



**ЦЕНТР
ПОЛИТИЧЕСКОЙ
ИНФОРМАЦИИ**

ПРАВОВОЕ РЕГУЛИРОВАНИЕ СЕГМЕНТОВ ИНТЕРНЕТА

Информационно-аналитический доклад

Москва 2013

Москва, Zubovskiy bulvar, d.4,
подъезд "Союз журналистов России", 4 этаж
+7(495) 637-48-85; +7(495) 637-49-54
E-mail: cpi@polit-info.ru

Оглавление

| | |
|----------------------|----|
| США | 3 |
| ВЕЛИКОБРИТАНИЯ | 6 |
| ФРГ | 7 |
| ФРАНЦИЯ | 8 |
| ИТАЛИЯ | 9 |
| АВСТРАЛИЯ | 9 |
| КАНАДА | 9 |
| ЯПОНИЯ..... | 10 |
| НОРВЕГИЯ | 10 |
| ФИНЛЯНДИЯ..... | 11 |
| БЕЛЬГИЯ | 11 |
| НИДЕРЛАНДЫ..... | 11 |
| ДАНИЯ | 11 |
| ЧЕХИЯ | 12 |
| ВЕНГРИЯ | 12 |
| ПОЛЬША..... | 13 |
| ЛИТВА..... | 13 |
| ТУРЦИЯ..... | 13 |
| ВЫВОДЫ..... | 14 |

ПРАВОВОЕ РЕГУЛИРОВАНИЕ СЕГМЕНТОВ ИНТЕРНЕТА

Информационно-аналитический доклад

В ряде стран цензуру сети часто осуществляют сами Интернет-провайдеры и операторы связи под давлением властей или добровольно - из соображений лояльности к правительству.

Практически во всех западных странах под предлогом обеспечения внутренней безопасности (без судебной санкции) правоохранные органы и спецслужбы ведут плотный мониторинг интернет-трафика, осуществляют перехват переписки и получают персональные данные пользователей, используя, как свой технический потенциал, так и посредством запросов или в сотрудничестве с провайдерами.

США

В Соединённых Штатах Америки согласно принятому в 2001 году «Акту о защите детей в Интернете» (Children's Internet Protection Act, CIPA) ограничен доступ к ряду интернет-ресурсов, содержащих информацию непристойного характера, в общественных местах (школы, библиотеки). Для фильтрации используются коммерческие фильтрующие программные пакеты, однако в ряде штатов применяется блокирование IP-адресов на уровне провайдера. Некоторые программы-фильтры были замечены в избыточной фильтрации.

Законы «О противодействии терроризму» от 2001 г. (Patriot Act) и «О надзоре за деятельностью спецслужб» (Foreign Intelligence Surveillance Act) с поправками от 2008 г. наделяют правоохранные органы широкими полномочиями по мониторингу интернет-трафика и, в первую очередь, переписки граждан.

Власти США путем давления через Конгресс или через распределение бюджетных ассигнований вынуждают интернет-компании сотрудничать с правоохранными органами. Так, на основании «Акта о защите детей в Интернете» установление программных пакетов-фильтров стало обязательным условием для предоставления школам и библиотекам федеральных скидок на оплату телекоммуникационных услуг и доступа в Интернет.

Одновременно федеральные власти напрямую сотрудничают с провайдерами и поисковиками с целью блокирования доступа к интернет-ресурсам и фильтрации контента. Так, за период с июля по декабрь 2011 года компания Google получила от госорганов США на 103% больше запросов на

удаление контента, чем за предыдущий период, а также более 12 тысяч запросов на раскрытие данных о пользователях. Большинство из таких запросов удовлетворяется.

ФБР США расширяет практику активного мониторинга открытого сегмента виртуального пространства. Сотрудники ФБР после регистрации в Интернете под вымышленными именами предпринимают шаги по установлению контакта с интересующими их лицами, отслеживанию деятельности определенных сайтов, созданию подставных сайтов-ловушек, используемых для сбора сведений на проявивших к нему интерес граждан, ведению пропагандистской работы.

Учитывая расположение «корневых» интернет-серверов в США, Агентство национальной безопасности (АНБ) имеет возможность контролировать значительную часть трафика, в том числе из других регионов мира. Получение и первичный анализ информации осуществляется агентством самостоятельно в соответствии с указаниями руководства страны и ориентировками коллег по силовому блоку.

Задача по анализу общего информационного фона в открытом сегменте Интернета, прежде всего в социальных сетях, поручена специальным подразделениям по общественным контактам Национального центра операций Министерства внутренней безопасности (МВБ) США (NationalOperationsCenterSocialNetworkingMediaCapability). На основе анализа обобщенных сведений об активности в Интернете, предоставляемых провайдерами, центр формирует комплексную картину общественных настроений в Интернете относительно отдельных событий.

Для функционирования существующих и создаваемых в США средств контроля информационного пространства необходимы значительные ресурсы. В настоящее время на территории страны действуют 20 специализированных информационных центров, которые занимаются аккумуляцией на постоянной основе сообщений электронной почты и поисковых запросов интернет-сервисов. На третий квартал 2013 г. АНБ США запланировало ввод в строй нового, более совершенного комплекса по сбору, анализу и дешифровке перехватываемой информации (UtahDataCenter). Указанный комплекс призван обеспечить установление тотального контроля над ресурсами Интернета, которые не просматриваются традиционными поисковыми системами и становятся популярