов, но также и посредством толкования действующих правовых норм.

При рассмотрении каждого дела Европейский суд руководствуется правовыми позициями, выраженными в его решениях по аналогичным делам[34]. Поскольку многие вопросы, рассматриваемые Европейским судом, актуальны для большинства европейских государств, правительства учитывают решения Европейского суда в своей законотворческой деятельности и изменяют национальное право в упреждающем порядке, чтобы избежать привлечения к международной судебной ответственности[35].

Конвенция о защите прав человека и основных свобод через прецедентное право Европейского суда оказывает постоянное и эффективное влияние на национальное право. Более того, на сегодняшний день Конвенция зачастую рассматривается как «конституционный инструмент европейского правопорядка», в рамках которого права человека уникальным образом превращаются из категории политической в категорию правовую. Такой феномен пока не имеет аналогов в международном праве. Необходимо упомянуть и воздействие права Конвенции на развитие сотрудничества в рамках других механизмов Совета Европы. Под ее влиянием был принят целый ряд многосторонних соглашений и рекомендаций, призванных способствовать признанию и соблюдению прав человека, которые не были зафиксированы в Конвенции. Успешная деятельность контрольных органов Конвенции способствовала развитию соответствующих механизмов в рамках других многосторонних соглашений Совета Европы.

---

[34] См.: Практическое руководство по критериям приемлемости. Совет Европы, 2011 // www.echr.coe.int.

[35] См.: Европейский Суд по правам человека: правила обращения и судопроизводства: Сборник статей и документов. Екатеринбург, 2001.

В Европейской конвенции основной статьей, регулирующей отношения, связанные с интернет-сферой, является ст. 10 о праве на свободу выражения мнения. Свобода выражения мнения гарантируется в п. 2 ст. 10, который предусматривает, что «осуществление свободы выражения мнения, налагающее обязанности и ответственность, может быть сопряжено с определенными формальностями, условиями, ограничениями или санкциями, которые предусмотрены законом и необходимы в демократическом обществе в интересах национальной безопасности, территориальной целостности или общественного порядка, в целях предотвращения беспорядков и преступлений, для охраны здоровья и нравственности, защиты репутации или прав других лиц, предотвращения разглашения информации, полученной конфиденциально, или обеспечения авторитета и беспристрастности правосудия». В практике толкования Конвенции Европейским судом было отмечено, что легитимными критериями ограничения данного права будут только такие ограничения, которые предусмотрены законом, соразмерны содержанию реализуемого права и «необходимы в демократическом обществе». В России, в частности, свобода выражения мнения в интернете, безусловно, ограничена законодательством о противодействии экстремистской деятельности и законом об охране персональных данных.

1.2. Основные документы по правам человека национального и регионального уровней

Параллельно международным основополагающим документам в сфере прав человека существует ряд соглашений и договоров, расширяющих и уточняющих их применимость к различным национальным и региональным законодательствам. Среди них:

— Американская конвенция прав человека (1978, страны Центральной и Южной Америки);

— Африканская Хартия прав человека и народов (1986, страны Африканского континента);

— национальные конституции.

Большинство указанных международных, региональных и национальных документов не просто запрещают нарушения в отношении прав человека, но эксплицитно накладывают на государства обязательства по продвижению и улучшению защиты и реализации этих прав.

Применимость международных положений и обязательств к национальным законодательным корпусам может разниться. Большинство подходов к такой применимости можно разделить на два вида. Первый подход предлагает монистскую модель, согласно которой международные соглашения есть часть национального законодательства, и является приоритетным по отношению к нему. Второй подход — дуалистский, при котором национальное и международное законодательства являются различными системами и пересекаются только в случаях, когда национальное инкорпорирует международное и последнее, таким образом, имеет статус и распространяется на сферы, закрепленные за соответствующим национальным законом, в который оно инкорпорировано.

Российская Федерация придерживается первого подхода, что закреплено Конституцией РФ (ст. 15, п. 4):

> 4. Общепризнанные принципы и нормы международного права и международные договоры Российской Федерации являются составной частью ее правовой системы. Если международным договором Российской Федерации установлены иные правила, чем предусмотренные законом, то применяются правила международного договора.

Для целей данной работы из региональных документов по правам человека будут рассмотрены лишь европейские соглашения и Конституция Российской Федерации.

ГЛАВА 2
Интерпретация прав человека применительно к информационной сфере и сфере интернета

2.1. Доступ к интернету

Право на доступ к интернету является ключевым правом пользователя. Оно непосредственно следует из права на свободу выражения убеждений, которая включает «свободу искать, получать и распространять информацию и идеи любыми средствами и независимо от государственных границ», как определено в ст. 19 ВДПЧ, ст. 19 МПГПП, ст. 10 ЕКПЧ, ст. 11 ХЕСОП, ст. 26 ХЕБОБСЕ и ст. 29 Конституции РФ («Каждый имеет право свободно искать, получать, передавать, производить и распространять информацию любым законным способом»). Право на доступ к интернету настолько же универсально и фундаментально, как право на средства массовой информации, и даже превосходит его в полноте выражения, предоставляя возможность одновременно не только распространять, но и искать и получать информацию посредством одного и того же инструмента. Отсюда следует, что право на доступ к интернету не зависит от цели его использования: в той же степени, в какой у каждого человека есть право на обучение и выражение политических убеждений с помощью интернета, у него есть право использовать интернет в развлекательных, коммуникационных и других подобных целях.

Право на доступ к интернету также является ключевым для защиты других прав человека, имплицитно содержась в качестве одного из аспектов в каждом из остальных прав.

В частности поскольку интернет является ключевым образовательным инструментом, постольку он защищен универсальным правом на образование. Таким же образом доступ к интернету является неотъемлемой практической частью выборного процесса в некоторых странах (ст. 25 МПГПП и др.). Будучи фундаментальным инструментарием социальной активности, право на доступ к интернету защищено сильнее, чем более общее право на свободу выражения.

Повсеместно возрастает убежденность, что право на доступ к интернету как фундаментальное право человека не только налагает на государства обязательство не запрещать доступ пользователей к интернету, но, более того, обязывает развивать возможности и качество этого доступа.

Совместная Декларация о свободе выражения мнений и интернете, принятая в 2011 г. совместно ООН, ОБСЕ, Организацией американских государств и Африканской комиссией по правам человека и народов (СДСВМИ), эксплицитно обозначает все вышеуказанные права пользователей и обязанности государств в п. 6:

> 6. Доступ к интернету
>
> a. Осуществление права на свободу выражения мнений обязывает государства содействовать обеспечению всеобщего доступа к интернету. Доступ к интернету также необходим в целях обеспечения соблюдения других прав, таких как право на образование, здравоохранение и труд, свободу собрания и ассоциации, а также права на свободное участие в выборах.
>
> b. Ограничение доступа к интернету или какой-либо его части для всего населения или для определенных его сегментов (отключение интернета) не может быть оправдано ни при каких обстоятельствах, даже если это происходит в связи с необходимостью сохранения общественного порядка или в интересах национальной безопасности. То же относится к замедлению операций в интернете в целом или в каких-либо его частях.
>
> c. Отказ физическим лицам в праве на доступ к интернету в качестве наказания представляет собой крайнюю меру, которая может быть оправдана только в случае отсутствия более мягких форм наказания или в случае

принятия судом соответствующего решения, с учетом воздействия этой меры на осуществление прав человека.

d. Другие меры, ограничивающие доступ к интернету, например введение обязательной регистрации или других требований к поставщикам услуг, не являются законными, за исключением тех случаев, когда эти меры соответствуют международному праву в части мер по ограничению свободы выражения мнений.

e. Государства имеют позитивные обязательства содействовать обеспечению всеобщего доступа к интернету. Как минимум они должны:

i. Создать законодательные механизмы, включающие схемы ценообразования, всеобщие требования к техническому обслуживанию и лицензионные соглашения, которые способствовали бы более широкому доступу к интернету, распространяющемуся даже на бедные и отдаленные сельские районы.

ii. Оказывать прямую поддержку в целях содействия доступу к интернету, включая создание центров ИКТ на базе местных сообществ и других пунктов коллективного доступа.

iii. Способствовать повышению осведомленности населения как о пользовании интернетом, так и о выгодах, которые он способен обеспечить, в особенности среди бедных, детей, пожилых, а также населения отдаленных сельских районов.

iv. Принять специальные меры в целях обеспечения равного доступа к интернету инвалидам и лицам, находящимся в неблагоприятных условиях.

f. В целях осуществления вышеуказанных рекомендаций государства должны принять подробные и многолетние планы действий по содействию доступу к интернету, включающие четкие и конкретные цели, а также нормы в отношении прозрачности, отчетности перед общественностью, а также системы мониторинга.

В июне 2011 г. Организация Объединенных Наций признала право на доступ в интернет одним из неотъемлемых прав человека[36].

[36] http://goo.gl/MDjS7 Дата обращения 12.04.2013.

Согласно документу, принятому ООН, распространение информации в Сети должно быть максимально свободным, ограничиваясь лишь теми ситуациями, когда оно может привести к нарушению чьих-нибудь прав.

В настоящее время право на доступ в интернет закреплено законом в Коста-Рике, Эстонии, Финляндии, Франции, Греции и Испании.

Указанное право включает в себя следующие составляющие или следствия:

— качественный сервис и беспрепятственный доступ к технологическим возможностям, предоставляемым интернетом;

— свобода выбора и использования программного обеспечения и технических устройств, с которых осуществляется доступ в интернет;

— требование сетевой нейтральности;

— сторона, ответственная за передачу или маршрутизацию данных, обязана одинаково относится к любому пакету данных вне зависимости от контента, источника или назначения, сервиса, терминала или приложения;

— запрет любой дискриминации трафика или ухудшения качества услуг, который нельзя отнести к необходимым техническим требованиям для адекватного предоставления услуг, препятствование получению или отправке легального контента, приложений и сервисов, а также запрет на подключение определенных устройств к Сети, если они не наносят вред другим пользователям, используются для кражи сервисов или нарушения работы Сети;

— обеспечение максимального охвата доступа в интернет с мобильных устройств и в общественных местах.

Это, в частности, подтверждается п. 5а СДСВМИ:

> При распределении трафика и данных в интернете не должно быть какой-либо дискриминации на основании класса устройства, контента, авторства, происхождения и/или назначения публикаций, услуг или приложений.

Изложенные принципы также являются аргументом для утверждения принципа свободы выбора в использова-

нии платформы и программного обеспечения для доступа к интернету, а также касающихся этого вопроса интероперабельности и открытых стандартов.

Несмотря на отсутствие явным образом выраженного аналогичного права, закрепленного в Конституции Российской Федерации, Россия, являясь членом ООН, также обязана признавать данное право человека, а также все следствия из указанного права.

2.2. Недискриминация в обладании интернет-правами

В ст. 2 ВДПЧ указывается, что каждый человек должен обладать всеми правами и свободами без ограничений или дискриминации «в отношении расы, цвета кожи, пола, языка, религии, политических или иных убеждений, национального или социального происхождения, имущественного, сословного или иного положения». Аналогичные нормы содержат МПГПП, ЕКПЧ и Конституция РФ.

В интернете право не подвергаться дискриминации при осуществлении всех прав включает в себя:

— равенство доступа. Некоторые группы в обществе имеют худший доступ в интернет, чем другие. Фактически это является дискриминацией в отношении их возможности пользоваться правами человека, которые должны обеспечиваться в интернете. В связи с этим необходимо расширять возможности доступа, а также признать такое неравенство и стремиться к его устранению;

— гендерное равенство. Женщины и мужчины имеют равные права на доступ к интернету и его использованию;

— люди с различными потребностями и возможностями. Интерфейсы, контент и приложения должны быть разработаны для обеспечения доступности для людей с ограниченными возможностями и людей с различными возможностями чтения или записи. Разработки и использование технологий должны стремиться к тому, чтобы инва-

лиды в полной мере и на равной основе с другими людьми могли использовать интернет.

Конкретные потребности людей всех возрастов, в том числе молодых и пожилых людей, в использовании интернета должны быть рассмотрены как часть их прав на достоинство, на участие в общественной и культурной жизни, а также реализацию других прав человека.

2.3. Свобода и безопасность

В ст. 3 Всеобщей декларации прав человека говорится: «Каждый человек имеет право на жизнь, на свободу и на личную неприкосновенность».

Аналогичное право закреплено в Конституции РФ в ст. 22 «Каждый имеет право на свободу и личную неприкосновенность».

Все меры безопасности должны соответствовать нормам международного права человека. Меры, принимаемые в целях обеспечения безопасности онлайн, часто непропорционально ограничивают права человека, прежде всего права на частную жизнь.

В интернете право на жизнь, свободу и безопасность включает в себя следующее:

— защиту от преступлений в любых формах. Каждый должен быть защищен от всех форм преступлений, совершенных с помощью интернета, включая преследования и злоупотребления своей цифровой идентификации и неправомерное использование персональных данных;

— безопасность в интернете. Каждый человек имеет право на обеспечение безопасного соединения с интернетом и безопасную деятельность в интернете.

Право на безопасное использование интернета также следует из права на свободу выражения, так как полная актуализация права на выражение невозможна при небезопасном характере соединения; распространение вирусов, кража личных данных и виртуальной идентификации и

другие угрозы, таким образом, должны предотвращаться, в том числе и государственными средствами.

2.4. Право на развитие

«Каждый человек как член общества имеет право на социальное обеспечение и на осуществление необходимых для поддержания его достоинства и для свободного развития прав в экономической, социальной и культурной областях через посредство национальных усилий и международного сотрудничества и в соответствии со структурой и ресурсами каждого государства» (ст. 22 ВДПЧ) — данное право в полной мере раскрывается в отдельной Декларации ООН.

В Конституции России данное право закрепляется в ст. 7: «Российская Федерация — социальное государство, политика которого направлена на создание условий, обеспечивающих достойную жизнь и свободное развитие человека».

Интернет в настоящее время является наиболее мощным инструментом для развития как в экономической, так и в социальной или культурной сфере. Таким образом, право на развитие включает в себя полное осуществление всех возможностей и прав, связанных с интернетом.

Необходимо отметить, что развитие посредством интернета, как и развитие самого интернета, должно в полной мере учитывать нормы международного права в отношении безопасности и сохранения окружающей среды.

2.5. Свобода убеждений и выражения

В ст. 19 Всеобщей декларации прав человека говорится: «Каждый человек имеет право на свободу убеждений и на свободное выражение их; это право включает свободу беспрепятственно придерживаться своих убеждений и свободу искать, получать и распространять информацию и идеи любыми средствами и независимо от государственных границ».

Это право гарантируется также Конституцией России, где в ст. 29 указано:

1. Каждому гарантируется свобода мысли и слова.

2. Не допускаются пропаганда или агитация, возбуждающие социальную, расовую, национальную или религиозную ненависть и вражду. Запрещается пропаганда социального, расового, национального, религиозного или языкового превосходства.

3. Никто не может быть принужден к выражению своих мнений и убеждений или отказу от них.

4. Каждый имеет право свободно искать, получать, передавать, производить и распространять информацию любым законным способом. Перечень сведений, составляющих государственную тайну, определяется федеральным законом.

5. Гарантируется свобода массовой информации. Цензура запрещается.

В интернете право на свободу убеждений и их выражение включает следующее:

— право на информацию. Каждый человек имеет право получать и распространять информацию и идеи через интернет. Каждый также имеет право на доступ к правительственной информации, которая должна быть предоставлена гражданам в своевременной и доступной форме в соответствии с национальным и международным правом;

— свобода интернет-протеста. Каждый человек имеет право на использование интернета для организации и участия в онлайн- и оффлайн-протестах;

— отсутствие цензуры — премодерации контента;

— свобода от незаконного блокирования и фильтрации.

Любое ограничение свободы выражения мнения должны быть тщательно взвешены, ориентированы на законную цель и соразмерны.

В интернете это означает, что фильтрация и блокирование не допускаются, если они являются неточной и случайно приводят к ограничению доступа к законной информации.

В случаях, если блокирование и фильтрация используются для законных ограничений распространения информации, должны соблюдаться следующие принципы:

— каждый человек должен быть проинформирован о критериях, используемых для ограничения доступа к информации;

— законы, предусматривающие ограничение, должны описывать прозрачные механизмы и возможности для общественного контроля, а также ответственность за нарушение принципов соразмерности ограничений доступа к информации;

— каждый должен иметь доступ к четким, эффективным и удобным механизмам апелляции, чтобы каждый может обратиться к поставщику услуг или органам государственной власти, если они считают, что информация незаконно или случайно ограничена.

В ст. 19 п. 3 Международного пакта о гражданских и политических правах (МПГПП) указывается:

> Пользование предусмотренными в п. 2 настоящей статьи правами налагает особые обязанности и особую ответственность. Оно может быть, следовательно, сопряжено с некоторыми ограничениями, которые, однако, должны быть установлены законом и являться необходимыми:
>
> a) для уважения прав и репутации других лиц;
>
> b) для охраны государственной безопасности, общественного порядка, здоровья или нравственности населения.

Таким образом, право на свободу выражения мнения может быть сопряжено с некоторыми ограничениями, однако эти ограничения должны быть предусмотрены законом и являться необходимыми для обеспечения прав и репутации других лиц, для обеспечения национальной безопасности или общественного порядка, здоровья или нравственности населения. Зачатую, именно ссылаясь на эту статью, правительства оправдывают цензуру и иные ограничения.

Важно отметить озабоченность этим вопросом, не так давно возникшую на международном уровне относительно

использования предлога защиты от клеветы и во многом связанную с развитием интернета. Еще в 2010 г. специальный докладчик ООН по вопросу о поощрении и защите права на свободу мнений и их свободное выражение в ежегодном докладе отметил:

> Хотя ст. 19 (3) МПГПП разрешает государствам вводить определенные ограничения на право свободно выражать свое мнение, специальный докладчик озабочен тем, что государства нередко ссылаются на это положение для оправдания необоснованного вмешательства в осуществление журналистами права на свободу выражения своего мнения, с тем чтобы помешать им изобличить коррупцию или серьезные проступки со стороны правительства или влиятельных частных предприятий или не допустить сообщения ими информации о других щекотливых политических проблемах. Хотя такие ограничения могут предусматриваться законом, как того требует ст. 19 (3), во многих случаях положения об этом носят туманный и двусмысленный характер и предусматривают суровые меры наказания, включая заключение в тюрьму и непропорционально большие штрафы. Специальный докладчик хотел бы напомнить государствам, что ограничение права на свободу выражения своего мнения должно быть исключением, а не общим правилом.

В ст. 3 СДСВМИ также явным образом указывается на недопустимость применения фильтрации:

> 3. Фильтрация и блокирование
>
> a. Принудительное блокирование целиком веб-сайтов, IP-адресов, портов, сетевых протоколов или отдельных разновидностей интернет-ресурсов (например, социальных сетей) представляет собой крайнюю меру, аналогичную запрещению газет или вещания, и может быть оправдано лишь при соответствии таких действий международным нормам, например в случаях, когда необходимо защитить детей от сексуального насилия.
>
> b. Вводимые государством или коммерческим поставщиком услуг системы фильтрации интернет-контента, которые не подконтрольны конечным пользователям, являются формой предварительной цензуры и не могут

быть оправданы, будучи ограничением свободы выражения мнений.

В упоминавшейся уже ст. 6b СДСВМИ также говорится о недопустимости прекращения работы и изоляции сегментов интернета друг от друга:

> Ограничение доступа к интернету или какой-либо его части для всего населения или для определенных его сегментов (отключение интернета) не может быть оправдано ни при каких обстоятельствах, даже если это происходит в связи с необходимостью сохранения общественного порядка или в интересах национальной безопасности. То же относится к замедлению операций в интернете в целом или в каких-либо его частях.

Необходимо еще раз подчеркнуть, что право на свободу выражения в применении к интернету означает и свободу поиска и получения информации, что зачастую интерпретируется как право на получение информации о деятельности органов государственной власти.

2.6. Свобода собраний и объединений

В ст. 20 Всеобщей декларации прав человека указано: «Каждый человек имеет право на свободу мирных собраний и ассоциаций. Никто не может быть принуждаем вступать в какую-либо ассоциацию».

В Конституции РФ данное положение детализируется в ст. 31 следующим образом: «Граждане Российской Федерации имеют право собираться мирно без оружия, проводить собрания, митинги и демонстрации, шествия и пикетирование».

Применительно к интернету право на свободу собраний и ассоциаций включает следующее:

— свободное участие в различных группах и объединениях в интернете. Каждый человек имеет право создавать, присоединяться, встречаться или посетите веб-сайт или сетевые собрания, группы или объединения по любой причине, в том числе по политическим и социальным причинам.

Доступ к собраниям и ассоциациям с использованием ИКТ не должны блокироваться или фильтроваться;

— свобода участия в интернет-сообществах и свобода онлайн протеста. Каждый имеет право свободно учреждать интернет-сообщества или вступать в интернет-сообщества.

2.7. Неприкосновенность частной жизни

Ст. 12 ВДЧП гласит: «Никто не может подвергаться произвольному вмешательству в его личную и семейную жизнь, произвольным посягательствам на неприкосновенность его жилища, тайну его корреспонденции или на его честь и репутацию. Каждый человек имеет право на защиту закона от такого вмешательства или таких посягательств».

В Конституции РФ в ст. 23 это право детализируется следующим образом:

> 1. Каждый имеет право на неприкосновенность частной жизни, личную и семейную тайну, защиту своей чести и доброго имени.
>
> 2. Каждый имеет право на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений. Ограничение этого права допускается только на основании судебного решения.

В интернете право на неприкосновенность частной жизни включает следующее:

— национальное законодательство о неприкосновенности частной жизни. Так как интернет является средой трансграничной, национальные законодательства стран о неприкосновенности частной жизни должны в максимальной степени основываться на международных принципах защиты частной жизни;

— политики конфиденциальности в интернете. Политика конфиденциальности и настройки всех услуг должны быть изложены четко и ясно, находиться в легкодоступном месте на ресурсах, а управление настройками конфиденциальности должно быть комплексным и удобным в использовании;

— стандарты конфиденциальности и интегрированность (связанность) IT-систем. Право на частную жизнь должно защищаться по стандартам конфиденциальности IT-системы, обеспечивая защиту всех элементов систем от несанкционированного доступа к IT-системам без согласия;

— право на виртуальную личность. Каждый человек имеет право на виртуальную личность: виртуальная человеческая личность (т. е. идентификация личности в информационных системах) неприкосновенна. Цифровые подписи, имена пользователей, пароли, PIN-коды не должны использоваться или изменяться другими лицам без согласия владельца. Тем не менее право на виртуальную личность не должно быть использовано в ущерб другим;

— право на анонимность и использование шифрования. Каждый человек имеет право общаться анонимно в интернете. Каждый человек имеет право на использование технологии шифрования для обеспечения безопасного, частного и анонимного общения в интернете. Данное право также закреплено Декларацией о свободе интернет-коммуникаций Совета Европы: «Для того чтобы обеспечить защиту от онлайн-слежения и совершенствовать свободу выражения обмена информацией и идеями, государства-члены должны уважать право пользователей интернета не раскрывать свою идентичность»;

— свобода от слежки. Каждый имеет право свободно общаться без произвольного наблюдения или перехвата информации или угрозы наблюдения или перехвата информации. Любое соглашение о доступе к онлайн-услугам, которое включает принятие наблюдения, должно в четкой и доступной форме указать на характер предполагаемого наблюдения за пользователем;

— свобода от клеветы (диффамации). Интерпретируется данное ограничение следующим образом: никто не должен подвергаться незаконным посягательствам на его честь и репутацию в интернете. Каждый человек имеет право на защиту от таких посягательств. Однако защита репутации

не должна использоваться в качестве предлога для ограничений свободы слова.

Право на защиту частной жизни непосредственно связана с правом на защиту репутации, чести и достоинства (см. выше). Как уже указывалось, эти права могут вступать в конфликт между собой; в таких случаях необходимо обеспечение баланса интересов в соответствии с СДСВМИ.

2.8. Защита данных, в том числе персональных

Важный аспект права, закрепленный в той же ст. 12 ВДЧП, касается права на защиту персональных данных каждого человека.

Это право раскрывается в ст. 24 Конституции РФ: «Сбор, хранение, использование и распространение информации о частной жизни лица без его согласия не допускаются. Органы государственной власти и органы местного самоуправления, их должностные лица обязаны обеспечить каждому возможность ознакомления с документами и материалами, непосредственно затрагивающими его права и свободы, если иное не предусмотрено законом».

В интернете право на защиту персональных данных включает:

— защиту персональных данных. При соборе, использовании, обработке и хранении персональных данных необходимо соблюдать международные нормы по защите частной жизни. Так как интернет является трансграничной средой, то международные нормы должны быть имплементированы в национальные законодательства разных стран и соглашения о предоставлении услуг компаний и правительств, которые являются операторами персональных данных;

— обязанности по сбору данных. Сбор, использование, раскрытие и хранение персональных данных должны производиться на основе прозрачных политик конфиденциальности. Тот, кто требует личных данных от лиц, должен

запрашивать также информированное согласие человека и сообщать о содержании, целях, местах хранения, механизмах доступа, поиска и изменения персональных данных. Каждый человек должен иметь возможность осуществлять контроль за порядком использования его персональных данных, в том числе органами государственной власти и при оказании государственных услуг в электронном виде. Каждый человек имеет право на доступ, получение и удаление своих персональных данных, в том числе на отказ использовать государственные электронные услуги;

— мониторинг защиты персональных данных. Мониторинг правильности защиты персональных данных должен осуществляться независимыми контролирующими органами, которые работают прозрачно, без коммерческой выгоды или политического влияния.

Принципы сбалансированной защиты персональных данных закреплены разрабатываемой в ходе европейской реформы новой версией директивы Европейского парламента и Совета Европейского Союза о защите физических лиц при обработке персональных данных и свободном обращении таких данных.

2.9. Право на образование

«Каждый человек имеет право на образование» — гласит 26-я ст. ВДПЧ и п. 1 ст. 46 Конституции РФ.

Кроме этого, в ст. 46 (5) Конституции РФ есть важное дополнение, непосредственно касающееся интернет-права на образование: «Российская Федерация устанавливает федеральные государственные образовательные стандарты, поддерживает различные формы образования и самообразования».

В интернете право на образование включает:

— право на образование через интернет. Виртуальная среда обучения посредством мультимедиа, публикации и распространения книг в интернете открывает широкие возможности для роста знаний. Научные исследования, учеб-

ники, различные виды учебных материалов должны быть опубликованы на открытых образовательных ресурсах с правом свободно использовать, копировать, адаптировать, переводить и распространять их. Следует избегать договорных обязательств, которые препятствуют публикации научных и других работ в интернете. Бесплатное или недорогое обучение, методики и материалы, связанные с использованием интернета, должны всесторонне поощряться;

— медиаграмотность. Учитывая широкие возможности, посредством которых может быть реализовано право на образование в интернете, необходимо стремиться к повышению образованности людей о самом интернете, а цифровая грамотность должна стать ключевым компонентом образования;

— поддержку самообразования. Российская Федерация, поддерживая самообразование, придает особое значение свободному распространению знаний и информации через интернет как среды, обеспечивающей широкие возможности для самостоятельного обучения граждан. Кроме того, для реализации данного права необходимо содействовать созданию и свободному распространению образовательного контента в интернете.

2.10. Доступ к знаниям и культурным ценностям

В ст. 27 Всеобщей декларации прав человека указывается: «Каждый человек имеет право свободно участвовать в культурной жизни общества, наслаждаться искусством, участвовать в научном прогрессе и пользоваться его благами».

Кроме того, закрепленным в ст. 27 Всеобщей декларации прав человека является право, согласно которому «каждый человек имеет право на защиту его моральных и материальных интересов, являющихся результатом научных, литературных или художественных трудов». Это право гарантируется также в Конституции Российской Федерации (ст. 44): «Каждому гарантируется свобода литературного,

художественного, научного, технического и других видов творчества, преподавания. Интеллектуальная собственность охраняется законом. Каждый имеет право на участие в культурной жизни и пользование учреждениями культуры, на доступ к культурным ценностям».

Эти потенциально конфликтующие права должны быть сбалансированы в интернет-среде. Режим охраны авторских прав не должен несоразмерно ограничивать возможности интернета для поддержки доступа общества к знаниям и культуре.

В интернете право на свободное участие в культурной жизни включает следующее:

— право на участие в культурной жизни общества. Каждый человек имеет право использовать интернет для доступа к знаниям, информации и научным исследованиям. Каждый имеет право свободно получать доступ и обмениваться информацией общественно-политической и социальной ценности, не подвергаясь преследованиям или ограничениям. Каждый человек имеет право на использование знаний и инструментов из прошлого для повышения личного и коллективного знания о будущем. Каждый человек имеет право привносить новое в содержание, приложения и услуги без необходимости проходить централизованное разрешительные процедуры и проверки. Это также означает, что результаты интеллектуальной деятельности не должны быть ограничены техническими средствами защиты авторских прав;

— разнообразие языков и культур. В интернете должен быть обеспечен доступ к качественной и разнообразной информации с различным культурным содержанием. Культурное и языковое разнообразие в интернете должно поощряться;

— право на использование родного языка. Все люди и социальные группы имеют право пользоваться родным языком, создавать, распространять и обмениваться информацией и знаниями через интернет;

— свободу от ограничений на доступ к знаниям путем лицензирования и авторского права. Авторы должны получать вознаграждение и признание за свою работу таким образом, чтобы не ограничивать инновации или доступ к государственным, образовательным учреждениям, к знаниям и ресурсам. Защита авторских прав не должна препятствовать росту знаний. Наиболее перспективными и отвечающими балансу прав пользователей и авторов являются механизмы защиты авторских прав, не препятствующие свободному распространению знаний и росту знаний, например Creative Commons;

— общественное достояние. Финансируемые государством научные исследования и произведения искусства должны быть доступны свободно для широкой публики в интернете.

2.11. Использование интернета детьми и защита детей в интернете

Дети имеют закрепленное в ст. 25 Всеобщей декларации прав человека «право на особое попечение и помощь».

В ст. 38 Конституции Российской Федерации также гарантируется право и одновременно обязанность родителей заботиться о ребенке: «Забота о детях, их воспитание — равное право и обязанность родителей».

Кроме того, в Декларации прав ребенка в принципе 7 ясно обозначено, что ответственность за наилучшее обеспечение интересов ребенка лежит прежде всего на его родителях.

С точки зрения интернета это означает, что детям должна быть предоставлена свобода пользоваться интернетом, а родителям — средства защиты своих детей от опасностей, связанных с интернетом. При этом, согласно тексту российской Конституции и Декларации прав ребенка, обязанность заботиться о ребенке возлагается на родителей, что, в свою очередь, означает, что родителям должна быть предоставлена возможность заботиться о своем ребенке и

самостоятельно определять, какая информация в интернете является неприемлемой для детей.

В этом контексте правильным представляется подход, когда вмешательство государства состоит в контроле за наличием на ресурсах в интернете механизмов ограничения доступа к опасной для детей информации, с тем чтобы родители могли самостоятельно воспользоваться такими фильтрами и защитить своего ребенка.

Право на особую заботу и помощь детям в интернете включает:

— право на доступ в интернет на пользование интернетом. Дети должны иметь возможность использовать интернет, чтобы осуществлять свои гражданские, политические, экономические, культурные и социальные права. К ним относятся право на охрану здоровья, образование, неприкосновенность частной жизни, доступ к информации, свобода выражения мнений и свободу объединений;

— свободу от эксплуатации и жестокого обращения с детьми. Дети имеют право расти и развиваться в безопасной среде, свободной от сексуальных и других видов эксплуатации. В связи с этим также должны быть приняты меры для предотвращения использования интернета для нарушения прав детей, однако такие меры должны быть строго направленными и соразмерными — нужно избегать мер, которые могут препятствовать свободному распространению информации в интернете.

2.12. Право на труд

В ст. 23 Всеобщей декларации прав человека говорится: «Каждый человек имеет право на труд».

В Конституции Российской Федерации данное право гарантируется в ст. 37: «Труд свободен. Каждый имеет право свободно распоряжаться своими способностями к труду, выбирать род деятельности и профессию».

В интернете, право на труд включает в себя:

— соблюдение прав трудящихся. Каждый человек имеет право на использование интернета для организации профессиональных союзов, в том числе для защиты своих прав на труд и свободную реализацию своих способностей к труду;

— интернет на рабочем месте. Рабочие и служащие имеют доступ к интернету на своем рабочем месте, где это возможно. Это требование следует как из права на труд, так и из права на доступ в интернет. Соответственно любые ограничения на использование интернета на рабочем месте должны быть четко сформулированы в политике компании и доведены до сведения трудящегося. Условия и имеющиеся возможности наблюдения за использованием интернета сотрудниками компаний должны быть четко разъяснены трудящемуся, а на рабочем месте должно быть обеспечено право на защиту данных и ясны все условия и причины ограничения этого права.

2.13. Участие в управлении интернетом

Ст. 21 Всеобщей декларации прав человека декларирует: «Каждый человек имеет право принимать участие в управлении своей страной непосредственно или через посредство свободно избранных представителей».

В интернете право принимать участие в управлении страной своему включает право на равный доступ к электронным услугам и необходимость обеспечения права на участие в электронном правительстве. В ст. 21 Всеобщей декларации прав человека также говорится, что «каждый человек имеет право равного доступа к государственной службе в стране». Применительно к интернету это означает, что каждый человек имеет право равного доступа к электронным услугам в своей стране. Для России это означает как минимум обеспечение доступа к интернету.

2.14. Презумпция невиновности и справедливый суд

Ст. 8 Всеобщей декларации прав человека закреплено право, каждого человека «на эффективное восстановление в правах компетентными национальными судами в случаях нарушения его основных прав, предоставленных ему конституцией или законом».

В соответствии со ст. 10 ВДПЧ «каждый человек имеет право на основе полного равенства на справедливое и публичное разбирательство дела независимым и беспристрастным судом в случае спора о его правах и обязанностях и при рассмотрении любого уголовного обвинения, предъявляемого ему».

В Конституции РФ данное право также гарантируется ст. 46: «Каждому гарантируется судебная защита его прав и свобод», а в ст. 49 закрепляется презумпция невиновности: «…пока его виновность не будет доказана в предусмотренном федеральным законом порядке и установлена вступившим в законную силу приговором суда. Обвиняемый не обязан доказывать свою невиновность. Неустранимые сомнения в виновности лица толкуются в пользу обвиняемого».

Уголовные процессы должны следовать стандартам справедливого судебного разбирательства, как это определено международным правом, включая право считаться невиновным, пока вина не доказана в соответствии с законом — ст. 11 Всеобщей декларации прав человека (1); право не быть осужденным за деяние или бездействие при совершении какого-либо уголовного преступления в интернете вследствие какого-либо действия или упущения, которое не являлось уголовным преступлением в соответствии с национальным или международным правом в то время, когда оно было совершено. Не может также налагаться наказание более тяжкое, нежели то, что могло быть применено в то время, когда преступление было совершено — ст. 11 Всеобщей декларации прав человека (2).

Эти положения имеют значение в контексте правовой неопределенности, которая зачастую возникает при судебных спорах относительно преступлений, совершенных в интернете. Все чаще право на справедливое судебное разбирательство и на эффективные средства правовой защиты в интернет-среде нарушается, например, информационных посредников просят выносить суждения о том, является ли контент незаконным, и призывают удалять контент без постановления суда. Поэтому необходимо вновь подчеркнуть, что процессуальные права должны соблюдаться, защищаться и реализовываться в интернете, как в оффлайне.

2.15. Сводная таблица прав пользователей

Ниже представлена сводная таблица прав человека применительно к информационному обществу и интернету с отсылками на источники международного права, а также статьи Конституции Российской Федерации, в которых соответствующее право закреплено.

Табл. 1. Основные права человека применительно к сфере интернета

Право	**ВДПЧ**	**МПГПП**	**ЕКПЧ**	**ХЕСОП**	**ХЕБОБСЕ**	**Конституция РФ**
Доступ к интернету*	ст.19	ст.19	ст.10	ст.11	ст.26	ст.29
Недискриминация в обладании интернет-правами	ст.7	—	ст.14	—	ст.19	ст.19
Свобода и безопасность	ст.3	ст.9	ст.5	ст.6	ст.51	ст.22
Право на развитие	ст.22, ДПРЗ	—	общие положения	—	—	ст.7

Право	**ВДПЧ**	**МПГПП**	**ЕКПЧ**	**ХЕСОП**	**ХЕБОБСЕ**	**Конституция РФ**
Свобода убеждений и их выражения	ст.19	ст.19	ст.10	ст.11	ст.26	ст.29
Свобода мирных собраний и ассоциаций	ст.20	ст.21	ст.11	ст.12	—	ст.31
Неприкосновенность частной жизни	ст.12	ст.17	ст.8	ст.7	—	ст.23
Защита данных, в том числе персональных	ст.12	ст.17	ст.8	ст.8	—	ст.24
Право на образование	ст.26	—	—	ст.14	—	ст.43
Доступ к знаниям и культурным ценностям	ст.27	—	—	ст.13	—	ст.44
Использование интернета детьми и защита детей в интернете	ДПР	ст.18	—	ст.24	—	ст.38
Право на труд	ст.23		—	ст.15	—	ст.37
Участие в управлении интернетом	ст.21	ст.25	—	—	—	ст.32
Презумпция невиновности и справедливый суд	ст.11	ст.14	ст.6	ст.48	—	ст.49

ГЛАВА 3
Анализ подходов различных государств к регулированию прав пользователей интернета

3.1. Подходы различных государств к регулированию правоотношений в интернете

США

Соединенные Штаты Америки являются родиной интернета и по этой причине борьба между общественными и государственными силами, стремящимися поставить эту технологию под контроль, и теми, кто отстаивает свободу ее использования, началась раньше, чем в других странах.

В 1996 г. Конгрессом США был принят закон о соблюдении моральных норм в системах коммуникации (Communication Decency Act, или CDA). Этот акт был принят как часть Телекоммуникационного акта. Согласно этому акту, уголовному преследованию подвергалось распространение «непристойных» материалов для лиц младше 18 лет, а также материалов «очевидно враждебных» по отношению к меньшинствам[37]. Характерно, что закон преследовал не только авторов «непристойных» материалов, но и провайдеров.

Затем последовала серия законодательных действий по торпедированию этого закона. Однако в феврале 1996 г. Федеральный суд США заблокировал действие этого закона,

[37] U.S.C.A. §§ 223(a), § 223(d). 1997.

в июне 1996 г. признал неконституционным — как противоречащий Первой поправке Конституции США. В июне 1997 г. Верховный суд США отменил CDA.

В октябре 1998 г. Конгресс принял закон о защите личных сведений детей в интернете (COPA). Однако уже в ноябре 1998 г. Верховный суд США ограничил его правоприменение. В 2000 г. Апелляционный суд США оставил в силе ограничение правоприменения COPA.

Закон о защите детей в интернете (CIPA) от 2000 г. вынуждал государственные школы и библиотеки использовать технологии фильтрации в качестве условия получения федерального финансирования в рамках программы E-Rate. Фильтрации должны подвергаться материалы, «вредные для несовершеннолетних», детская порнография и другие непристойные материалы. Верховный суд страны отклонил применимость Первой поправки к CIPA, утверждая, что лица, публично высказывающие свою точку зрения (спикеры), не имеют права доступа к библиотекам[38]. Следует отметить, что некоторые библиотеки и школы отказались от участия в программе, предпочтя сохранить независимость.

После CDA, COPA и CIPA фильтрация интернета в США осуществляется в основном частными производителями. Школы, организации, родители и другие лица, желающие заблокировать доступ к определенному содержанию, имеют возможность выбора среди широкого спектра доступных программных пакетов[39]. Одни программы позволяют доступ только к «белому списку» проверенных сайтов, годных для просмотра детьми, другие — генерируют черные списки сайтов, которые составляются автоматически с помощью скрининга Глобальной сети. Несмотря на то что многие школы и библиотеки обязуются фильтровать контент, фактически это право делегируется разработчикам и настройщикам программ. Критерии «непристойность»,

[38] United States v. American Library Association. 2003. 539 U.S. 194.

[39] Internet Content Filtering and Blocking: Reviews of Internet Filtering Software // http://goo.gl/jYBJ9.

«вредность для меньшинств» определяются CIPA и другими законами, однако конкретное правоприменение, то есть интерпретация этих расплывчатых понятий, отдано на окуп производителей и пользователей частного софта.

Попытки фильтрации интернет-контента в США существуют и на государственном уровне. В 2004 г. Генеральный прокурор штата Пенсильвания законодательным актом уполномочил заставить провайдеров блокировать доступ жителей Пенсильвании к сайтам, содержащим детскую порнографию. Районный суд отменил эту практику как антиконституционную, отметив, что сфера деятельности закона распространяется за пределы штата и существует множество доказательств, что реализация закона привела бы к массовому подавлению свободы слова, защищенной Первой поправкой Конституции США[40].

Для защиты детей от возможного вреда, связанного с пребыванием в социальных сетях, в которых есть вероятность столкнуться с педофилами-соблазнителями, правоохранительные органы оказывают давление с целью убедить частные компании взять на себя добровольные регуляторные обязательства. В прессе часто привлекается внимание к сервисам Facebook и MySpace, относительно которых утверждается, что дети могут не только вступить в контакт с «сексуальными хищниками», но и подвергнуться травле и запугиванию со стороны сверстников, в том числе анонимному. Правоохранительные органы предлагают ввести систему идентификации личности с целью дать возможность полиции эффективно проводить расследования[41]. Для решения этой проблемы был создана Техническая группа по вопросам интернет-безопасности (Internet Safety Technical Task Force), в которую вошли технологические компании, компании, задействованные в интернет-бизнесе, неправительственные

[40] CDT v. Pappert, 337 F. Supp. 2d 606 (E. D. Penn. 2004). For an extensive analysis, see: Jonathan Zittrain. 'Internet Points of Control // Boston College Law Review. 44 (2003). P. 653.

[41] Stone B. Online Age Verification for Children Brings Privacy Worries // New York Times. 2008. November 15 // http://goo.gl/gwRwo

организации и ученые. Группа появилась благодаря специальному соглашению, в котором декларировалась необходимость изучения безопасности в интернете по отношению несовершеннолетних и которое было подписано генеральными прокурорами 49-ти американских штатов. В результате в январе 2009 г. был представлен доклад, в котором рекомендовалось сотрудничество промышленных групп, правоохранительных органов и других акторов, а не только внедрение простых мер обязательного технического контроля для защиты детей в интернете.

Другой попыткой законодательно контролировать общение в интернете является федеральный законопроект, известный как «Акт Меган Майер о предотвращении киберзапугивания» (bullying), предполагающий уголовное преследование за «жесткие, систематические и враждебные» онлайн-разговоры[42]. Акт назван в честь девушки, подвергнувшейся систематическим запугиваниям в социальной сети и покончившей жизнь самоубийством, и, хотя он жестко критиковался, 17 американских штатов приняли свои законы против киберзапугивания[43].

Политика ЕС в сфере регулирования интернета

В Европейском Союзе интернет контролируется в основном правительствами и информационно-коммуникационными компаниями (ИКК). Двадцать семь стран, входящих в ЕС, в той или иной степени регулируют интернет, некоторые из них модерируют контент, связанный с детской порнографией, клеветой или нарушением авторских прав. В отличие от других частей мира, Европа регулирует интернет в значительной степени через скоординированные действия государств, в основном через механизм Европейского Союза.

На уровне ЕС не существует явного требования обязывать другие правительства или ИКК фильтровать или уда-

---

[42] Там же.

[43] First Amendment Center's overview of state cyberbullying laws // http://goo.gl/VGK7L.

лять онлайн-контент, хотя эта позиция может в скором времени измениться. В декабре 2008 г. ЕС одобрил следующую фазу исследований по новым фильтрационным технологиям против нелегального контента. Интернет-программа Сейфер (The Safer Internet Program), принятая Советом министров ЕС, направлена на защиту несовершеннолетних от нелегального и тлетворного контента, в частности «материалов относительно детского сексуального насилия, груминга и кибериздевательств». Эта программа действует с 2009 по 2013 г. и стоит 55 млн евро[44]. Часть программы включает в себя развитие технологий трассировки, которая будет отслеживать детскую порнографию и поможет построить базу данных Европола по нелегальному поведению в интернете. Эта программа последняя из серии инициатив ЕС. Первой попыткой был «План действий по безопасности интернета», который действовал с 1999 по 2003 г. Нелегальный контент различается по странам: пропаганда нацизма, например, нелегальна во Франции и в Германии, но не в Великобритании. Вредный контент определяется более широко и может включать все, что может оскорбить расовые ценности и расовые чувства, религиозные группы и меньшинства. В плане действий подчеркивалась необходимость предпринять шаги в пяти основных областях с целью пресечения незаконного и вредного контента в интернете:

1. Содействие добровольному саморегулированию интернет-отрасли и внедрению схем мониторинг контента, в том числе с использованием горячих линий для общественности, чтобы сообщать о незаконном или вредном содержании.

2. Поощрение провайдеров в обеспечении потребителей инструментами фильтрации и рейтинговыми системами, которые позволяют родителям и учителям регулировать доступ детей в интернет.

[44] Safer Internet Programme 2009–2013 // http://goo.gl/Z5QpM.

3. Повышение осведомленности об услугах, предлагаемых ИКК, позволяющих пользователям управлять доступом к контенту.

4. Изучение правовых последствий поощрения безопасного использования интернета.

5. Поощрение международного сотрудничества в области регулирования.

Две европейские директивы могут стать основой экспансивных шагов законодательства, регулирующего интернет в ближайшие годы. Директива об электронной коммерции[45] ограничивает ответственность интернет-провайдеров за передачу, кэширование и хостинг незаконного контента. Директива аудиовизуальных медиауслуг[46] (AVMSD) тем временем стремится расширить текущее регулирование ЕС для трансляции телевизионного контента в Сети. Правила включают среди прочего право государств-членов судиться с контент-провайдерами, живущими за пределами их юрисдикции и ответственности, чтобы сделать вредоносный контент недоступным для несовершеннолетних. Поскольку AVMSD был принят только в 2008 г., остается неясным, будет ли директива распространяться на все содержание интернет-видео или только на видео, передающееся по TCP/IP по программным запросам.

Большинство существующих правил ЕС в отношении фильтрации пересекается или дополняет актуальную политику отдельных государств в этой сфере. По вопросам детской порнографии, работорговли, террористической пропаганды, мошенничества существует широкий консенсус в отношении отслеживания и блокировки опасного материала. Удивительно, но не существует консенсуса в том, кто должен нести ответственность за такие материалы. Большинство стран согласились считать интернет-провайдеров просто каналами передачи информации. Тем не менее некоторые страны утвердили нормы, согласно которым эти

[45] Directive 2000/31/EC of the European Parliament // http://goo.gl/xs6WF

[46] Audiovisual Media Services Directive (AVMSD) // http://goo.gl/5rjmh

организации являются ответственными за оскорбительный материал.

Европейский Союз поддерживает либеральную политику в отношении региональных интернет-провайдеров, ограничивающую ответственность в соответствии с директивой электронной коммерции. Однако некоторые государства-члены оказались непоследовательными в применении директивы. В июле 2007 г. бельгийский суд потребовал от провайдеров реализации технических мер с целью пресечь нарушения авторского права, совершенные его абонентами через пиринговые сети[47]. В 2008 г. британское правительство предупредило, что отсутствие у провайдеров «добровольного саморегулирования» будет иметь последствием юридическую ответственность за предоставление в свободный доступ незаконных файлов (расшаривание).

Несмотря на недостаток сильного регулирования на уровне ЕС, многие государства-члены взяли на себя фильтрацию нежелательного контента. Такие страны, как Великобритания, Швеция, Финляндия, Дания, Германия и Италия фильтруют детскую порнографию. Некоторые правительства, например в Великобритании и Франции, оказывают давление на провайдеров, побуждая использовать фильтрацию для предотвращения нарушений авторских прав. Любопытен случай блокировки веб-сайтов в Бельгии. В отличие от других стран, веб-сайты были отфильтрованы не потому, что содержали порнографический контент, но для того, чтобы гарантировать конфиденциальность прав подозреваемых или преступников, совершивших преступления на сексуальной почве в отношении детей[48]. Помимо фильтрации по инициативе правительств, контроль и фильтрацию спорного контента и поисковых системы взяли на себя интернет-провайдеры. Основным мотивом этих

[47] SABAM v. s. a. Scarlet (anciennement Tiscali) // http://goo.gl/YbPBQ

[48] Bockstaele B. B. V. Belgian Government Trying to Censor the Internet // Digital Journal.— 2009. // http://goo.gl/YZQkN

компаний было упреждение государственного регулирования.

Кодекс интернет-прав ЕС

Раздел 1. Права и принципы, применимые, когда вы получаете доступ и используете онлайн-сервисы

Часть 1. Доступ к сетям электронных коммуникаций и сервисам

Каждый в ЕС должен иметь возможность доступа к минимальному набору электронных коммуникационных сервисов хорошего качества по приемлемой цене. Это также называется «универсальный сервисный принцип». Согласно праву доступа в интернет, все разумные запросы на подключение к публичным сетям коммуникации в конкретном месте должны иметь дело, по крайней мере, одним оператором. Подобное подключение должно поддерживать голос, факс и пересылку данных со скоростью передачи, позволяющей обслуживать функционально полный доступ в интернет и обеспечивать голосовые телефонные сервисы.

Часть 2. Доступ к сервисам и приложениям по своему выбору

Каждый в ЕС должен обладать доступом и распространять любую информацию и запускать любое приложение или сервис по своему выбору через сети электронных коммуникаций. Фундаментальные права и свободы человека гарантируются Хартией фундаментальных прав ЕС, ЕКПЧ, общие принципы законодательства ЕС должны уважаться в этом контексте. По этой причине любые меры, имеющие отношение к доступу потребителя или к использованию сервисов и приложений, ответственные за ограничение этих фундаментальных прав или свобод, могут быть наложены только государством-членом, если эти меры будут адекватны, пропорциональны и необходимы с точки зрения демократического общества.

Исполнительные органы власти, регулирующие электронные коммуникации, должны обеспечивать способность каждого в ЕС иметь доступ к любой информации и распространять ее, запускать любое приложение или сервис по своему выбору через сети электронных коммуникаций. Это называется принципом «открытого и нейтрального характера интернета». Эти регулирующие

органы власти имеют власть устанавливать минимальный набор сервисных требований в случае проблем с безопасностью открытости интернета. С целью предотвратить деградацию сервисов и снижения скорости трафика государства-члены должны быть убеждены, что национальные регулирующие органы способны установить минимальный набор сервисных требований в обеспечении публичных сетей.

Каждый потребитель-инвалид должен иметь возможность выбрать лучшего провайдера из доступных для большинства потребителей.

Несовершеннолетние защищены от аудиовизуальных медиапрограмм и коммерческих коммуникаций, которые могут серьезно повредить их физическому, психическому и моральному развитию. В ЕС подобное содержание может быть сделано доступным онлайн только по явному запросу, но только таким образом, который дает уверенность, что несовершеннолетние при обычных условиях не услышат и не увидят таких сервисов.

Подстрекательство к ненависти на расовой, сексуальной, религиозной или национальной почве в аудиовизуальных медиасервисах запрещено. Правительства должны быть уверены что ни аудиовизуальные медиопрограммы, ни аудиовизуальные коммерческие коммуникации, которые есть в интернете, не сдержат подобного подстрекательства.

Раздел 3. Отсутствие дискриминации при доступе к онлайн-сервисам

Потребителям, которые хотят получить доступ к онлайн-сервисам в другом государстве-члене ЕС, продавцы должны быть гарантировать доступ к публичной информации, согласно общим условиям доступа.

Потребителям не должно быть отказано в доступе к онлайн-сервисам на землях их государства проживания, кроме отказа, обусловленного объективными критериями, оговоренными в ст. 20 Директивы 2006/123 ЕС о сервисах на внутреннем рынке. Продавцы должны информировать потребителей о невозможности предоставления сервиса на конкретной территории. Когда невозможно широко информировать публику, они должны предоставить такую информацию по запросу пользователя.

Когда потребитель пытается получить доступ к сервису онлайн, сервис-провайдеры не должны предоставлять менее выгодные условия доступа к сервису на территории другого государства-члена ЕС, за исключением объективных обстоятельств, изложенных в ст. 20 Директивы 2006/123 ЕС.

Раздел 4. Прайвеси, защита персональных данных и безопасность.

Защита персональных данных является фундаментальным правом, это право также закреплено в Лиссабонском соглашении[49]. Раздел «Фундаментальные права Европейского Союза» гарантирует, что «каждый имеет право на защиту персональных данных. Такие данные могут обрабатываться для конкретных целей на основании согласия человека или на другом законном основании, явным образом оговоренном законом. Каждый имеет право доступа к данным, которые были собраны в его или ее отношении, так же как и право их исправления. Каждое физическое лицо имеет право на адекватную защиту персональных данных. Обработка персональных данных должна быть необходимой, беспристрастной, законной и пропорциональной. Данные, которые индивиды непосредственным образом предоставляют, не должны быть использованы способом, иным от изначальных намерений. Данные не могут быть неразборчиво переданы юридическим лицам, которые человек не выбирал как лица, которые могут быть вовлечены в обработку данных. Эти права применимы ко всем, независимо от национальности или места проживания. Обработка персональных данных, раскрывающая расовое или этническое происхождение, политические мнения, религиозные или философские убеждения, членство в профсоюзах, данные о здоровье и сексуальной жизни, может быть разрешена только на основании явно выраженного согласия индивида, где это разрешено национальным законодательством.

Физическое лицо имеет право получить информацию от людей и компаний, хранящих некоторые из их персональных данных в своих файлах, таких как веб-сайты,

[49] Имеется в виду «Лиссабонский договор о внесении изменений в Договор о Европейском союзе» и договор «Об учреждении Европейского сообщества».

базы данных, сервис-провайдеров и т.п. («дата-контроллеры»), кроме того, он имеет право исправлять или стирать эти данные, если они неполные или неаккуратные:

— дата-контроллеры обязаны информировать потребителей, когда они собирают личные данные о них;

— физические лица имеют право знать имя дата-контроллера, предполагаемую цель обработки данных, кому эти данные могут быть переданы;

— физические лица имеют право запрашивать дата-контроллера, занимается ли он обработкой персональных данных;

— физические лица имеют право на получение копии своих персональных данных в понятной форме;

— физические лица имеют право совершить запрос на удаление, блокировку или стирание данных, если они является неполными, неточными или получены незаконно. Физические лица имеют право возражать против обработки персональных данных.

Физические лица имеют право не быть субъектом, в отношении которого принимается решение, имеющее юридические последствия, значительно влияющие на них и которые основаны исключительно на автоматизированной обработке данных, предназначенных для оценки определенных личностных аспектов, связанных с ними, например производительности на работе, уровня кредитного доверия, надежности, поведения и т. п.

Эти права также применимы в интернете, где люди имеют, кроме того, следующие права:

— быть полностью информированым и давать свое согласие, если сайт хранит и извлекает информацию из своих конечных узлов коммуникационного оборудования или собирается отслеживать их, когда они выходят в интернет;

— право на конфиденциальность своих онлайн-коммуникаций, таких как сообщения электронной почты;

— право получать уведомления в случае, если безопасность их личных данных, хранящихся у провайдера была нарушена, а именно данные были потеряны или украдены, что может иметь негативное воздействие на их частную жизнь;

— право не получать нежелательные коммерческие сообщения, известные как спам, если на это не получено согласие.

Великобритания

Телекоммуникационная отрасль Великобритании регулируется Управлением связи («Офком»). Мандат «Офком» включает в себя, помимо других обязанностей, защиту аудитории от вредоносного материала, несправедливости и нарушений частной жизни[50]. Как государство-член Европейского Союза Великобритания инкорпорировала коммуникационные директивы ЕС в свое национальное право.

В 2000 г. ЕС принял предложение, касающееся, в частности, распространения детской порнографии в интернете[51]. Некоммерческая организация Internet Watch Foundation (IWF), базирующаяся в Великобритании, сотрудничает с правительством и составляет список сайтов, которые она считает незаконными и передает эту информацию провайдерам.

В Великобритании действует один из самых свободных режимов, провайдеры не обязаны фильтровать контент. Однако крупнейший провайдер Великобритании все-таки фильтрует детскую порнографию, но при этом утверждает, что сам не занимается поиском такого контента, а пользуется черными списками, получаемыми от общественности. Действительно, можно сказать, что система фильтрации порнографии основана на деятельности общественности и заявлениях граждан. Такая фильтрационная практика известна под названием «Клинфид» (CleanFeed). В основе «Клинфид» лежит деятельность неправительственной организации IWF (Internet Watch Foundation)[52]. Черный список, составляемый IWF, содержит URL страниц с детской

[50] Statutory Duties and Regulatory Principles // http://goo.gl/iUwaz

[51] Combating Trafficking in Human Beings, the Sexual Exploitation of Children and Child Pornography http://goo.gl/HDluw

[52] Internet Watch Foundation (IWF) // http://www.iwf.org.uk/

порнографией и материалами сексуального насилия над детьми; эта НКО также ищет и старается закрыть сайты, имеющие хостинг под юрисдикцией Великобритании, пропагандирующие расовую нетерпимость, которая запрещена специальным законодательным предписанием (1986)[53].

Технология «Клинфид» подвергается критике за то, что черный список фильтруемых сайтов не публикуется, что может привести к злоупотреблениям. Кроме того, поскольку провайдеры и НКО IWF не являются государственными ведомствами, они, согласно британским законам, не подлежат обязательным юридическим проверкам.

В декабре 2008 г. некоторые британские провайдеры по заявлению IWF заблокировали изображение пластинки «Virginkiller» (1976) группы Scorpions, поскольку на обложке этой пластинки изображена обнаженная девочка.

В 2003 г. после громкого убийства Джейн Лонгхурст выяснилось, что убийца Грэхэм Коутс был одержим интернет-порнографией, правительство объявило планы ликвидации сайтов, изображающих изнасилования, удушение, пытки и некрофилию[54]. В августе 2005 г. правительство Великобритании заявило, что, вместо преследования публикаций таких материалов, оно планирует объявить вне закона частное владение тем, что правительство назвало «экстремальной порнографией». Этим планам суждено было реализоваться в январе 2009 г.[55]

В парламенте Шотландии предпринимаются неоднократные попытки объявить вне закона вообще всю порнографию на основании эмпирических свидетельств криминалистов о связи насилия и увлечения порнографией. Движение «Шотландские женщины против порнографии» предлагает абсурдную инициативу — считать порнографию преступлением на почве ненависти к женщинам. С этим

[53] Public Order Act, chapter 64, section 4, Fear or Provocation of Violence.

[54] The Consumer Experience—Research Report 07 // http://goo.gl/m5MWZ

[55] Ibid.

предложением борется организация «Феминистки против цензуры».

В Великобритании, согласно Террористическому акту (2006) цензуре подвергается информация, восхваляющая терроризм или подстрекающая к нему. Согласно этому акту, провайдер, не блокирующий доступ к такому контенту, может понести ответственность[56].

В 2007 г. среди стран демократического мира Великобритания оценивалась организацией Privacy International как один из худших в мире режимов, вторгающихся в частные права[57]. Великобритания и США являются признанными пионерами внедрения средств электронной разведки в глобальном масштабе, поэтому было бы удивительно, если бы эти средства не использовались в масштабе национальном. Это делается на легальных основаниях и обусловливается необходимостью национальной безопасности, в частности необходимостью противодействия террористической активности.

Франция

Власти Франции декларируют поддержку свободы прессы и интернет-полемики, однако осуществляют фильтрацию детской порнографии и сайтов, продвигающих терроризм и призывы к насилию по расовому и национальному признаку. Помимо политики ограничения контента этого типа, французские власти уделяют особое внимание защите авторских прав в интернете. В этом вопросе они продвинулись настолько далеко, что готовы ограничивать доступ пользователей под своей юрисдикцией за нарушение авторских прав. Правовым основанием для этого послужил так называемый закон Хадопи (2009), названный в честь французского агентства HADOPI, обязанностью которого является мониторинг соблюдения авторских прав в Сети.

---

[56] Terrorism Act, 2006, c. 11 (U.K.).

[57] Privacy International. The 2007 International Privacy Ranking. http://goo.gl/TVoyT

Этот закон позволяет отключать от интернета пользователей, уличенных в нелегальной загрузке контента, нарушающей авторские права, или отказе защитить свои операционные системы (с помощью настроек или специального ПО) против подобных нелегальных скачиваний. В августе 2009 г. этот закон был дополнен так называемым законом Хадопи-2.

Стоит также обратить внимание на билль, более известный как Loppsi-2, который позволяет правоохранительным органам скрытно внедрять на компьютеры подозреваемых программное обеспечение, с помощью которого они могут следить за тем, что пользователь набирает на клавиатуре (кейлоггеры), а также собирать эти данные в базу. Согласно закону, кейлоггеры могут быть инсталлированы на конкретный компьютер до четырех месяцев. По решению суда этот срок может быть продлен еще на четыре месяца. Loppsi-2 предписывает интернет-провайдерам тесно сотрудничать с государственными ведомствами. В случае необходимости провайдеры должны подчиниться требованиям властей и блокировать доступ к конкретным сайтам.

Кроме того, в предварительный вариант законопроекта было включено положение о создании глобальной базы данных Pericles, которые будут содержать супердосье с информацией о французских гражданах — будут любые сведения, какие только можно будет собрать в автоматическом режиме вроде номеров водительских удостоверений и мобильных идентификаторов IMEI.

В 2010 г. парламент Франции выступил против всех перечисленных законов с целью снизить использование систем фильтрации интернет-сайтов. Это событие всколыхнуло дебаты во французском обществе. Противники фильтрации утверждали, что использование этих систем впоследствии может быть расширено и использовано не только против производителей и распространителей детской порнографии. Критики говорили, что фильтрация URL-адресов не имеет эффекта, поскольку распространители детской

порнографии и прочих материалов уже используют шифрование систем p2p для пересылки своей продукции.

В 2011 г. Конституционный совет Франции ратифицировал ст. 4 закона Loppsi-2, позволяющей фильтровать интернет без судебного решения. Согласно закону, черный список сайтов находится под контролем исполнительных властей, в первую очередь министерства внутренних дел без всякого независимого мониторинга. 21 апреля 2011 г. Hadopi проанонсировала свои планы интегрировать скрытое программное обеспечение в модемы и маршрутизаторы французских провайдеров с ясно артикулируемой целью отслеживать все коммуникации, включая частную переписку и мгновенные сообщения. 14 октября 2011 г. французский суд предписал французским провайдерам блокировать сайт Copwatch Nord Paris I-D-F website. Сайт содержал фотографии и видео, на которых видно, как офицеры полиции арестовывают подозреваемых, словесно издеваются над протестующими и будто бы совершают акты насилия против представителей этнических меньшинств. В полиции сказали, что они в некоторой степени обеспокоены содержанием сайта, поскольку на фотовидеоматериалах можно опознать офицеров, даже приводятся их личные данные, что может поставить под угрозу их безопасность.

Сервис Твиттер удалил антисемитские посты по решению суда. В суд обратился Союз еврейских студентов (UEJF) и французская группа адвокатов. 24 января 2013 г. суд предписал Твиттеру раскрыть персональные данные пользователя, который размещал антисемитские посты, которые рассматриваются французскими властями как нарушение французских законов, направленных против речей, разжигающих ненависть. Администрация Твиттера отписалась: она «рассмотрит варианты» относительно французских обвинений. Твиттеру было дано две недели, чтобы выполнить решение суда, иначе будет наложен ежедневный штраф в размере тысячи евро. Вопрос о юрисдикции во исполнение решения оказался существенным, поскольку у Твиттера не оказалось ни офисов, ни сотрудников во Франции, поэтому совершенно непонятно, как будет исполняться решение суда.

С целью предотвращения пропаганды идеологии фашизма в мае 2000 г. французский суд предписал компании Yahoo!Inc. закрыть для французских пользователей доступ к сайтам, продающим на интернет-аукционах реликвии нацистов. Yahoo! ответила, что технически невозможно блокировать пользователей из Франции от контента, имеющего отношение к нацизму, на американских сайтах, и что, вообще говоря, исполнять решения французского суда дело французских сайтов.

В ноябре 2001 г. Окружной суд США постановил, что компания Yahoo! не должна исполнять просьбу французского суда. Суд мотивировал свое решение тем, что Первая поправка Конституции США защищает контент, созданный в США американскими компаниями, от регулирования со стороны властей в странах, в которых действуют более запретительные законы относительно свободы самовыражения. В 2006 г. Апелляционный суд США отменил решение Окружного суда, обосновав это как недостатком подсудности, так и невозможностью реализовать это решение во Франции. Верховный суд США отказал в рассмотрении апелляции.

Германия

В Германии блокировке подвергается некоторая часть интернет-контента и поисковых запросов, как правило, из соображений защиты несовершеннолетних и в рамках политики денацификации. Правовой основой цензуры является в первую очередь Базовый закон (Grundgesetz[58]), аналог конституции, который ограничивает свободу слова только в тех случаях, когда выражается нечто «оскорбительное, несправедливое или неприличное». Германия поддерживает черный список книг, комиксов, журналов, видеокассет и музыки, так называемый индекс. Список, первоначально предназначенный для защиты молодежи от порнографии, был расширен и стал включать антифашистские материалы,

[58] https://www.btg-bestellservice.de/pdf/80201000.pdf.

где идеализируется история Германии, продвигаются идеи неонацизма или отрицается холокост. Риторика ненависти (Volksverhetzung), определенная в Германии как «разжигание ненависти в отношении меньшинств при определенных условиях», также строго запрещена и уголовно наказуема[59]. Закон о теле- и медиакоммуникации (Telemediengesetz[60], TMG), принятый парламентом в январе 2007 г., в § 8 TMG прямо говорит, что поставщики не несут ответственности за передаваемую информацию, если они не инициировали передачу или изменение передаваемых данных[61].

Серьезной проблемой для системы цензуры Германии является политика по отношению к иностранным сайтам. Так, в сентябре 1996 г. по предписанию Генеральной прокуратуры Германии немецкие провайдеры предприняли попытки блокировать доступ к сайтам, таким, например, как размещенный в Нидерландах сайт праворадикального журнала «Радикал». Эта акция имела обратный эффект в виде дальнейших публикаций этого материала, включая его расползание по зеркалам сайта, сгенерированным в различных частях мира под различными юрисдикциями. В июле 2000 г. правительство Германии объявило, что оно прекращает ограничивать доступ к контенту за пределами страны, однако полиция продолжит мероприятия по предотвращению размещения «доморощенного» материала. Агентство Рейтер сообщило: «Германия, которая обладает самым суровым законодательством в мире против разжигания расовой пропаганды, потерпела неудачу с трансграничным обменом данных в интернете при попытке ограничить доступ к иностранным неонацистским сайтам. Заместитель министр внутренних дел Германии Бриджит Зиприс, отвечающая за интернет-безопасность в стране, ответила в интервью Рейтер, что нереалистично пытаться

[59] Strafgesetzbuch [German Criminal Code], Section 130 // http://goo.gl/EVaFC

[60] Telemediengesetz // http://www.gesetze-im-internet.de/tmg/

[61] Telemediengesetz // http://goo.gl/VOQ4c

экранировать Германию от иностранных сайтов, даже если полиция имеет своей целью пресечь деятельность доморощенных нацистов. Настолько же нереалистично бороться с другими угрожающими материалами, такими как детская порнография, — заявила она»[62]. В настоящее время провайдеры Германии снова обязаны блокировать праворадикальные сайты.

Федеральное устройство Германии позволяет осуществлять интернет-цензуру на региональном уровне. В 2002 г. земельный правительственный округ Дюссельдорф обязал провайдеров ограничивать доступ к четырем сайтам, зарегистрированным в США и содержащим праворадикальные материалы. Ограничения, которые должны были действовать в федеральном округе Северный Рейн — Вестфалия, могли быть реализованы любым из трех способов: DNS-блокировкой, IP-блокировкой или использованием прокси-серверов[63]. Онлайн-петиции, осуждающие эти попытки заблокировать доступ, собрали более 26 тыс. подписей. Однако ни политические демонстрации, ни судебные иски против этого решения не достигли успеха — решением административного суда Дюссельдорфа в 2005 г. блокировка была одобрена.

Другой важной причиной интернет-цензуры в Германии является защита молодежи. Список медиаресурсов, запрещенных к показу несовершеннолетним, составляется Федеральным медиадепартаментом[64]. Распространение в интернете порнографических материалов запрещается, если провайдер не в состоянии обеспечить недоступность такого контента для несовершеннолетних (п. 184d Уголовного кодекса Германии[65]). Например, портал Flickr выполнил это требование, запретив немецким пользователям доступ

---

[62] Tanner A. Germany won't block access to foreign Nazi sites // Silicon Valley News. 2000. 25 Jul.

[63] Sperrungsverfügung [Blocking Order], http://goo.gl/gFRTO

[64] www.bpjm.com

[65] Strafgesetzbuch [German Criminal Code], Section 184 // http://goo.gl/2OTOV

к фото с пометой «ограничено»[66]. В феврале 2005 г. сервисы Google Germany, Lycos Europe, MSN Germany, Germany AOL, Yahoo и T-Online решили самостоятельно регулировать поисковые результаты под руководством ассоциации «Добровольное саморегулирование мультимедийных поставщиков» (FSM)[67]. Один из приемов FSM состоит в исключении сайтов, содержащихся в черном списке BPjM, из поисковых индексов членов ассоциации. В настоящее время список BPjM регулярно передается на специальный скрытый сервер; поисковые системы загружают список и автоматически удаляют соответствующие записи.

В ноябре 1999 г. немецкий апелляционный суд отменил приговор против бывшего главы провайдера «КомпуСерв-Германия» по обвинению в распространении детской порнографии в Сети. Суд постановил, что для главы КомпуСерв было невозможно блокировать публикацию детской порнографии в Сети[68].

В апреле 2009 г. правительство Германии подписало законопроект, который должен был начать крупномасштабные фильтрации сайтов с детской порнографией. Тем не менее от этого закона отказались в 2011 г. вследствие избыточности его мер, так как обнаружилось, что интернет-провайдеры быстро удаляют детскую порнографию после того, как узнают о ней. Еще до вступления этого закона в силу на это обращали внимание организации и партии, защищающие свободу интернета, такие как Свободная демократическая партия и Партия пиратов.

Дания

Дания считается одной из стран с высочайшим уровнем свободы прессы, согласно оценкам организации «Репор-

---

[66] Flickr Content filters // http://www.flickr.com/help/filters/#249

[67] Selbstregulierung der Suchmaschinenanbieter' [Self-regulation of Search Engine Providers] // http://goo.gl/Kq3jN

[68] Court reverses Net porn charge, AFP, 23 Nov 1999.

теры без границ»[69]. Датское королевство не имеет закона, уголовно преследующего за размещение в интернете материалов, неприемлемых для несовершеннолетних и не намеревается издать подобный закон.

Тем не менее цензура интернета стала обсуждаться в Дании начиная с 2005 г. в связи с проблемой детской порнографии, распространением файлообменников и в особенности роста популярности The Pirate Bay, которая была заблокирована провайдерами на уровне DNS. 23 декабря 2008 г. 3863 сайта, разместивших документы Викиликс, были подвергнуты фильтрации[70]. В ноябре 2011 г. блокирование DNS было распространено на сайты, продающие наркотики, и на сайты азартных игр, не имеющих лицензии.

Эта ситуация была подвергнута критике и в июне 2011 г. в открытом письме[71]. Конфедерация датских IT-компаний обратилась к правительству страны с призывом изменить практику по этому вопросу и сделать законодательство ясным и недвусмысленным. В 2012 г. провайдеры и владельцы авторских прав согласились на концепцию, согласно которой все провайдеры будут блокировать доступ к конкретному контенту, нарушающему авторские права, при условии, что если одного из провайдеров к этому обяжет суд. Министерство культуры Дании планировало сотрудничать с провайдерами и правообладателями с целью формализовать соглашение в виде «письменного кодекса поведения».

Еще 27 мая 2010 г. датский Верховный суд поддержал решение суда низшей инстанции, обязывающее провайдеров блокировать доступ к сайтам, которые могут содержать или содержать ссылку на материалы, нарушающие авторские права. Это решение неоднократно критиковалось как попрание интернет-свободы в Дании. Критики утверждали, что решение придало слишком большой вес правам

[69] 2013 world press freedom index: dashed hopes after spring // http://goo.gl/dd7zY

[70] http://goo.gl/62BGQ

[71] Samlet it-branche i skarp protest mod dansk internetcensur // http://goo.gl/rNMX4

правообладателей интеллектуальной собственности, игнорируя очевидную опасность ограничения свободы доступа к информации в интернете. Они также отмечали, что решение может привести к блокировке сайтов, которые в основе своей не содержат материалов, нарушающих авторские права, и, таким образом, ограничить свободу распространения информации. Указывалось и на явный недостаток надлежащих правовых процедур: фактическое наделение провайдеров полицейскими функциями без ясных и внятных процессуальных правил принятия решения о блокировке создает опасный прецедент, который позволяет расширить черный списки и включить в них другие «нелегальные» и «опасные» материалы в будущем.

В 2005 г. датская полиция инсталлировала так называемый «фильтр детской порнографии» совместно с НКО «Спаси Ребенка». В 2008 г. утечки Викиликс показали, что среди заблокированных сайтов некоторые сайты были неактивны, а некоторые не имели никакого отношения к детской порнографии[72].

В 2010 г. датский парламент принял спорный закон, который позволил налоговым органам требовать от провайдеров блокировки доступа к сайтам азартных игр. В том же 2010 г. Социалистическая народная партия Дании предложила криминализовать серфинг (блуждание по сайтам) по «сайтам, имеющим отношение к террору» и дважды предлагала забанить «психоделический» ресурс www.psychedlica.dk за распространение информации о наркотиках. Датское правительство также было очень активно в закрытых переговорах по заключению Торгового соглашения по борьбе с контрафакцией (ATCA[73]). Согласно утечкам, поступившим от участников переговоров, в черновике соглашения предусмотрены меры, которые можно рассматривать как

[72] http://goo.gl/8QpO

[73] http://www.ustr.gov/acta

глубоко нарушающие свободу интернета и право на частную жизнь[74].

Малайзия

В 90-е годы XX века Малайзия была известна как страна, в которой практически отсутствовала интернет-цензура, более того, в 1999 г. правительство страны заявило, что намерено придерживаться политики отказа от регулирования интернета. Так дела обстояли до 2012 г., пока не случилось событие, известное в мировых СМИ, как «интернет-блэкаут». Обычно блэкаутом называют потерю электроснабжения, охватывающую целые территории. В данном случае никаких технических сбоев не было. Этим словом была названа серия скоординированных протестных акций против одного законопроекта, которые осуществляли Центр за независимую журналистику[75] (CIJ) при поддержке Международной ассоциации по защите свободы слова (IFEX) и Юго-восточного азиатского альянса прессы (SEAPA). Протест был вызван второй поправкой к процессуальному закону о предоставлении доказательств (1950). Эта поправка известна, как раздел 114A закона о доказательствах[76].

Поправка была выдвинута министром юстиции Назри Азизом в нижней палате парламента (Деван Ракат) 18 апереля 2012 г. Поправка была принята после третьего чтения. 9 мая в верхней палате парламента Малайзии (Деван Негара) поправка вступила в действие, после утверждения и публикации в официальном бюллетене от 31 июля 2012 г.

Поправка позволяет сотрудникам правоохранительных органов оперативно привлекать к ответственности за публикацию крамольного, дискредитирующего, клеветнического контента в интернете. Раздел 114A «Презумпция факта в публикации» позволяет привлечь к ответственности за

[74] http://goo.gl/a3tVm

[75] http://cijmalaysia.org/

[76] About section 14A. // http://goo.gl/xiE1a

публикацию на сайте перечисленные выше виды контента следующие категории лиц :

— граждан, владеющих, управляющих и редактирующих веб-сайты, открытые для общественности участниками, такими как интернет-форумы или блоги;

— лиц, предоставляющих услуги веб-хостинга и доступа в интернет;

— граждан, владеющих компьютером или мобильным устройством, использующих их для публикации материалов онлайн.

Другими словами, если техническими средствами будет установлено, что предположительно клеветническое содержание ведет к вашему имени пользователя, электронному прибору и/или Wi-Fi Сети, согласно разделу 114A, вы являетесь виновными в незаконной публикацией контента в интернете по законам Малайзии.

Даже если у вас украли личные данные и от вашего имени сделали клеветнические записи в социальных сетях, в соответствии со ст. 114A вы по-прежнему считается виновным, пока не доказано обратное. Претензии правозащитников к разделу 114A выглядят следующим образом:

— закон обременяет среднего пользователя интернета несоразмерными обязанностями и ответственностью в случае неправомерного обвинения в публикации крамольного или клеветнического содержания;

— различные интернет-посредники, а именно стороны, которые обеспечивают работу интернет-форумов, сообществ, блогов и хостингов, солидарно несут ответственность за опубликованный на их ресурсах контент;

— закон позволяет хакерам и киберпреступникам оставаться на свободе, подставляя под уголовную ответственность лицо, чей компьютер был взломан и от чьего имени размещались противоправные материалы;

— закон принят поспешно и не учитывает общественные интересы.

Австралия

В режим интернет-цензуры в Австралии включается законодательство как на федеральном уровне Австралийского Союза, так и на уровне правительств штатов/территорий. Любопытно, что австралийский режим является системой, основанной на жалобах к хостинг-провайдерам, а не к создателям или контент-провайдерам. Хост-узелом должен быть удален австралийский контент с сервера, который считается «нежелательным» или «неприемлемым для несовершеннолетних», согласно рекомендациям правительственного регулятора Австралийское телерадиовещательное управление (ABA). До марта 2002 г. закон действовал таким образом, что не предписывал провайдерам блокировать доступ к контенту, размещенному на хостах за пределами Австралии. Однако ABA уведомила провайдеров, осуществляющих фильтрацию и блокировку, что контент за пределами Австралии должен быть включен в их черные списки.

Кроме того, уголовные законы штатов и территорий позволяют преследовать пользователей интернета, которые делают доступными материалы, считающиеся «нежелательными» или «неприемлемыми для несовершеннолетних». Особенности уголовного преследования отличаются в рамках каждой юрисдикции.

В апреле 1999 г. правительство Австралии представило в парламент билль «О цензуре в интернете». Этот билль, если бы он был принят без поправок, предписывал бы интернет-провайдерам среди прочего блокировать доступ взрослых пользователей к содержанию сайтов за пределами Австралии на основании угроз о несоответствии национальному законодательству. Предполагаемый закон подвергся всесторонней критике и был исправлен. В него включили положение о методе дополнительного предупреждения (отличном от блокирования зарубежного материала, размещенного на правах хостинга, на уровне сервера).

Закон с поправками, известный как Поправка телерадиовещательных сервисов (интернет-сервисов), был принят 1 января 2000 г.

Канада

В августе 1998 г. канадская комиссия по телерадиокоммуникациям (CRTC[77]) организовала публичную дискуссию с целью определить, какую роль комиссия должна играть (если вообще должна) в области регулирования детской порнографии, проявлений нетерпимости и так называемого «канадского контента» в Сети.

Впоследствии, 17 мая 1999 г., CRTC выпустил медиарелиз под заголовком «CRTC не хочет регулировать интернет»[78], содержащий следующее утверждение: «Канадская комиссия по телерадиокоммуникациям пришла к выводу, что новые медиа в интернете достигли целей телерадиовещательного закона и являются живыми, высококонкурентными и успешными без регуляции. CRTC пришла к заключению, что всякая попытка регулировать канадские новые медиа могут вызвать в отрасли ущерб с точки зрения мировой конкуренции»[79].

Иран

Исламская Республика Иран вкладывает немалые средства в технологии фильтрации интернет-контента, которые являются одними из самых развитых в мире. В 2000 г. в стране была установлена система выявления и блокировки нежелательных сайтов с усиленной фильтрацией на уровне провайдера; за публикацию онлайн-материалов власти арестовали несколько десятков человек. В то же время Иран перешел на усиленную и более сложную систему интернет-цензуры, которая координируется различными ведомствами и службами. С 2008 г. стали вводиться средства централизованной фильтрации, причем собственного производства, что уменьшило зависимость Ирана от западных технологий. Основой контент-контроля страны является

[77] http://www.crtc.gc.ca/eng/home-accueil.htm

[78] http://goo.gl/zd83F

[79] Ibid.

маршрутизация всего интернет-трафика через прокси-серверы. Это позволяет блокировать конкретные веб-страницы, а также ключевые слова. Так, во время президентских выборов 2009 г. блокировались политические сайты, в частности www.yaarinews.ir — сайт в поддержку бывшего президента Мохаммада Хатами[80]. В 2006–2009 гг. были случаи блокировки Facebook, блокировалась загрузка с таких видеохостов, как Youtube и Flickr.

«Репортеры без границ» до настоящего времени включают Иран в список «врагов интернета»[81]. В 2012 г. эта страна наряду с Китаем признана крупнейшим в мире пользователем систем цензуры[82]. За уклонение от национальной системы контроля за интернетом здесь предусмотрены суровые наказания вплоть до лишения гражданских прав.

Иранский сектор интернета растет быстрыми темпами. За 2005–2008 гг. число пользователей в Иране выросло с менее чем миллион человек до 23 млн[83]. Эти темпы роста выше, чем в любой другой стране на Ближнем Востоке. Иранская блогосфера была объявлена одной из крупнейших и самых активных в мире. Число активных персидских блогеров, по оценкам, около 60 тыс.[84] Иранская политика по отношению к интернету отражает сильное противоречие между попытками контроля и поддержкой инноваций и экономического роста, осуществляющихся за счет ИКТ.

В четвертом пятилетнем плане развития Ирана были призывы к расширению интернетизации с помощью создания 1,5 млн точек высокоскоростного подключения по всей стране[85]. Тем не менее в октябре 2006 г. министерство связи

---

[80] Cracking Down on Digital Communication and Political Organizing in Iran// http://goo.gl/ZqKXY

[81] http://surveillance.rsf.org/en/

[82] Scrom P. SOPA & PIPA: Human Rights in Intellectual Property & Freedom of Speech // http://goo.gl/TWLPf

[83] ITU Internet Indicators // http://goo.gl/Z3CBl

[84] Kelly J., Etling B. Mapping Iran's Online Public: Politics and Culture in the Persian Blogosphere. Berkman Center for Internet and Society. 2008.

[85] Bahar A. Iran Telecom Brief. 2008.

и информационных технологий издало указ, который запрещал провайдерам предоставлять домашним хозяйствам и общественным пунктам доступ подключения к интернету на скоростях больше 128 Кб/с. Эта политика ограничения возможности скачивать мультимедийный контент, скорее всего, направлена на затруднение доступа к альтернативным интернет-СМИ, которые могли бы конкурировать с жестко контролируемым радио- и телевещанием.

На фоне ограничений свободы слова в прочих сферах интернет в Иране первоначально давал относительную свободу общения, позволяя процветать независимым СМИ и выражать оппозиционные мнения, например точку зрения сторонников секуляризации и политических реформ. С ростом популярности виртуальной среды цензура стала увеличиваться. Контроль за выражением особого мнения в интернете стал одной из целей государственной политики. В настоящее время независимые интернет-СМИ доступны в Иране практически только на английском языке. Постоянное ужесточение контроля ухудшает атмосферу в онлайн и способствует самоцензуре.

Институциональные основы для технологии фильтрации в Иране выросли из ряда указов Верховного совета культурной революции (ВСКР) в декабре 2001 г. о необходимости использовать систему фильтров для провайдеров. Год спустя был создан межведомственный комитет, ответственный за определение неавторизованных сайтов. Этот комитет также принимает решение о блокировке определенных доменов. ВСКР определяет для этого комитета руководящие принципы и курирует его членов, среди которых есть представители министерства связи и информационных технологий, министерства культуры и исламской ориентации, министерства разведки и национальной безопасности, а также генеральный прокурор Тегерана[86].

Что касается законодательных основ, то поправки (2000, 2009) к иранскому закону о печати (1986) распростра-

[86] A Report on the Status of the Internet in Iran // http://goo.gl/Qqt90.

нили его на все интернет-издания[87]. В этом законе изложены не только основные ограничения на свободу слова, но и нормативы для прессы, которая обязана «распространять и продвигать подлинную исламскую культуру и выражать этические принципы»[88]. Уголовный кодекс Ирана определяет такие преступления, как пропаганда против государства, «оскорбление религии», создание «тревоги и беспокойства в общественном сознании», распространение «ложных слухов», критика чиновников. Другой ключевой частью законодательства для регулирования онлайн-контента в Иране стал билль о киберпреступлениях, ратифицированный в ноябре 2008 г. Он требует от провайдеров, чтобы «запрещенный» контент не отображался на их серверах, информация о нем немедленно поступала в правоохранительные органы и контент сохранялся в качестве доказательств.

Активную роль в установлении стандартов контента также начал играть Корпус стражей исламской революции (КСИР). Представители этой организации заявили о создании десяти тысяч блогов, ведущихся членами Басидж — добровольческих отрядов народного ополчения, подчиняющихся КСИР. Таким образом, информационная война в интернете включает различные стратегии и поддерживается правительством Ирана.

Саудовская Аравия

Две трети пользователей Саудовской Аравии — женщины, всего интернетом пользуются 38,5% подданных. Женщины этой родины ислама в подавляющем большинстве — домохозяйки, их свобода ограничена строгими религиозными правилами. По этой причине интернет является для них как окном в мир, в который они не могут выйти без

[87] The new decision for the internet media by the parliament // http://www.ghalamnews.ir/news-6261.aspx.

[88] Memorandum on Regulation of the Media in the Islamic Republic of Iran. Article 19. // http://goo.gl/5PYfQ.

сопровождения мужчины, так и способом социализации и эмансипации.

В Королевстве Саудовская Аравия с февраля 1999 г. публичный доступ к интернету, включая входящий и исходящий трафик, ведет к «бутылочному горлышку» единственного в стране правительственного контрольного центра. Следует отметить, что в этом экономически преуспевающем государстве интернет стал доступен именно в 1999 г., т.е. не раньше момента, когда государство сумело наладить соответствующую инфраструктуру для цензуры.

Внутренний сегмент саудовского интернета сообщается с Глобальной сетью через прокси-ферму, расположенную в Королевском технополисе (KACST). Контент-фильтр основан на программном обеспечении фирмы «Secure Computing». С октября 2006 г. комиссия по коммуникациям и информационным технологиям (CITC) разместила на этой ферме структуру DNS и систему фильтрации. Кроме того, множество сайтов были заблокированы согласно двум черным спискам, составленным и пополняемым подразделением интернет-сервиса Internet Services Unit (ISU)[89] Королевского технополиса. На страничке этого подразделения совершенно разъясняется, что и какими средствами блокируется. Отмечается, что 95% заблокированных сайтов являются порнографическими, остальные посвящены наркотикам, алкоголю, азартным играм, антиисламской и антигосударственной пропаганде. Пропаганда религиозной идеологии шиизма также может привести к блокировке. Королевская семья очень чувствительна к любой критике официальной ваххабитской версии ислама, и все сайты, в которых критикуется ваххабизм, заблокированы. Характерная особенность данной системы цензуры: она направлена на сотрудничество с подданными, на сайте подразделения можно написать заявление о блокировке того или иного ресурса. Для этого существует специальная форма,

[89] http://goo.gl/TGwdA

и, как сообщается, сотни заявлений приходят каждый день от обеспокоенных моралью подданных королевства.

Блокируются и безобидные с точки зрения западного общества сайты, посвященные, например, планированию семьи, сексуальному образованию, феминизму и правам сексуальных меньшинств. 11 июля 2006 г. была заблокирована Википедия и сервис Гугл-переводчик, который использовался нарушителями режима цензуры для обхода фильтров с помощью перевода страниц блокированных сайтов[90].

Юридические основания для фильтрации контента содержатся в резолюции Совета министров от 12 февраля 2001 г., под названием «Саудовские интернет-правила»[91]. Обратим внимание на то, что этот документ является постановлением правительства, т.е органа исполнительной, а не законодательной власти. В большинстве стран мира информационная политика является приоритетом законодательной власти, поскольку затрагивает фундаментальные права и свободы. Впрочем, Саудовская Аравия является по форме правления абсолютной монархией и ни о каких демократических стандартах и представлениях не может быть и речи. Интернет-правила предписывают всем пользователям на территории королевства воздержаться от публикации или попытки доступа к данным, содержащим, в частности, следующее:

— все, противоречащие основополагающим принципам законодательства или попирающее святость ислама и шариата или нарушающее общественные приличия;

— все, что против государства или его системы власти;

— все, что наносит ущерб достоинству глав государств или глав аккредитованных в королевстве дипломатических представительств других стран или вредит отношениям с этими странами;

---

[90] http://archive.is/SrHQ

[91] http://www.al-bab.com/media/docs/saudi.htm

— любую ложную информацию, приписываемую государственным чиновникам, частным лицам и организациям, способную нанести им вред или нарушить их целостность;

— пропаганду подрывных идей, нарушения общественного порядка и диспутов между гражданами.

Правила предписывают также всем создателям медиасайтов, которые публикуют новости на регулярной основе, получать разрешение в министерстве информации. Кроме того, отмечается, что «все юридические и физические лица несут полную ответственность за свои сайты и страницы, за информацию, содержащуюся в них».

Отдельно резолюция апеллирует к множеству регуляторных и технических процедур, направленных на укрепление безопасности компонентов национальной Сети с помощью эффективного программирования и архитектуры Сети, в частности следующее:

— провайдеры обязаны фиксировать факты доступа в интернет через специальные аккаунты, включающие идентификацию пользователей и эффективные пароли для использования в точке доступа или в последующих точках; отслеживать их с помощью трассировки и специальных программ мониторинга, которые записывают время, фиксируют место доступа или место, через которое была предпринята попытка доступа, размер и тип копируемых файлов;

— контролировать использование антивирусных программ и программ защиты против скрытия адресов или набора паролей и загрузки файлов;

— хранить в бумажном и электронном виде полные регистрационные данные конечных пользователей, их адреса, номера телефонов, цели использования, данные аккаунтов доступа; обеспечивать власти копиями этих данных в случаях необходимости.

В 2011 г. правительство ввело новые правила и регулятивные нормы для онлайн-газет и блогеров, требующие специальной лицензии от министерства культуры и инфор-

мации[92]. Согласно новым правилам, все авторы в Сети, включая авторов на форумах и авторов коротких сообщений вроде Твиттера должны получить лицензию, срок действия которой составляет три года.

Правительство объяснило нововведение тем, что оно должно защитить общество от тлетворных влияний и отметило, что оно уже давно осуществляет политику интернет-цензуры. Следует обратить внимание на то, что Саудовская Аравия имеет одно из самых больших количеств блогеров среди арабских стран. Заявители на получение лицензии должны быть старше 20 лет и иметь законченное полное среднее образование. Им также требуется предъявить документы, которые «доказывают их хорошее поведение». Любой, кто будет пойман за блогингом без лицензии, подвергается штрафу в 100 тыс. риалов (примерно 27 тыс. долларов) и/или будет забанен, возможно, навсегда. В то же самое время, когда вышли новые правила, саудовское правительство заблокировало страницу Викиликс на арабском языке.

Эти законодательные нововведения были жесточайшим образом раскритикованы арабской сетью за права человека, представители которой сказали, что саудовское правительство своими действиями поставило себя в топлист автократических режимов не только в арабском мире, но и во всем мире: «Это не регуляция деятельности в сфере электронных публикаций, как они утверждают, но скорее система мер по ограничению свободы слова в интернете». Большинство влиятельных СМИ королевства поддержали новые правила. Выпускающий редактор газеты «Асхарах Алавасат» Тарик аль-Хомайед заявил: «Министерство все сделало верно. Кто сказал, что свобода приходит без ответственности? Разве не было сказано, что в сферу публицистики двери остаются широко открытыми? Все, кто хочет писать, быть опубликованным, критиковать других, должны делать это достоверно, с твердых позиций, а не прятаться за экраном компьютера, чтобы опорочить кого-то, распространять

[92] http://goo.gl/fJLn7.

уродливые слухи или разжигать общественную рознь под чужим именем, а затем иметь смелость, чтобы сказать: дайте мне выразить мою свободу!»[93] В Саудовской Аравии многие статьи английской и арабской Википедии подвергнуты цензуре безо всякого объяснения.

Китай

В сентябре 1996 г. Китай сообщил, что он заблокировал доступ примерно к ста сайтам с помощью системы фильтрации для предотвращения распространения информации, посягающей безопасности страны. Заблокированные сайты включали в себя западные информационные порталы, тайваньские новостные агентства, антикитайские диссидентские сайты и сайты с откровенным сексуальным содержанием.

Начиная с 1996 г. китайское правительство приняло множество строгих законодательных актов, запрещающих политическую полемику, нежелательную с точки зрения правительства, и т.п. Множество сайтов зарубежных медиа и правозащитных сайтов были заблокированы.

Информационное агентство «Ассошиэйтед Пресс» сообщило 18 января 2002 г., что Китай создал наиболее навязчивую систему контроля интернета, предписывающую досматривать частные электронные письма на предмет выявления политического содержания и налагать ответственность за размещение подрывной информации на сайтах провайдеров. Согласно новым правилам, интернет-порталы должны инсталлировать программы безопасности с целю досмотра и архивирования входящей и исходящей электронной переписки. Те материалы, которые будут распознаны программами как содержащие «чувствительные материалы», должны переадресовываться властям. Также провайдеры ответственны за стирание всех запрещенных текстов, включая чаты и доски объявлений.

Новые правила включают в себя длинный перечень запрещенного контента, раскрывающего государственные

[93] Ibid.

тайны, от которого страдает репутация Китая как государства и в которых призывается к свержению коммунизма, а также пропагандируется сепаратизм или «культы зла».

Последняя категория включает в себя духовное движение «Фалуньгун», которое часто прибегает к возможностям интернета с целью противостоять суровым репрессиям в последние два года. Запрещены также порнография и сцены насилия.

Китай обладает одной из самых развитых и сложных систем интернет-фильтрации в мире. Сообщество китайских пользователей продолжает расти, в то время как государство наращивает свою способность блокировать контент, который может угрожать социальной стабильности, ужесточая положения о местных СМИ, делегируя ответственность провайдерам, или с помощью временных фильтров и кампаний «зачистки». Организация «Репортеры без границ» постоянно дает Китаю худшую из возможных оценок свободы интернета[94].

Китайские сайты до появления в интернете подлежат регистрации и проверке. Практически весь иностранный контент также проходит те или иные фильтры. Широко известен китайский проект централизованной фильтрации «Золотой щит» (The Golden Shield Project, неофициальное английское название Great Firewall of China намекает на Великую китайскую стену), введенный в использование в 2003 г. Он представляет собой систему серверов на интернет-канале между провайдерами и международными сетями, где ведется фильтрация по ключевым словам и адресу сайта. Иностранные поисковые машины, работающие в Китае, включая Google, Yahoo и Bing, аналогичным образом фильтруют результаты поиска. Так, в январе 2009 г. власти Китая закрыли доступ к интернет-сайту, на котором были выложены пляжные фотоснимки китайской актрисы Чжан Цзыи в компании с израильским бизнесменом Авива Нево.

---

[94] The Enemies of the Internet Special Edition : Surveillance, Reporters Without Borders // http://goo.gl/OfcBr.

Запрет привел лишь к тому, что эти фотографии стали самыми разыскиваемыми и скачиваемыми в Тайване, а авторитетное израильское издание «The Marker» посвятило этой истории статью[95]. Под блокировку «Великого китайского файрволла» 25 сентября 2009 г. попали 80% IP-адресов публичных серверов анонимной сети Tor[96].

В Китае разрабатываются и другие способы интернет-фильтрации. Одним из них был проект фильтрации на уровне пользовательского компьютера «Green Dam Youth Escort». Программное обеспечение, которое должно было устанавливаться на все компьютеры китайского производства, было заявлено как защита несовершеннолетних от контента для взрослых. В исследовании специалистов из ONI и Stop Badware выяснилось, что эти программы не только не эффективны в фильтрации порнографии, но и блокируют многие политические и религиозные материалы, обычно ассоциирующиеся с проектом «Золотой щит»[97]. После публикации этих выводов министерство промышленности и информационных технологий (MIIT) сделало установку программ опциональной. Несмотря на очевидный провал проекта, подобный пакет под названием «Blue Dam» в сентябре 2009 г. было поручено установить всем провайдерам.

Хотя не более половины населения Китая имеет доступ в интернет, это самая многочисленная группа пользователей в мире, и она постоянно растет. Масштабной реструктуризации телекоммуникационная отрасль в Китае подверглась в 2008 г., когда шесть государственных компаний объединились в три сети, что значительно увеличило возможности выхода на рынок крупных фирм. С развитием китайского сектора интернета по всей стране создаются яркие и динамичные сообщества, привлекающие внимание властей. Онлайн-обсуждения часто придают локальным

[95] http://newsru.co.il/rest/03dec2009/aviva_ziyi_111.html

[96] Tor partially blocked in China // http://goo.gl/ha7Xh

[97] China's Green Dam: The Implications of Government Control Encroaching on the Home PC// http://goo.gl/Viru2

событиям общенациональное звучание, угрожая репутации высших чиновников. В неопубликованном отчете об исследовании, предпринятом Дэвидом Бандурски из China Media Project[98], сказано, что две трети из нескольких сотен тайных внутренних отчетов, которым лидеры КПК уделяют особое внимание, приходят из отдела интернета Управления информации Государственного совета[99].

Активная контринформационная кампания в Китае была стимулирована важными политическими событиями 2008–2009 гг. В годовщину Тибетского восстания (1959), протесты вспыхнули в Лхасе 10 марта 2008 г., слышались призывы к защите прав человека, к свободе вероисповедания и в некоторых случаях к политической независимости. И когда в преддверии Олимпийских игр внимание международного сообщества было обращено на Китай, вспыхнули протесты не только в тибетских общинах Китая, но и по всему миру. Китайское правительство в ответ начало репрессии в Тибетском автономном районе, подавляя отечественные и зарубежные средства массовой информации, систематически блокируя онлайн-контент, относящийся к инциденту[100]. По мере приближения Олимпиады Китай испытывал возрастающее международное давление: уменьшить цензуру и выполнять свои обязательства в предоставлении условий иностранным СМИ для свободного вещания во время игр. В итоге официальная политика предоставила небывалый уровень свободы, однако правительство продолжало осуществлять строгий контроль над местными СМИ, жестко пресекая объективное освещение событий на китайском языке. Кроме того, хотя правительство КНР первоначально согласилось предоставить журналистам неограниченный доступ в интернет во время Олимпийских

[98] Bandurski D. China's Guerrilla War for the Web // Far Eastern Economic Review. 2008 // http://testfeer.wsj-asia.com/essays/2008/august/chinas-guerrilla-war-for-the-web

[99] Ibid.

[100] China: Investigate Crackdown before Torch Relay's Passage through Tibet // http://goo.gl/oTgcJ

игр, это обещание было переосмыслено как относящееся только к тем сайтам, которые «связаны с играми»[101]. Множество сайтов, ориентированных на политику и права человека, продолжали блокироваться, пока продолжались игры. После Олимпиады новые правила для иностранных СМИ, работающих в Китае, оставались некоторое время неизменными. Однако события следующего года привели к ужесточению ограничений и усилению контроля.

В апреле 2009 г. был выпущен документ — «Национальный план действий Китая относительно прав человека», в котором, в дополнение к многочисленным другим обязательствам, давалось обещание: «…государство будет принимать эффективные меры по развитию прессы и отраслевых изданий и обеспечит разблокировку всех каналов, чтобы гарантировать право граждан быть услышанными»[102]. Тем не менее в течение года Китай продолжал ужесточать цензуру и усиливать ограничения для внутренних средств массовой информации и коммуникации. В рамках подготовки к многочисленным важным событиям: к 60-летию основания КНР, к 50-летию Тибетского восстания и отступления далай-ламы в Индию, и первой годовщине протестов в Тибете, начатых того же числа, к 20-летию событий на площади Тяньаньмэнь и 10-летию объявления духовного движения «Фалуньгун» вне закона — правящая партия намеревалась ужесточить контроль. Известно о блокировке поисковых запросов и удалении записей блогов по ключевым словам, касающимся соответствующих исторических событий.

В июле 2009 г. произошли столкновения между хань и уйгурами в Урумчи, спровоцированные убийством нескольких уйгурских рабочих на фабрике игрушек. Это были самые серьезные гражданские беспорядки на терри-

[101] Batty D. Media Face Web Censorship at Beijing Olympics // The Guardian. 2008 // http://goo.gl/OZRaQ

[102] Information Office of the State Council of the People's Republic of China, National Human Rights Action Plan of China (2009–2010) // http://goo.gl/5WCju

тории Китая за последние десятилетия. Они привели к суровым и множественным ограничениям деятельности китайских средств массовой информации и коммуникации. В отличие от волнений прошлого года, Китай допускал и даже поощрял иностранные СМИ в освещении этого конфликта. Однако прессе разрешалось пребывать только в Урумчи и описывать насилие только с уйгурской стороны. Запрещалось сообщать о ликвидации последствий инцидента — многочисленных арестах и допросах уйгуров или загадочном исчезновении подозреваемых[103]. Некоторые китайские журналисты при попытке объективного освещения событий подверглись моральному и физическому преследованию[104]. Резко ужесточилась интернет-цензура по всей стране, в том числе были заблокированы Facebook, Twitter и другие социальные сети, а в провинции Синьцзян, кроме того, доступ в интернет и к телефонной связи[105]. Утверждалось, что всемирный уйгурский лидер Ребия Кадир «использовал интернет и другие средства связи для вдохновления бунта». Хотя телефонное сообщение постепенно восстанавливалось, доступ к интернету фактически отсутствовал в течение десяти месяцев.

В январе 2010 г. Google после серии кибератак, за которые взяли на себя ответственность китайские активисты, объявил, что больше не будет поддерживать китайский стандарт фильтрации контента. После серии напряженных переговоров китайский Google.cn был закрыт, его пользователи стали перенаправляться на Google.com.hk в Гонконге. Позднее сообщалось, что правительство блокирует оба адреса, хотя и спорадически[106]. Чтобы сохранить китайских пользователей, Google изменил подход и включил ссылку на

[103] http://goo.gl/DqqK3

[104] China: Journalists Protest Savage Attacks on Colleagues // http://goo.gl/1WoT5

[105] China Shuts Down Internet in Xinjiang Region after Riots // http://goo.gl/OjlFL

[106] Tan K. The Google.cn/Google.com.hk Lockdown Has Begun: ALL Search Queries Now End in a Connection Reset // http://goo.gl/NGwRw

Google.com.hk в китайскую страницу. Эти события привлекли международное внимание к интернет-цензуре в Китае. В том же году Государственный секретарь США Хиллари Клинтон критиковала страну за препятствие свободному обмену информацией.

Туркменистан

Туркменистан получил доступ к интернету в 1997 г. на основе договора с MCI Communications (позже — MCI WorldCom). Небольшое число независимых провайдеров были изгнаны из бизнеса в 2001 г., когда Туркментелеком получил монополию на услуги передачи данных. Теперь все интернет-каналы проходят через систему серверов и центральный узел Туркментелеком и тщательно контролируются службами безопасности. Есть основания полагать, что на серверах установлена технология фильтрации, настроенная на определенные ключевые слова или, например, на шифрованные сообщения, а отправители сообщений могут быть отслежены[107].

Предпочтительным методом ограничения контента является блокирование. С 2009 г. блокировке подвергались Youtube, LifeJournal, Facebook и некоторые другие известные иностранные интернет-ресурсы. Кроме того, многие частные пользователи, имеющие свои веб-ресурсы (сайты, почту и прочее) на хостинг-площадках за пределами страны, испытывали трудности в доступе к ним[108]. «Репортеры без границ» с декабря 2010 г. включают Туркменистан в список «врагов интернета»[109].

Туркментелеком предупреждает на своем сайте, что интернет не является «местом для непродуманного поведения». Пользователи должны воздерживаться, например, от размещения материалов, содержащих нецензурную брань,

---

[107] Turkmenistan Helsinki Foundation for Human Rights // http://goo.gl/qgrYD.

[108] http://www.electroname.com/story/4665.

[109] Internet Enemies, Reporters Without Borders // http://goo.gl/nkVLo.

от демонстрации «неадекватного поведения» в онлайн, размещения информации, которая конфликтует с общепринятыми нормами поведения и законодательства, а также от загрузки порнографических материалов. Контракт, подписанный оператором и пользователем, содержит еще больше ограничений, таких как запрет на доступ к сайтам, содержащим сцены насилия, и сайтам, распространяющим «неправдивую и клеветническую информацию» (определение, которое включает в себя оппозиционные сайты). Пользователи несут ответственность за любые действия, которые могут нанести вред правительству или «кому-либо другому».

Если организации удается приобрести постоянное соединение, она заключает контракт, в котором оговаривается, что учетная запись предназначена только для собственного пользования, предоставлять ее другим запрещено. Заявки на подключение частных лиц с начала деятельности Туркментелекома до 2008 г. не принимались. Зависимость от дорогих спутниковых каналов ограничивала число пользователей примерно до двух тысяч. Чтобы обновить интернет-магистрали, министерство связи подписало контракт с Tata Communications для маршрутизации трафика через волоконно-оптический канал[110]. В результате этого Туркментелеком начал предлагать доступ к более высокой скорости интернета с ADSL потребителям в Ашхабаде. По данным этой организации, в 2008 г. в стране насчитывалось около четырех тысяч частных абонентов. Их было значительно больше в 1996–1999 гг., когда доступ к интернету обеспечивали несколько провайдеров[111]. В 2008 г. МТС начала предоставлять интернет-услуги для абонентов мобильной связи через GPRS, открыв возможность доступа к интернету более низкого качества, но более дешевого.

[110] http://goo.gl/NArpw.

[111] http://hitech.newsru.com/article/05jun2008/inet.

*Табл. 2. Прайс-лист Туркментелекома на домашний интернет с ADSL в 2013 году**

Скорость	Абонентская плата	Стоимость 1 Мб	Стоимость в месяц включая абонентскую плату					
			1 Гб	2 Гб	3 Гб	4 Гб	5 Гб	10 Гб
256 Кб	50	0,04	90,96	131,92	172,88	213,84	254,8	459,6
512 Кб	115	0,03	145,72	176,44	207,16	237,88	268,6	422,2
1024 Кб	200	0,02	220,48	240,96	261,44	281,92	302,4	404,8
2048 Кб	280	0,01	290,24	300,48	310,72	320,96	331,2	382,4

* Курс туркменского маната к российскому рублю на 29.03.2013: 1 TMT = 10.8747 RUR.

Для частных организаций, коммерческих и других в Туркменистане сохраняется запрет на открытие интернет-кафе. В государственных интернет-кафе посетители предъявляют паспорт, их деятельность записывается на правительственном сервере. Кроме того, при вступлении в должность президент Бердымухамедов обещал доступ в интернет каждой школе и запретил открывать новую школу без интернет-класса, что привело к закупке массы компьютеров. Однако из-за неподготовленности учителей и санкций при возможном нарушении цензуры многие интернет-классы закрыты.

Хотя и старая, и новая конституции Туркменистана гарантируют свободу слова, не только интернет, но и другие средства массовой информации и коммуникации контролируются правительством. Предусмотрены уголовное наказание за клевету, оскорбление правительства и президента — такие обвинения часто выдвигаются журналистам.

Южная Корея

Хотя Республика Корея является одним из самых передовых секторов информационно-комуникационных технологий в мире, интернет остается под строгим правовым и технологическим контролем центрального правительства. В 2009 г. Южная Корея была включена «Репортерами без границ» в

список стран «под наблюдением» и продержалась там до 2011 г. В 2008 г. 15 тысяч сообщений в интернете были заблокированы или удалены, в 2011 г. — более 53 тыс. Цензура выражается, например, в закрытии сайтов противников воинской обязанности, гомосексуальных сайтов, в пресечении деятельности партий, симпатизирующих Северной Корее, и аресте их активистов, а также в удалении записей блогов, критикующих президента. Наиболее частым методом является блокирование по IP на уровне провайдера. Провайдер же несет ответственность за то, чтобы содержащийся в его сети контент для взрослых был недоступен несовершеннолетним. Недавно правительство объявило о планировании новых систем предварительной цензуры в будущем.

Южная Корея является мировым лидером в области распространенности и скорости интернет-соединения. К 2010 г. более 81% граждан имели доступ к интернету[112] и более 16 млн человек подписались на широкополосный сервис[113]. Южная Корея предоставляет своим гражданам национальную сеть, которая передает данные со средней скоростью от 17 Мбт[114], самой высокой в мире, — Сеул был назван «мировой столицей пропускной способности». С 2010 г. в стране действовали 126 провайдеров, взаимосвязанных через пять точек обмена трафиком. Тем не менее из этих 126 провайдеров три (KT, ранее известный как Korea Telecom, Hanaro Telecom и Корея Thrunet) контролируют почти 85% рынка широкополосного доступа. KorNet обеспечивает примерно половину ADSL-линий в стране, что делает его крупнейшим поставщиком ADSL в мире.

Несмотря на либеральный политический режим Южной Кореи, свобода слова в интернете защищена здесь меньше, чем в других подобных странах. Ст. 21 южнокорейской

---

[112] Internet Indicators: Subscribers, Users and Broadband Subscribers// http://goo.gl/Z3CBl

[113] Survey on the Wireless Internet Usage Executive Summary // http://goo.gl/wOlkx

[114] Darren A. South Korea Tops Akamai Broadband Averages with 17 Mbps // http://goo.gl/nnkGT

конституции гарантирует, что «все граждане пользуются свободой слова и печати». В то же время статья содержит оговорку, что «ни речь, ни пресса не должны оскорблять честь или нарушать права других лиц, подрывать общественную мораль или социальную этику». Ст. 53 (1), заложенная в основу регулирования контента, закона о телекоммуникационном бизнесе предусматривала, что «человек при использовании телекоммуникаций не должен осуществлять коммуникацию с таким содержанием, которое наносит ущерб общественному спокойствию и порядку или общественной морали и добропорядочности». После ряда изменений в формулировке незаконная информация определяется как нарушающая общественные интересы и общественный порядок, это, в частности, непристойность, клевета, насилие и жестокость, а также подстрекательство к азартным играм. Специальные законы о защите молодежи, национальной безопасности и других национальных приоритетов задают рамки контента, который регулируется органами, ответственными за фильтрацию: Комитетом по регулированию вещания (Broadcasting Regulation Committee, BRC), Корейским советом по рейтингу медиа (Korea Media Rating Board, KMRB) и Корейской комиссией по коммуникационным стандартам (Korea Communications Standards Commission, KCSC).

В 2008 г., незадолго до президентских выборов, в Южной Корее был введен в действие скандально известный среди интернет-общественности закон о системе действительных имен в интернете (Internet Real-Name System), который требовал, чтобы все крупные интернет-порталы проверяли личность своих пользователей. Это относилось ко всем пользователям, которые выкладывали контент в открытый доступ. Например, чтобы добавить комментарий к новостной статье, требовались регистрация и указание идентификационного номера гражданина. Иностранцы, которые не имели такого номера, должны были отправлять по факсу копию паспорта. Хотя этот закон изначально встретился с протестами общественности, большинство крупных порта-

лов, в том числе Daum, Naver, Nate и Yahoo Korea, осуществляли такие проверки[115]. YouTube отказался подчиниться закону, предпочтя отключить функцию комментирования на корейском сайте. Закон был принят в целях борьбы с киберпреступностью, а также чтобы уменьшить количество клеветы и оскорбительных комментариев в южнокорейском интернете. Согласно статистике, количество издевательств и угроз составляло 13,9% от общего числа сообщений, написанных гражданами Южной Кореи. Новый закон предписывал системным администраторам раскрывать данные пользователей, публиковавших комментарии с угрозами или раскрывающие тайну личной жизни других участников дискуссии.

В течение пяти лет южнокорейские пользователи интернета не могли анонимно оставлять комментарии на местных сайтах. Однако сделать интернет-пространство более дружелюбным властям так и не удалось. Южнокорейские интернет-пользователи, чтобы сохранить свою анонимность, просто перешли на зарубежные веб-ресурсы, популярность же отечественных сайтов значительно упала. При этом количество оскорбительных комментариев уменьшилось лишь на 0,9%. Конституционный суд Южной Кореи 24 августа 2012 г. отменил закон о раскрытии данных, по мнению других стран, нарушающий свободу слова в стране, гарантированную конституцией. Согласно судебному постановлению, отмененный закон препятствовал формированию плюрализма, который является основой демократии. Главная интернет-ассоциация Южной Кореи горячо поддержала решение конституционного суда.

Свобода критики правительства ограничена для корейцев там, где она «ставит под угрозу национальную безопасность» или является «киберклеветой». Так, в 2010 г. канцелярия премьер-министра установила наблюдение

[115] Kim Hyung-eun Do new Internet regulations curb free speech? // http://goo.gl/j4kxw.

за гражданским лицом, высмеивавшим президента Ли Мен Бака[116]. В 2012 г. был заблокирован аккаунт в Twitter, на котором была критика в адрес военно-морского флота, а судья, выступивший против интернет-цензуры, был уволен.

В 2010 г. южнокорейское правительство продемонстрировало свою решительность в борьбе с интернет-пропагандой КНДР[117]. Все началось с того, что КНДР с июля того же года стала размещать в YouTube десятки видеоклипов, а также создала официальный ресурс в Twitter. Большинство материалов имели пропагандистскую направленность. Вопреки ожиданиям, северокорейские видеоклипы и микроблоги стали рекордными по посещаемости и комментируемости. В ответ власти в Сеуле попытались блокировать доступ к этому контенту со своей территории и дали гражданам категорический совет его избегать. Параллельно Сеул стал блокировать и иные сайты КНДР. Блокировка продолжилась в 2011 г. Сообщалось об аресте местного блогера, который похвалил Северную Корею в Twitter, а также о взломе северокорейских аккаунтов в Twitter и YouTube, ответственность за который взяла на себя интернет-группа DC Inside[118].

3.2. Информационное общество и право на доступ к информации. Нормативно-правовое регулирование в России

В 1993 г. в России, через два года после смены политического режима и государственной власти, была принята Конституция Российской Федерации, которая является высшим нормативно-правовым актом страны. В Конституции

[116] Korea Policing the Net. Twist? It's South Korea // http://goo.gl/5TxFP

[117] Южная Корея испугалась популярности КНДР в интернете // http://goo.gl/BZCy5

[118] Корея запретила своим гражданам посещать северокорейский домен // http://goo.gl/3RmHY

России закреплены все основные права человека, которые должны обеспечиваться человеку в демократическом обществе. После вступления России в ОБСЕ (1992), Совет Европы (1996) и ратификации ключевых европейских конвенций и других международных правовых актов возникли новые международные обязательства по обеспечению прав человека.

Важно отметить, что хотя Конституция и имеет высшую юридическую силу на территории России, в ней говорится, что при появлении разногласия между нормами международного договора и законами, принятыми в России, действуют правила международного договора. При этом не соответствующие Конституции РФ международные договоры Российской Федерации не подлежат введению в действие и применению (ч. 6 ст. 125). В силу этого конституционные нормы следует рассматривать в контексте международных обязательств России.

Конституция РФ сформулирована таким образом, чтобы полностью отвечать всем международным соглашениям, которые подписала и ратифицировала Россия. Основные права человека, в том числе свобода мысли, слова и свобода информации, присутствуют во многих международных соглашениях. Эти документы создают международное понимание сути прав человека, которые приобретают особенную значимость именно в своей совокупности в условиях трансграничности интернета и необходимости обеспечения аналогичных прав и свобод в интернет-пространстве.

Таким образом, возникает ситуация, когда для понимания прав пользователей интернета недостаточно рассмотреть какое-то одно соглашение, ратифицированное Российской Федераций, — необходимо анализировать совокупность международных документов и проверять принимаемые в государстве законы на соответствие положениям фундаментальным правам и свободам человека, а также их интерпретации в информационной среде.

Основания для ограничения прав и свобод пользователей интернета в России

Наиболее остро в связи с развитием интернета возникает вопрос об обеспечении права пользователей интернета на свободу выражения мнения, поиска, распространения информации (ст. 19 ВДПЧ и ст. 29 Конституции России). Это право может ограничиваться на основании п. 2 ст. 10 Европейской конвенции по правам человека о свободе выражения мнения и свободе информации (ЕКПЧ) и представляет собой норму об ограничениях права на свободу выражения мнения, которая касается регулирования интернета:

> Осуществление свободы выражения мнения, налагающее обязанности и ответственность, может быть сопряжено с определенными формальностями, условиями, ограничениями или санкциями, которые предусмотрены законом и необходимы в демократическом обществе в интересах национальной безопасности, территориальной целостности или общественного порядка, в целях предотвращения беспорядков и преступлений, для охраны здоровья и нравственности, защиты репутации или прав других лиц, предотвращения разглашения информации, полученной конфиденциально, или обеспечения авторитета и беспристрастности правосудия.

Данная оговорка толкуется как трехсоставный критерий, согласно которому любые ограничения в странах Совета Европы (в том числе и в России) должны:

— предусматриваться законом;

— преследовать одну из указанных целей;

— быть необходимыми в демократическом обществе.

В своей работе «Международные стандарты и зарубежная практика регулирования журналистики»[119] профессор Ю. Г. Рихтер раскрывает суть данного критерия: «Европейский суд по правам человека (ЕСПЧ) заявил, что первое из трех условий будет исполнено, только если соответствующий закон является общедоступным и „сформулирован с

[119] Рихтер А.Г. Международные стандарты и зарубежная практика регулирования журналистики: Учеб. пособие. М., 2011.

точностью, достаточной для того, чтобы позволить гражданину регулировать свое поведение“».

Второй критерий касается того, что вмешательство должно осуществляться ради одной из целей, перечисленных в п. 2 ст. 10; этот перечень является исчерпывающим, тем самым любое вмешательство, которое не направлено на достижение одной из этих целей, нарушает статью конвенции.

Третье условие: в демократическом обществе вмешательство должно быть необходимым. Слово «необходимо» означает, что вмешательство должно быть продиктовано «настоятельной общественной потребностью». Причины, приводимые государством для оправдания вмешательства, должны быть «релевантными и достаточными». Кроме того, в случае спора в ЕСПЧ государство должно продемонстрировать, что вмешательство является «соразмерным преследуемой цели»[120].

Из решений ЕСПЧ следует, что необходимость в интересах демократии определяется следующими двумя принципами:

— ограничение свободы должно быть направленным и соразмерным необходимости удовлетворения законной цели;

— для применения ограничения как «необходимого» недостаточно только его связи с перечнем причин для возможных ограничений, указанных в п. 2 ст. 10.

Таким образом, для того чтобы понять, насколько закон, принятый в государстве, отвечает требованиям международных стандартов, необходимо ответить на следующие вопросы.

1. Сформулирован ли закон с точностью, достаточной для того, чтобы позволить гражданину регулировать свое поведение?

2. Является ли ограничение принятым в интересах национальной безопасности, территориальной целостности или общественного порядка, в целях предотвращения

---

[120] Там же.

беспорядков и преступлений, для охраны здоровья и нравственности, защиты репутации или прав других лиц, предотвращения разглашения информации, полученной конфиденциально, или обеспечения авторитета и беспристрастности правосудия?

3. Существует ли настоятельная общественная потребность для такого ограничения?

Рассмотрим в общем, удовлетворяет ли российское законодательство указанным критериям.

Регулирование интернета в России

В настоящее время в России практика признания информации запрещенной к распространению регламентируется рядом федеральных законов. Причем в последние годы появляются законы, вводящие более серьезные ограничения на распространение информации в интернете, чем на телевидении, радио, в газетах и пр.

Основным нормативным правовым актом, регулирующим отношения в информационной сфере, является Федеральный закон от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и защите информации». Этот акт включает основные понятия, такие как «информация», «доступ к информации», «электронный документ», «распространение информации», «доменное имя», и т. д., закрепляет общие принципы правового регулирования, а также определяет порядок блокирования доступа.

Важно отметить, что в ст. 3 закона «Об информации…» формулируется общий принцип свободы поиска, получения, передачи, производства и распространения информации любым законным способом. Любое ограничение доступа к информации при этом возможно лишь на основании федерального закона и только в правомерных целях защиты основ конституционного строя, нравственности, здоровья, прав и законных интересов других лиц, обеспечения обороны страны и безопасности государства.

Принятая в июле 2012 г. и вступившая в силу в ноябре 2012 г. ст. 15.1 закона «Об информации, информационных

технологиях и защите информации» (№149-ФЗ) и ст. 46 закона «О связи» (№126-ФЗ) стали наиболее громкими законодательными инициативами в сфере регулирования интернета в России. Указанные поправки были введены федеральным законом №139-ФЗ от 28 июля 2012 г. «О внесении изменений в федеральный закон „О защите детей от информации, причиняющей вред их здоровью и развитию“ и отдельные законодательные акты Российской Федерации по вопросу ограничения доступа к противоправной информации в сети интернет».

Суть нового закона заключается в создании Единого реестра доменных имен, указателей страниц сайтов в Сети и сетевых адресов, позволяющих идентифицировать сайты, содержащие информацию, распространение которой в Российской Федерации запрещено.

Реестр ведет государственный орган (в настоящее время Роскомнадзор) или уполномоченная организация, которые на основании заключений, выданных специалистами ФСКН, Роспотребнадзора или Роскомнадзора (данные функции возложены на ведомства на основании постановления правительства № 1101) принимают решение о включении в реестр отдельных страниц, сайтов или IP-адресов.

В реестр попадают сайты, которые содержат категории запрещенной информации, попасть в реестр они могут на следующих основаниях:

— информация признана запрещенной решением органа исполнительной власти, уполномоченного правительством;

— информация признана запрещенной на основании судебного решения.

К первой категории относится детская порнография, информация о способах изготовления и употребления наркотиков и информация о способах совершения самоубийства, а также призывы к совершению самоубийства. Ко второй — любая информация, признанная судом запрещенной, в том числе экстремистские материалы.

Данный закон прошел три чтения и был подписан президентом в течение полутора месяцев. Основными лейтмотивами критики инициативы экспертами были следующие:

— отсутствие публичного обсуждения текста инициативы;

— отсутствие в законе механизмов общественного контроля за решениями уполномоченных органов;

— слишком широкий перечень информации, подлежащей блокированию или удалению;

— нарушение связности интернета в перспективе;

— имплицитное нарушение ст. 29 Конституции Российской Федерации и ст. 3 №149-ФЗ, связанное с возможной блокировкой законной информации при блокировке по сетевым адресам, на которых может находиться более одного ресурса.

Критика законопроекта

В течение всего времени, пока законопроект рассматривался Государственной думой, и после его принятия в СМИ появлялись многочисленные критические публикации и комментарии как представителей интернет-отрасли, так и правозащитников и юристов.

Российская ассоциация электронных коммуникаций (РАЭК) предложила целый ряд поправок в законопроект, отметив, что «слишком широкий класс материалов, подлежащих внесению в Реестр на основании решения уполномоченного правительством Российской Федерации федерального органа исполнительной власти, может привести к злоупотреблениям и саботированию исполнения норм закона. Экспертные оценки, которые будут лежать в основе определения, является ли материал „побуждающим к совершению действий, представляющих угрозу их жизни и (или) здоровью, в том числе к причинению вреда своему здоровью, самоубийству“ не вызывают доверия и должны быть обоснованы в судебном порядке»[121].

[121] Поправки РАЭК к законопроекту №89417-6 // http://goo.gl/TMPj4

В официальном блоге Google было опубликовано сообщение о том, что «негативные последствия от применения закона превысят ожидаемый положительный эффект, поставив под угрозу доступ пользователей к легальным ресурсам»[122].

Живой Журнал заявил, что «поправки в закон могут привести к введению цензуры в русскоязычном сегменте интернета, созданию черного списка и стоп-листов и блокировке отдельных сайтов. К сожалению, практика применения законодательства в России говорит о высокой вероятности именно этого, худшего сценария»[123].

Яндекс: «Предложенные методы дают почву для возможных злоупотреблений и вызывают многочисленные вопросы со стороны пользователей и представителей интернет-компаний»[124].

Накануне принятия законопроекта, 10 июля 2012 г., русскоязычная Википедия на один день прекратила работу в знак протеста против введения цензуры[125]. В специальном пресс-релизе заявлялось: «Лоббисты и активисты, поддерживающие данные поправки, утверждают, что они направлены исключительно против контента наподобие детской порнографии „и тому подобных вещей“, но следование положениям и формулировкам, вынесенным на обсуждение, повлечет создание в России аналога „великого китайского файервола“». Акция была поддержана Яндексом, Живым Журналом, Луркоморьем, ВКонтакте и другими сервисами и порталами.

Законопроект критиковала и представитель ОБСЕ по вопросам свободы СМИ Дунья Миятович: «…любая попытка запретить нечетко определенные типы контента в интернете при отсутствии прозрачной процедуры, скорее

---

[122] Новый закон угрожает свободному интернету // http://goo.gl/JRQDv

[123] Живой Журнал за свободу информации // http://goo.gl/UodzH

[124] О законопроекте №89417-6 http://goo.gl/yokKH

[125] http://goo.gl/mtNVw

всего, приведет к чрезмерному блокированию контента, а возможно, и к цензуре, что в результате будет препятствовать свободному информационному потоку»[126].

Спустя несколько месяцев вступления закона в силу на дефекты регулирования обратил внимание уполномоченный по правам человека в Российской Федерации Владимир Лукин. Он отметил в своем ежегодном докладе, что «понимая и разделяя мотивы, побудившие законодателей разработать перечисленные законы» полагал бы все же «необходимым в наступившем году осуществить мониторинг их применения на предмет выявления возможных пробелов и недочетов, в том числе обусловленных их необъяснимо быстрым принятием»[127].

С точки зрения прав пользователей интернета, опасения вызывает прежде всего нечеткость критериев и отсутствие предусмотренных законодателем механизмов общественного контроля.

Включение в Реестр означает, что все провайдеры обязаны блокировать доступ к данной информации для своих абонентов. Таким образом, у владельца сайта есть выбор: удалить информацию, в отношении которой экспертом по непубличным основаниям принято решение о запрещении, или обжаловать блокировку в суде. С учетом скорости работы российских судов процесс может занять не один год, в течение которого сайт будет блокирован.

При этом перечень заблокированных ресурсов является закрытым, но можно проверить на официальном сайте www.zapret-info.gov.ru, не находится ли в Реестре конкретный адрес, сайт или страница.

Проблемой является также способ осуществления блокировки. Из-за одной страницы, содержащей запрещенную информацию, может оказаться заблокирован не только целый сайт, но даже IP-адрес, на котором могут располагаться

---

[126] http://www.osce.org/ru/fom/92029

[127] Доклад уполномоченного по правам человека в Российской Федерации за 2012 год // Российская газета. Федеральный выпуск. №6044. 29.03.2013 // http://goo.gl/RKW02

сотни или даже тысячи ресурсов, не содержащих запрещенной государством информации.

Согласно данному закону, провайдер вынужден сначала исполнить заведомо незаконное решение о блокировке по сетевому адресу и только после этого может его обжаловать. При этом весь период обжалования предполагается, что все ресурсы, которые оказались на одном сетевом адресе с тем, где была найдена информация, признанная запрещенной, весь период судебных разбирательств будут оставаться заблокированными. В подавляющем большинстве случаев провайдеры, бизнес которых зависит от лицензионных условий, выполняют решения о блокировках сетевых адресов и не заботятся об обеспечении прав пользователей интернета, справедливо полагая, что это обязанность скорее не их, но государства и самих пользователей.

Если анализировать данный закон с точки зрения «трехсоставного критерия», то как минимум на один вопрос ответ отрицательный (вопрос относительно защиты нравственности сугубо схоластический; настоятельная общественная необходимость всегда может быть искусственно создана посредством подконтрольных государству СМИ и некорректных срезов общественного мнения). Вызывает сомнение, что закон сформулирован с точностью, достаточной для того, чтобы гражданин самостоятельно регулировал свое поведение: постоянные отказы удалять информацию со стороны пользователей интернета, а также споры относительно критериев отнесения информации к запрещенной прямо указывают на то, что интернет-пользователи не поддерживают и не понимают, какая информация и почему должна быть запрещена, отмечают излишнюю широту предписанных к запрету категорий.

Дополнения к статье 15.1 №149-ФЗ

К настоящему времени[128] президентом России подписан закон о дополнении перечня информации, блокирующейся,

[128] Апрель 2013 года.

на основании решения уполномоченного органа, информацией о несовершеннолетнем, пострадавшем в результате противоправных действий (бездействия), распространение которой запрещено федеральными законами[129]. Законопроект также подвергается критике интернет-индустрии и общества, в частности, Российская ассоциация электронных коммуникаций отмечает:

«Принимая во внимание, что статья 15.1

— вызывает как существенное и обоснованное недовольство как интернет-индустрии (1% ВВП), так и интернет-пользователей (50% населения Российской Федерации);

— причиняет ущерб глобальной связности интернета;

— противоречит Конституции Российской Федерации и ст. 3 п. 1 того же закона;

— находится в стадии активного обсуждения, уточнения подзаконных актов и формирования правоприменения;

— предложенная новая категория информации, подлежащая удалению, имеет существенное отличие от имеющихся в настоящее время в указанной статье видов запрещенной информации, поскольку непосредственно из содержания данной информации не следует ее незаконность, для признания ее таковой необходима проверка наличия или отсутствия соответствующего согласия или разрешения уполномоченного лица. Такой порядок не соответствует концепции ФЗ „Об информации…“, указанным в ней срокам для принятия решения, и будет нереализуем в рамках принятых в настоящее время подзаконных актов, которые регулируют применение указанной ст. 15.1. ФЗ „Об информации…“, что может повлечь за собой серьезные нарушения прав владельцев соответствующих интернет-ресурсов;

а также учитывая обозначенные выше недостатки законопроекта, считаем дополнение излишним и опасным для развития интернета в Российской Федерации»[130].

---

[129] http://goo.gl/hAnEe

[130] http://raec.ru/times/detail/2415/, дата обращения 12.04.2013

Инициативы по расширению оснований для блокировки ресурсов в интернете

В настоящее время представители правообладателей (в основном американских) совместно с Министерством культуры РФ предлагают дополнить ст. №149-ФЗ «Об информации…» новой ст. 15.2, где будет описываться порядок уведомлений владельцев сайтов, провайдеров хостинга и операторов связи по схеме, аналогичной описанной в ст. 15.1 и предполагающей создание реестра авторских прав.

Проект закона «О внесении изменений в отдельные законодательные акты Российской Федерации в целях профилактики и пресечения нарушений интеллектуальных прав в информационно-телекоммуникационных сетях, в том числе в Сети интернет»[131] предполагает следующие изменения законодательства.

Закон об информации:

— ст. 1, ч. 2: Расширение сферы действия положений Федерального закона «Об информации, информационных технологиях и защите информации» на отношения, возникающие при правовой охране РИД в случаях, предусмотренных федеральным законом «Об информации, информационных технологиях и защите информации»;

— ст. 15.2: Перечень мер для прекращения нарушения интеллектуальных прав, а также порядок их осуществления провайдерами хостинга и владельцами сайтов в интернете;

— обязанность провайдеров хостинга и владельцев сайтов предоставлять персональные данные клиентов для осуществления судебного преследования;

— обеспечительные меры в отношении информационных посредников и владельцев сайтов — блокирование доступа.

КоАП:

— расширение предметной области на размещение объектов авторского права без извлечения дохода;

[131] http://mkrf.ru/dokumenty/3974/detail.php?ID=272242

— увеличение административной ответственности информационного посредника вплоть до конфискации и приостановления деятельности.

Очевидно, что данная инициатива как минимум нарушает право на справедливый суд, а также может привести к ограничению прав пользователей на развитие, доступ к знаниям и культурным ценностям.

Закон «О противодействии экстремистской деятельности»

В 2012 г. одним из самых распространенных оснований для блокирования ресурсов стал федеральный закон «О противодействии экстремистской деятельности». Ст. 12 указанного закона запрещает использование сетей связи общего пользования для осуществления экстремистской деятельности. При этом под экстремистской деятельностью понимается множество различных действий, так или иначе связанных с распространением информации: публичное оправдание терроризма и иная террористическая деятельность; возбуждение социальной, расовой, национальной или религиозной розни; пропаганда исключительности, превосходства либо неполноценности человека по признаку его социальной, расовой, национальной, религиозной или языковой принадлежности или отношения к религии; распространение экстремистских материалов; пропаганда нацистской и сходной с ней символики и пр. У прокуратуры и Роскомнадзора на основании указанной статьи имеется два основания требовать блокирования доступа к интернет-ресурсам: (1) распространение материалов, включенных в федеральный список экстремистских материалов, который составляет Министерство юстиции; (2) публикация материалов, которые ведомства сочтут возбуждающими социальную рознь или оправдывающими терроризм.

Положения антиэкстремистского законодательства также подвергаются критике за неконкретность и расплывчатость формулировок, допускающих произвольное толкование и применение, указывается на субъективность и оце-

ночность критериев отнесения информации к «возбуждающей социальную рознь».

Законы «О полиции» и «О прокуратуре»

Возможности для вынесения представлений о блокировке или удалении информации в Сети содержатся, кроме того, в ст. 13 закона «О полиции»: «Полиции для выполнения возложенных на нее обязанностей предоставляются следующие права: …вносить в соответствии с федеральным законом руководителям и должностным лицам организаций обязательные для исполнения представления об устранении причин и условий, способствующих реализации угроз безопасности граждан и общественной безопасности, совершению преступлений и административных правонарушений» (федеральный закон «О полиции» от 07.02.2011 № 3-ФЗ).

В рамках уголовного судопроизводства порядок внесения таких представлений установлен в 2001 г. федеральным законом — ст. 158, ч. 2 Уголовно-процессуального кодекса Российской Федерации.

Аналогичные указанным в законе «О полиции» полномочия имеются также у прокуроров согласно закону «О прокуратуре Российской Федерации» (№ 2202-ФЗ от 17.01.1992).

Согласно этим полномочиям, силовые структуры могут требовать от провайдеров хостинга или операторов связи блокировки определенного контента в интернете, признав его «причиной или условием» совершения правонарушения.

Таким образом, и эти полномочия, закрепленные за силовыми структурами, при полагании благородной цели не позволяют пользователю интернета сделать вывод о том, является ли его поведение правильным с точки зрения закона. А следовательно, можно утверждать, что закон сформулирован с недостаточной точностью, для того чтобы позволить гражданину регулировать свое поведение.

Открытость информации о деятельности государственных органов и право на доступ к информации об их деятельности

Принятое в России законодательство, регламентирующее порядок осуществления права граждан на доступ к публичной информации, в том числе в электронной форме, фактически создает реальную возможность распространения общественно значимой информации.

Официально российским руководством определена значимость правового обеспечения доступа граждан к информации. В стратегии развития информационного общества в Российской Федерации (утверждена президентом РФ 7 февраля 2008 г.), помимо других положений, органами власти предполагается обеспечить населению доступность информации и технологий, а также улучшить систему государственных гарантий конституционных прав человека и гражданина в информационной сфере. Эти концептуальные положения в дальнейшем были закреплены в ряде российских федеральных законов 2006–2010 гг.: «Об информации, информационных технологиях и защите информации», «Об обеспечении доступа к информации о деятельности судов в Российской Федерации», «О персональных данных», «Об организации предоставления государственных и муниципальных услуг».

В законе об информации одним из краеугольных принципов информационных отношений провозглашается принцип открытости и доступности информации, а одним из главных направлений государственной информационной политики — обеспечение открытости и прозрачности деятельности субъектов властных полномочий. Кроме того, в этом же законе дается и определение информации согласно порядку доступа к ней (конфиденциальная, тайная и служебная). Базовым же нормативным правовым актом является федеральный закон «Об обеспечении доступа к информации о деятельности органов государственной власти и местного самоуправления» (2009)[132].

[132] Федеральный закон №8-ФЗ от 9 февраля 2009 г. «Об обеспечении доступа к информации о деятельности органов государственной власти

В законе делается указание на то, что субъектами отношений, регулируемых законом, являются, в том числе, и органы публичной власти, осуществляющие поиск информации о деятельности других органов власти. Однако в других странах органы власти не считаются субъектами таких отношений с учетом специального правового статуса органов публичной власти.

В то же время терминологические сравнения явственно свидетельствуют о необходимости четкого закрепления основных понятий, связанных с регулированием доступа к информации и обращением различных видов публичной информации. В законе такие сроки закреплены в отдельной статье, где, кроме того, дается определение понятий в сфере электронного документооборота.

Российское законодательство об информационных ресурсах закрепляет правовые процедуры, которые позволяют гражданам обращаться в органы власти для получения публичной информации (информации о деятельности органов власти). Установлены сроки, в течение которых орган власти обязан дать письменный ответ на запрос по поводу получения информации, определение порядка использования электронных средств связи, содержание заявления о предоставлении информации из органа власти.

Например, согласно закону, запрос подлежит рассмотрению в 30-дневный срок со дня его регистрации, если иное не предусмотрено законодательством Российской Федерации. В случае же, если предоставление запрашиваемой информации в указанный срок невозможно, то в течение семи дней со дня регистрации запроса пользователю информации сообщается об отсрочке ответа на запрос с указанием ее причины и срока предоставления запрашиваемой информации, который не может превышать пятнадцати рабочих дней.

и местного самоуправления» // Собрание законодательства РФ. 2009. №7. Ст. 776.

Однако в законе не урегулированы на достаточном уровне процедуры парламентского, общественного и государственного контроля за соблюдением порядка законного предоставления гражданам публичной информации и ответственность должностных лиц за ее несвоевременное предоставление. Необходимо детально закрепить и виды нарушений законодательства о доступе к публичной информации, за которые предусматривается ответственность.

Рассмотренные российские законы в целом можно оценить как недостаточно четко сформулированные и в ряде случаев не позволяющие пользователю однозначно сделать вывод о том, является ли размещенная или распространяемая информация запрещенной законом. Недостаточно четкие формулировки не поддерживаются активными интернет-пользователями, что приводит к провокациям по отношению в исполнительной власти, обязанностью которой является исполнение закона в принятых законодательной властью формулировках. Оправданием законодателя, безусловно, служит тот факт что законодательство, касающееся регулирования сети интернет, находится в активной фазе развития и будет приведено в соответствие с имеющимися международными обязательствами и Конституцией Российской Федерации.

3.3. Соотношение форм и моделей государственного устройства и основных способов регулирования правоотношений в информационной среде

Государственные режимы регулирования Сети в рамках национальных юрисдикций различаются весьма существенно как по количественным, так и по различным качественным характеристикам. Считаем целесообразным выделить несколько классификаций государственных режимов по различным основаниям.

Во-первых, в целях анализа представляется целесообразным разделить государства дихотомически: государ-

ства, заинтересованные в развитии информационных технологий в публичной сфере, и государства, не заинтересованные в этом. Иными словами, существуют государства, в которых существует открытый и публичный доступ в интернет (подавляющее большинство), и государства, в которых такого доступа нет (явное меньшинство). К последним можно отнести некоторые государства из списка так называемых «врагов интернета», составленного и редактируемого организацией «Репортеры без границ». Это такие страны, как КНДР, Туркменистан, Куба, Мьянма и Йемен. Эти государства представляют собой вырожденный тип. Эти страны, кроме Мьянмы, в той или иной степени объединяет коммунистическое прошлое, однопартийная система и наличие аппарата цензуры. В Мьянме у власти находится военная хунта, в Йемене существует странная политическая система, совмещающая авторитарную центральную власть в столице и племенную демократию в провинциях.

В Мьянме Йемене количество граждан, имеющих свободный доступ к интернету на относительно постоянной основе, не превышает 1% от общего количества населения. Однако следует отметить, что сама по себе доля граждан, имеющих подобный доступ, не является достаточным критерием включения страны в рассматриваемую категорию. Гораздо важнее не абсолютное и даже не относительное количество пользователей Глобальной сети от общего количества населения (что существенно зависит от экономического развития, географии и плотности населения и образа жизни — оседлый/кочевой), а сама готовность и желание властей предоставлять населению доступ к интернету и развивать эту отрасль.

Классификация подходов по фактической степени богатств регулятивного инструментария

Рассмотрим режимы ограничения доступа к интернету, характерные для вырожденного типа. Эти режимы могут

применяться в комплексе, как в КНДР и на Кубе, так и по отдельности (Мьянма, Туркменистан и прочие «враги интернета»).

1. Политика экономического удушения доступа к интернету с помощью заградительных тарифов

В Северной Корее существуют интернет-кафе для иностранцев, которые в принципе могут посещать и граждане страны, однако тариф в $10 за час является грабительским не только для иностранцев, но и составляет месячную зарплату большинства жителей страны. В Туркменистане во времена правления президента С. Ниязова интернет был фактически запрещен, хотя об издании ни одной юридической нормы не известно. В настоящее время в стране появилось чуть более десяти интернет-кафе и возможность подключения к Сети по модему и выделенной линии. В настоящее время стоимость модемного подключения на домашний интернет типа ADSL с минимальной скоростью 256 кбит/с составляет 459,6 туркменских манат в месяц[133]. Если эту сумму перевести в рубли, то она составит более 4500 рублей в месяц. Учитывая, что средняя зарплата в Туркменистане ниже, чем в России, о доступности этого вида связи говорить не приходится. Подключение на скорости 34 Мбит/с по выделенной линии обойдется в космическую сумму в 96 023 манат, т. е. более миллиону рублей в месяц[134]. На Кубе средняя цена за один час доступа к интернету составляет от $5 до $8[135]. С учетом средней зарплаты кубинца $20 в месяц пользование Глобальной сетью для подавляющего большинства граждан просто разорительно.

---

[133] http://online.tm/adslconnect

[134] http://online.tm/vydelennaya-liniya

[135] https://opennet.net/research/profiles/cuba

2. Политика ограничения скорости и прочие искусственно создаваемые технические препятствия, превращающие сеанс доступа в интернет в издевательство

В рамках этой политики любая попытка воспользоваться интернетом должна восприниматься пользователями как крайне ненадежное предприятие, как издевательство: модемные соединения постоянно рвутся, скорость резко падает почти до нуля, загрузка файлов прерывается на 99%, сайты с java-приложениями отказываются загружаться, функции поиска и навигации затруднены.

Иногда подобные меры признаются открыто, однако обосновываются как меры по разумному использованию ресурсов Сети. В качестве примера можно привести Йемен. В правилах и условиях провайдера ТелеЙемен сказано следующее: «Доступ к приложениям, которые передают или получают видео или аудио в реальном масштабе времени, или другие запросы, существенно сказывающиеся на пропускной способности Сети, рассматриваются в качестве неразумных и не допускаются»[136].

3. Политика введения разрешительно-надзорной системы, удостоверяющей право граждан на доступ к интернету и контролирующей способ его использования

В рамках этой политики гражданин должен обосновать свою необходимость пользования ресурсами Глобальной сети в случае желания подключить домашний интернет; регистрировать каждый сеанс в интернет-кафе, получить разрешение на право завести блог и заниматься любой формой публицистической деятельности. В рамках этой политики интернет трактуется исключительно как ресурс для служебных целей (научно-образовательный или справочный).

---

[136] Terms and conditions for Y.Net Service // http://goo.gl/UH6PV

Подобная система существует на Кубе. В этой стране декларируется, что доступ в интернет является «фундаментальным правом» кубинцев[137], однако с момента появления в 1996 г. интернета в стране декрет 209 устанавливает процедуру аккредитации для использования интернета[138]. Фактически использование интернета было запрещено до 2000 г. С 2000 г. доступ в Глобальную сеть осуществляется при условии государственной авторизации. Владение частным компьютером, принтером или сотовым телефоном на Кубе вплоть до 2007 г. возможно было только с официального разрешения властей. Установка беспроводной сети Wi-Fi до сих пор требует такого разрешения. Вследствие слабой пропускной способности каналов связи, власти страны дают преимущество доступа к интернету на публичной основе: на рабочих местах, в школах, НИИ и библиотеках.

В Мьянме подавляющее большинство пользователей пользуется интернетом в общественных центрах доступа (ОЦД) со стоимостью от $0,3 до $0,5 за час. Операторы ОЦД обязаны регистрировать паспортные данные пользователей, более того, компьютеры пользователей настроены таким образом, что они делают скриншот каждые 5 минут работы и отсылают его в государственную корпорацию развития информационных технологий. Кроме того, администрация интернет-кафе и ОЦД обязаны размещать компьютеры таким образом, чтобы было видно содержимое экранов и принять меры, чтобы пользователи имели возможность пользоваться только государственными почтовыми сервисами. Доступ к политическим сайтам категорически запрещен[139].

---

[137] Patrick Symmes. Che is dead. Wired // http://goo.gl/GCS3W

[138] Reporters Without Borders. Going online in Cuba: Internet under surveillance // http://goo.gl/wHtWl

[139] OpenNet Initiative Blog. Burmese Regulations for Cybercafés Stringent as Expected. 2008. July // http://goo.gl/94ftb

4. Политика сегрегации интернета и национального интернета

В рамках этой политики создается внутренняя национальная компьютерная сеть преимущественно академического характера с ограниченным набором фиксированных функций и информационных ресурсов, жестко контролируемых государственными контент-провайдерами (НИИ, университетами, библиотеками, ведомствами). Подобная сеть призвана компенсировать недостаток доступа к Глобальной сети занятых интеллектуальным трудом граждан страны. Доступ к такой сети может быть либо бесплатным (служебным), либо существенно более дешевым, чем доступ к интернету.

Подобная политика проводится на Кубе и в КНДР. На Кубе интернет состоит из почтового сервиса, так называемой «Кубинской энциклопедии» и сайтов на государственном содержании. Доступ к этому ресурсу стоит $1,5, т.е. как минимум в 4 раза дешевле, чем к интернету[140]. Подобная сеть, известная как «Квангмьенг»[141], создана в КНДР. Есть сведения, что Иран и Мьямна также намерены создать аналогичные национальные сети, существующие практически автономно от Глобальной сети[142].

Для всех перечисленных режимов, за исключением четвертой позиции, ограничения свободного доступа граждан к интернету, очевидно, можно рассматривать как нарушение основных гражданских прав и прав человека.

Классификация подходов по типу регулирования и степени жесткости регулирования

Страны, заинтересованные в свободном доступе граждан к интернету, предпочитают регулировать использование

[140] https://opennet.net/research/profiles/cuba

[141] Lintner B. North Korea's IT revolution // Asia Times 2007.

[142] Rhoads Ch., Fassihi F. Iran Vows to Unplug Internet // Wall Street Journal. 2011. May 28.

интернета с помощью механизмов фильтрации контента. Важно иметь в виду, что «враги интернета», помимо мер по ограничению доступа к интернету вообще, непременно вводят режим фильтрации контента. Однако вследствие крайне низких скоростей и небольшого количества пользователей в таких странах нет необходимости в обширной фильтрации, поскольку почти все мультимедиаресурсы оказываются недоступными. Таким образом, государственные способы регулирования правоотношений в информационной среде можно классифицировать по критерию характера фильтрации.

Табл. 3. Типы фильтрации контента в интернете

Тип	**Описание**	**Государства**
Тотальная фильтрация	Характеризуется глубиной (режим блокировки, при котором блокируются большие порции целевого контента в данной категории) и широтой (режим блокировки включает фильтрацию множества категорий в данное время)	Иран, Китай
Существенная фильтрация	Фильтрация которая характеризуется глубиной или широтой: несколько категорий фильтруются на среднем уровне или множество категорий фильтруется слабым образом	Саудовская Аравия, ОАЭ, Южная Корея, Йемен, Мьянма, Вьетнам, Пакистан, Оман, Узбекистан, Сирия, Тунис, Бахрейн
Постоянная выборочная фильтрация	Фильтры блокируют небольшое количество специфических сайтов в единственной категории или всего нескольких категориях	Многие страны СНГ (Белоруссия, Азербайджан, Казахстан, Таджикистан), Индия, Сингапур, Германия, Франция. Австралия, Малайзия

Гибкая тактическая фильтрация	Существует набор заготовленных планов обеспечения информационной безопасности, включающих шаблоны фильтрации, которые активируются исходя из конкретной военной и политической обстановки. Профили могут быстро модифицироваться и настраиваться на конкретный контент	Россия
Отсутствие фильтрации, саморегулирование	Отсутствие режимов фильтрации на государственном уровне или на уровне провайдера. Поощрение саморегуляции на уровне конечного пользователя	США, Великобритания, Дания, Финляндия, Венесуэла

Так же следует обратить внимание на критерий степени прозрачности правил фильтрации контента. Предлагается следующая классификация:

Табл. 4. Степень прозрачности правил фильтрации контента

Тип	**Описание**	**Государства**
Криптофильтрационый режим глубокой фильтрации. (Факты фильтрации определенных категорий контента скрываются от своих граждан и не признаются перед международным сообществом с целью сохранения видимости декларируемой свободы слова)	Фильтрация глубокая, законодательная регламентация слабая	Китай, КНДР, Куба, Белоруссия, Туркменистан, Узбекистан, Эфиопия, Бахрейн
Криптофильтрационый режим поверхностной фильтрации	Фильтрация поверхностная, законодательная регламентация слабая	Мьянма Узбекистан, Судан, Йемен

Частично риптофильтрационный режим. (Факт фильтрации признается, но скрываются его детали)	Фильтрация любого уровня, законодательная регламентация средняя	Сирия, Вьетнам, Тунис, Индия, Россия
Режим полностью открытых правил фильтрации	Сильная законодательная регламентация	Саудовская Аравия, Сингапур, Израиль, Германия, Франция

Выявление наиболее существенных факторов, определяющих характер регулирования

Содержательно широта фильтрации определяется количеством категорий. Роберт Фарис (Robert Faris) и Нарт Виллановa (Nart Villeneuve) выделили следующие категории, подверженные фильтрации в мировых масштабах[143]: — свобода выражения и свобода СМИ; политика и оппозиционные партии;

политическая реформа, реформа права; вооруженные группы, экстремисты и сепаратисты; права человека; международные отношения и оборона; права меньшинств и этнические конфликты; права женщин; экология; экономическое положение; исторические события, вызывающие противоречивые интерпретации; искусство и литература, вызывающие конфликты в обществе; риторика ненависти; сексуальное образование и планирование семьи; состояние здравоохранения; гомосексуальный контент; порнография; провокативный контент; знакомства; азартные игры; алкоголь и наркотики; нетрадиционные религиозные верования; религиозная полемика, комментарии и критика; анонимность; хакерство; домены блогов и блог-сервисы; веб-хостинг; IP-телефония (VOIP); бесплатные почтовые сервисы; поисковые машины; переводческие сервисы; обмен мультимедиа; p2p; группы и социальные сети; коммерческие сайты.

[143] Faris R., Villeneuve N. Measuring Global Internet Filtering // Access Denied: The Practice and Policy of Global Internet Filtering (Information Revolution and Global Politics). 2008. P. 8.

Классификация подходов по выбранным объектам регулирования и декларируемым целям регулирования

Перечисленный список категорий достаточно детально отображает ситуацию и касается практически всех видов общественной деятельности. Анализ этих категорий позволяет выделить на их основании следующие классы (сферы) фильтрации.

Табл. 5. Сферы фильтрации контента в интернете

Сферы фильтрации	**Содержание класса**	**Тип политического режима или политической культуры; форма правления**	**Примеры стран, фильтрующие данную сферу**
Политическая	Оппозиционная политическая пропаганда, запрещенные судом или конституцией идеологические учения, права человека, свобода слова, права меньшинств	Особенно характерно для азиатских деспотий, диктатур, военных хунт и абсолютных монархий. Однако встречается и в демократических республиках	Китай, Иран, Саудовская Аравия, Германия, Франция, Россия
Религиозная	Учения сект и конфессий враждебных или считающихся властями враждебными официальной или доминирующей религии или светской идеологии	Характерно для теократических политических режимов и стран с официальной государственной религией. Также имеет место в некоторых странах, запрещающих деструктивные культы или религиозный экстремизм согласно решению судов или актам правительства	Саудовская Аравия, Иран, Ирак, Китай

Социальная	Сексуальный контент (эротика, порнография, сексуальное просвещение), азартные онлайн игры, запрещенные наркотики, вредные для общества течения и массовые увлечения	Встречается практически во всех странах в форме фильтрации детской порнографии. Особенно характерно для стран с сильными религиозными традициями, влиятельными консервативными партиями	Германия, Франция, Южная Корея, Малайзия, Сингапур, Иран, Саудовская Аравия
Конфликтная	Контент, имеющий отношение к вооруженным конфликтам, пограничным спорам, сепаратистским движениям, незаконным вооруженным формированиям и т. п.	Характерно для федеративных республик с нерешенными сепаратистскими конфликтами, стран, находящихся в состоянии перманентных гражданских войн и длительных пограничных конфликтов	Китай, Иран, КНДР, Куба
Авторское право и другие невещные права	Мультимедиа материалы и книги, содержащиеся в открытом доступе с нарушением авторских прав, а также ссылки на такие материалы	Характерно для западных стран с сильным лобби владельцев авторских прав	Франция
Интернет-сервисы и приложения	Почта, хостинг, поиск, перевод, телефонные сервисы VoIP, клиенты p2p, хакерские сайты	Характерно для «врагов интернета», деспотических режимов	КНДР, Куба, Йемен, Мьянма, Франция

Помимо сфер фильтруемого контента существует вариабельность по технологии фильтрации и блокировки.

Табл. 6. Технологии фильтрации и блокировки контента в интернете

Объект блокировки	**Страны, взявшие на вооружение метод**
IP-адрес	Азербайджан, Китай, Индия, Эфиопия, Южная Корея, Россия
DNS	Бахрейн, Индия, Пакистан, Южная Корея, Вьетнам, Россия
Конкретная страница	Азербайджан, Иран, ОАЭ, Саудовская Аравия, Йемен, Вьетнам, Сингапур, Сирия, Южная Корея
Ключевое слово	Китай, Иран

Одним из важных признаков, характеризующих отношение государства к праву доступа в интернет, является признание или непризнание этого права неотъемлемым правом человека. Таких стран, в первую очередь это Финляндия, Греция и Эстония, совсем немного, и все они признали это относительно недавно.

В Финляндии каждый гражданин имеет право доступа к интернету как минимум по мегабитному каналу. В стране к Глобальной сети не подключено всего четыре тысячи домов в труднодоступной местности, однако новый закон обязывает провайдеров проложить линии таким образом, чтобы каждое домохозяйство находилось на расстоянии не далее двух километров от точки широкополосного доступа. Исключение сделано только для двух тысяч домов, которые находятся в крайне труднодоступной местности, интернет этим домам не гарантирован. Правительство уже составило план, по которому к 2015 г. граждане Финляндии по закону могут требовать подключения к Сети со скоростью 100 Мб/с.

Пресс-секретарь министерства Лаура Викконен (Laura Vikkonen) отметила важность расширения доступа к глобальной сети: «Мы полагаем, что без него невозможно жить в современном обществе. Как в банковском обслуживании, воде или электричестве, вы нуждаетесь в Сети. Универсальный сервис — это индивидуальное право каждого гражданина».

Франция, только задекларировала концепцию предоставления гарантированного доступа к веб-ресурсам.

В январе 2013 г. Федеральный суд в Карлсруэ, рассматривая иск гражданина, по техническим причинам лишенного провайдером возможности выходить в интернет, удовлетворил иск. Как заявил представитель суда, «интернет сегодня играет очень важную роль и влияет на частную жизнь каждого, позволяя принимать существенные решения. Поэтому потеря возможности использовать интернет сравнима с потерей возможности использования автомобиля». Кроме того, в интервью «Deutche Welle» министр юстиции ФРГ Сабина Летюссер-Шнаренбергер заявила: «Решение [суда] демонстрирует, насколько фундаментальную роль стал играть интернет для информированной жизни. Использование интернета начинает осознаваться как гражданское право».

Можно сделать вывод, что хотя и существует некоторая зависимость между степенью демократичности политического режима в той или иной стране и свободой доступа к интернету, подобная зависимость не имеет жесткого характера. Единственное, что можно сказать достоверно, так это то, что для деспотических режимов восточного типа ограничение свободы доступа к интернету и цензурный режим органичны. Авторитарные режимы и военные хунты особый акцент делают на фильтрацию политического контента и гражданских конфликтов, непосредственно угрожающих им. В теократиях по понятным соображениям развита фильтрация морального и религиозного контента, но, поскольку религиозный контент в этих странах часто не отличим от политико-идеологического контента, политическая фильтрация также развита. Для демократических стран характерна фильтрация социального контента, однако антифашистское законодательство некоторых стран позволяет говорить и о политической фильтрации. С формой правления и типом политического устройства права доступа к интернету вообще не коррелируют. Как в республиках президентского, так и парламентского типа с равным успехом принимаются законодательные акты по фильтрации социально вредного контента и фильтрации ресурсов, нарушающих права пользователей. На

что следует обратить внимание, так это на то, что в странах с сильной президентской властью легче вводятся технические системы надзора за интернетом.

Основные типы правоотношений по целям и объектам регулирования

Для целей характерологизации правоотношений субъектов и объектов регулирования предлагается следующая теоретическая модель, основанная на соотношении декларируемых целей и истинных целей (объектов) регулирования.

Табл. 7. Типы правоотношений по целям и объектам регулирования

Истинная цель регулирования	**Декларируемая цель регулирования**		
Защита прав (детей, меньшинств, правообладателей и др.)	Защита прав (детей, меньшинств, правообладателей и др.)	Государственный контроль (цензура, свобода слова)	Национальная безопасность (экстремизм, терроризм)
Государственный контроль (цензура, свобода слова)	Открыто демократический	Шизофренически демократический	Параноидально демократический
Национальная безопасность (экстремизм, терроризм)	Закрыто тоталитарный	Открыто тоталитарный	Шизофренически тоталитарный
То же	Закрыто милитаристский	Параноидально милитаристский	Открыто милитаристский

Необходимо отметить, что в государствах могут параллельно развиваться тенденции к различным типам правоотношений, поэтому невозможно говорить о строгом отнесении страны к определенному типу, но лишь о наличии и степени каждого из типов в наличном правовом поле.

ЗАКЛЮЧЕНИЕ

Основные права человека, в том числе свобода мысли, слова и свобода информации, присутствуют во многих международных соглашениях. Эти документы создают международное понимание сути прав человека, которые приобретают особенную значимость именно в своей совокупности в условиях трансграничности интернета и необходимости обеспечения аналогичных прав и свобод в интернет-пространстве.

Некоторые государства ведут дискуссию о том, что свобода интернета явление опасное из-за различного рода «киберугроз», неразберихи с некоторыми понятиями, мешающими применению и подтверждению незыблемости международных соглашений в отношении интернета. Это положение должна изменить, в частности, совместная декларация (2011) о свободе выражения мнений в интернете. В преамбуле декларации подчеркивается «преобразующая роль интернета в плане предоставления права голоса миллиардам людей повсюду в мире и существенного расширения их возможности получать информацию, а также укрепления плюрализма и обеспечения отчетности». В ней также отмечается, что «некоторые правительства предприняли попытки ввести или приняли меры с конкретной целью значительно ограничить свободу выражения мнений в интернете вопреки нормам международного права». Первая статья СДСВМИ однозначно провозглашает принцип: «Принципы свободы выражения мнений распространяются на интернет так же, как и на все прочие средства коммуникации (выделено нами. — *Авт.*). Ограничения свободы выражения мнений в интернете приемлемы, только если они соответствуют установленным международным нормам, в том числе предусмотрены законодательством и

необходимы для защиты интересов, признанных в рамках международного права („тройной тест“)».

В условиях повышающегося градуса напряженности международного и локальных национальных диалогов вокруг регулирования интернета и правоотношений, возникающих в связи с его использованием, вопрос о правах пользователей звучит все более остро. Данное исследование позволяет делать вывод о том, что основным подходом на пути к сбалансированному и благоприятному для всех сторон управлению интернетом должно стать допущение к процессу всех участников правоотношений, в том числе пользователей.

Интерпретация прав человека применительно к информационному обществу и интернету позволяет наделить виртуальную личность человека вполне реальными правами, каждое из которых подтверждено и защищено тем или иным международным документом и раскрывается в национальном законодательстве.

Государство обязано создавать условия для реализации пользователями своих прав (так же, как и гражданам) путем, в частности, предоставления им технических возможностей, развития инфраструктуры телекоммуникаций; создания и развития благоприятных правовых и экономических условий для того, чтобы появлялись частные компании, которые будут заниматься развитием интернета; продвижением компьютерной и интернет-грамотности среди населения, создания национальных сетевых ресурсов, в том числе путем оцифровки хранящейся в государственных архивах информации; уважения прав и свобод своих граждан, не ограничивая свободу выражения мнения за пределами строго определенных в международных соглашениях и высших национальных законодательных актах целей.

Мы надеемся, что настоящее исследование будет способствовать повышению уровня правовой грамотности пользователей интернета, степени их вовлеченности в процессы управления интернетом, признанию их прав и повышению уровня их защиты.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Вельдер И.А. Система правовой защиты персональных данных в Европейском Союзе: Автореф. дис. ... канд. юрид. наук. Казань, 2006.

2. Стандарты Совета Европы применительно к положениям Конституции России. Избранные права. — М., 2002.

3. Положение об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденных постановлением Правительства РФ от 17 ноября 2007 г. // Российская газета. 2007. 21 ноября.

4. Поощрение, защита и осуществление прав человека в интернете. Резолюция Совета по правам человека № A/HRC/RES/20/8 от 16 июля 2012 г. // http://daccess-dds-ny.un.org/doc/RESOLUTION/GEN/G12/153/27/PDF/G1215327.pdf?OpenElement

5. Федеральный закон №8-ФЗ от 9 февраля 2009 г. «Об обеспечении доступа к информации о деятельности органов государственной власти и местного самоуправления» // Собрание законодательства РФ. 2009. №7.

6. Обязательства государств — участников Европейской конвенции о защите прав человека по исполнению постановлений Европейского Суда. Екатеринбург. 2005. Вып. 5. (Серия «Международная защита прав человека»).

7. Практическое руководство по критериям приемлемости. Совет Европы. 2011 // www.echr.coe.int

8. Companies Compete to Provide Saudi Internet Veil // New York Times. 2001. 19 ноября.

9. Kelly J., Etling B. Mapping Iran's Online Public: Politics and Culture in the Persian Blogosphere. Berkman Center for Internet and Society. 2008.

10. Bahar A. Iran Telecom Brief. 2008.

11. Faris R., Villeneuve N. Measuring Global Internet Filtering // Acess denied: The Practice and Policy of Global Internet Filtering. The MIT press. 2008.

12. Zittrain J., Palfrey J. Internet Filtering: The Politics and Mechanisms of Control // Acess denied: The Practice and Policy of Global Internet Filtering. The MIT press. 2008.

13. Murdoch S. J., Anderson R. Tools and Technology of Internet Filtering// Acess denied: The Practice and Policy of Global Internet Filtering. The MIT press. 2008.

14. Rundle M., Birdling M. Filtering and the International System: A Question of Commitment// Acess denied: The Practice and Policy of Global Internet Filtering. The MIT Press. 2008. P. 73–100.

15. Deibert R., Rohozinski R. Good for Liberty, Bad for Security? Global Civil Society and the Securitization of the Internet // Acess denied: The Practice and Policy of Global Internet Filtering. The MIT Press. 2008.

16. Deibert R., Rohozinski R. Beyond Denial: Introducing Next Generation Information Access Controls// Acess controlled: The Shaping of Power, Rights, and Rule in Cyberspace. The MIT Press. 2010..

17. Deibert R., Rohozinski R. Control and Subversion in Russian Cyberspace // Acess controlled: The Shaping of Power, Rights, and Rule in Cyberspace. The MIT Press. 2010.

18. Roberts H., Palfrey J. The EU Data Retention Directive in an Era of Internet SurveillanceAcess controlled: The Shaping of Power, Rights, and Rule in Cyberspace. The MIT Press. 2010.

19. Maclay C. Protecting Privacy and Expression Online: Can the Global Network Initiative embrace the character of the Net? Acess controlled: The Shaping of Power, Rights, and Rule in Cyberspace. The MIT Press. 2010.

20. Zittrain J., Palfrey J., Deibert R., Rohozinski R. Access Contested: Toward the Fourth Phase of Cyberspace Controls // Acess contested: Security, Identity, and Resistance in Asian Cyberspace. The MIT Press. 2010.

21. Thien Vee Vian The Struggle for Digital Freedom of Speech: The Malaysian Sociopolitical Blogosphere's

Experience // Acess contested: Security, Identity, and Resistance in Asian Cyberspace. The MIT Press. 2010.

22. Mueller M. L. China and Global Internet Governance: A Tiger by the Tail // Acess contested: Security, Identity, and Resistance in Asian Cyberspace. The MIT Press. 2010.

23. MacKinnon R. Corporate Accountability in Networked Asia // Acess contested: Security, Identity, and Resistance in Asian Cyberspace. The MIT Press. 2010.

24. Tanner A. Germany won't block access to foreign Nazi sites,., Silicon Valley News. 2000. 25 July.

Интернет-источники

1. Астахов подозревает, что в России действует педофильское лобби // http://www.interfax.ru/russia/news.asp?id=140551

2. Детская порнография: модель законодательства и всемирный обзор. 2010 // http://sartraccc.ru/Pub_inter/kindporno.pdf

3. Интернет гарантирован каждому жителю Финляндии // http://www.igotofin.ru/news/news81/

4. Корея запретила своим гражданам посещать северокорейский домен // http://www.cybersecurity.ru/crypto/112564.html

5. Между киберземлей и кибернебом: цензура в Сети рухнет 1 декабря // http://old.computerra.ru/print/297430/

6. Новая китайская секта «Фалуньгун» // http://iriney.ru/sects/falun/001.htm

7. Франция: тоталитарный закон Loopsi 2 // http://right-world.net/news/312

8. Южная Корея испугалась популярности КНДР в интернете // http://www.rg.ru/2010/08/23/korei-internet.html

9. Kim Hyung-eun Do new Internet regulations curb free speech? //http://joongangdaily.joins.com/article/view.asp?aid=2893577

10. Strafgesetzbuch [German Criminal Code], Section 130 // http://bundesrecht.juris.de/stgb/_130.html

11. South Korea ONI profile // https://opennet.net/research/profiles/south-korea

12. How Much of the Internet is Actually for Porn // http://www.forbes.com/sites/julieruvolo/2011/09/07/how-much-of-the-internet-is-actually-for-porn/

13. Symmes P. Che is dead // http://www.wired.com/wired/archive/6.02/cuba.html

14. Williams M. Google Disables Uploads, Comments on YouTube Korea // http://www.pcworld.com/article/162989/google_disables_uploads_comments_on_youtube_korea.html

15. Scrom P. SOPA & PIPA: Human Rights in Intellectual Property & Freedom of Speech // http://www.thehumanrightsblog.com/?p=1202

16. ITU Internet Indicators //http://www.itu.int/ITU-D/icteye/Reporting/ShowReportFrame.aspx?ReportName=/WTI/InformationTechnologyPublic&RP_intYear=2008&RP_intLanguageID=1

17. Cuba ONI profile // https://opennet.net/research/profiles/cuba

18. Terms and conditions for Y.Net Service // http://www.y.net.ye/support/rules.htm.

19. Going online in Cuba: Internet under surveillance // http://www.rsf.org/IMG/pdf/rapport_gb_md_1.pdf.

20. Burmese Regulations for Cybercafés Stringent as Expected // http://opennet.net/blog/2008/07/burmese-regulations-cybercafes-stringent-expected

21. Darren A. South Korea Tops Akamai Broadband Averages with 17 Mbps // http://www.techwatch.co.uk/2010/10/21/south-korea-tops-akamai-broadband-averages-with-17mbps

22. Lintner B. North Korea's IT revolution // http://www.nkeconwatch.com/category/dprk-organizations/companies/korea-computer-center-kcc/kwangmyong-computer-network/

23. Rhoads C., Fassihi F. Iran Vows to Unplug Internet // http://online.wsj.com/article/SB10001424052748704889404576277391449002016.html

24. Internet access is «essential» human right, rules German court // http://www.globalpost.com/dispatch/news/

business/technology/130128/internet-access-essential-rules-german-court

25. Wünsch S. Internet access declared a basic right in Germany // http://www.dw.de/internet-access-declared-a-basic-right-in-germany/a-16553916

26. Cracking Down on Digital Communication and Political Organizing in Iran // http://opennet.net/blog/2009/06/cracking-down-digital-communication-and-political-organizing-iran

27. The new decision for the internet media by the parliament // http://www.ghalamnews.ir/news-6261.aspx

28. The Enemies of the Internet Special Edition : Surveillance, Reporters Without Borders //http://surveillance.rsf.org/en/

29. http://newsru.co.il/rest/03dec2009/aviva_ziyi_111.html

30. Tor partially blocked in China //https://blog.torproject.org/blog/tor-partially-blocked-china

31. China's Green Dam: The Implications of Government Control Encroaching on the Home PC // http://opennet.net/sites/opennet.net/files/GreenDam_bulletin.pdf

32. Bandurski D. China's Guerrilla War for the Web // Far Eastern Economic Review.— 2008. // http://testfeer.wsj-asia.com/essays/2008/august/chinas-guerrilla-war-for-the-web

33. Bandurski D. China's Guerrilla War for the Web // http://testfeer.wsj-asia.com/essays/2008/august/chinas-guerrilla-war-for-the-web

34. Memorandum on Regulation of the Media in the Islamic Republic of Iran. Article 19. // http://www.unhcr.org/refworld/country,,ART19,,IRN,,475e4e270,0.html

35. China: Investigate Crackdown before Torch Relay's Passage through Tibet // http://www.hrw.org/en/news/2008/03/23/china-investigate-crackdown-torch-relay-s-passage-through-tibet

36. Batty D. Media Face Web Censorship at Beijing Olympics // The Guardian. 2008 // http://www.guardian.co.uk/world/2008/jul/30/china.olympicgames2008

37. Information Office of the State Council of the People's Republic of China, National Human Rights Action Plan of China (2009–2010) // http://news.xinhuanet.com/english/2009-04/13/content_11177126.htm

38. http://www.hrw.org/en/reports/2009/10/22/we-are-afraid-even-look-them

39. China: Journalists Protest Savage Attacks on Colleagues // http://www.unescobkk.org/information/news-display/article/china-journalists-protest-savage-attacks-on-colleagues

40. China Shuts Down Internet in Xinjiang Region after Riots // http://opennet.net/blog/2009/07/china-shuts-down-internet-xinjiang-region-after-riots

41. Tan K. The Google.cn/Google.com.hk Lockdown Has Begun: ALL Search Queries Now End in a Connection Reset // http://shanghaiist.com/2010/03/30/the_googlecn_googlecomhk_lockdown_h.php

42. Turkmenistan Helsinki Foundation for Human Rights // http://www.tmhelsinki.org/en/modules/news/article.php?storyid=3310

43. http://www.electroname.com/story/4665

44. http://www.electroname.com/story/4665

45. Internet Enemies, Reporters Without Borders // http://march12.rsf.org/i/Report_EnemiesoftheInternet_2012.pdf

46. http://www.turkmenistan.ru/?page_id=3&lang_id=en&elem_id=12682&type=event&sort=date_desc

47. http://hitech.newsru.com/article/05jun2008/inet

48. Internet Indicators: Subscribers, Users and Broadband Subscribers //http://www.itu.int/ITU-D/icteye/Reporting/

49. Survey on the Wireless Internet Usage Executive Summary // http://isis.kisa.or.kr/eng/sub01/?pageId=010400

50. Kim Hyung-eun Do new Internet regulations curb free speech? // http://joongangdaily.joins.com/article/view.asp?aid=2893577

51. Korea Policing the Net. Twist? It's South Korea //http://www.nytimes.com/2012/08/13/world/asia/critics-see-south-korea-internet-curbs-as-censorship.html?pagewanted=all

52. Safer Internet Programme 2009–2013 // http://ec.europa.eu/information_society/activities/sip/policy/programme/current_prog/index_en.htm.

53. Directive 2000/31/EC of the European Parliament //http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32000L0031:EN:HTML

54. Audiovisual Media Services Directive (AVMSD) // http://ec.europa.eu/avpolicy/reg/avms/index_en.htm.

55. SABAM v. s.a. Scarlet (anciennement Tiscali) // http://www.juriscom.net/documents/tpibruxelles20070629.pdf

56. Bockstaele B.B.V. Belgian Government Trying to Censor the Internet. // Digital Journal. — 2009 // http://www.digitaljournal.com/article/271340#tab=featured&sc=0&contribute=&local=

57. http://mirror.wikileaks.info/wiki/Denmark__3863_sites_on_censorship_list,_Feb_2008/

58. Samlet it-branche i skarp protest mod dansk internetcensur // http://www.version2.dk/artikel/19370-samlet-it-branche-i-skarp-protest-mod-dansk-internetcensur

59. http://advocacy.globalvoicesonline.org/2010/05/31/internet-freedom-under-pressure-in-denmark/

60. http://www.ustr.gov/acta

61. http://wikileaks.org/wiki/Proposed_US_ACTA_multilateral_intellectual_property_trade_agreement_(2007)

62. http://cijmalaysia.org/

63. About section 14A. // http://stop114a.wordpress.com/what-is-section-114a/

64. http://www.crtc.gc.ca/eng/home-accueil.htm

65. http://web.archive.org/web/20080119180947/http://www.crtc.gc.ca/eng/news/releases/1999/r990517.htm

66. http://surveillance.rsf.org/en/

67. http://www.genderit.org/upload/ad6d215b74e2a8613focf5416c9f3865/A_Report_on_Internet_Access_in_Iran_2_.pdf

68. http://www.isu.net.sa/saudi-internet/contenet-filtring/filtring.htm

69. http://archive.is/SrHQ

70. http://www.al-bab.com/media/docs/saudi.htm

71. http://www.tgdaily.com/business-and-law-features/53403-saudi-arabia-bans-blogging-without-a-licence

72. http://www.tgdaily.com/business-and-law-features/53403-saudi-arabia-bans-blogging-without-a-licence

73. http://www.hadopi.fr/

Ирина Левова, Глеб Шуклин, Дмитрий Винник
ПРАВА ИНТЕРНЕТ-ПОЛЬЗОВАТЕЛЕЙ:
РОССИЯ И МИР, ТЕОРИЯ И ПРАКТИКА

Редактор: Б. Левина
Дизайн: В. Харитонов

НП «Ассоциация интернет-издателей»
http://webpublishers.ru
join@webpublishers.ru

Подписано к печати 23.06.2013.
Уч.-изд. л. 6. Усл. печ. л. 9. Тираж 1000 экз.

ISBN 978-5-7525-2831-6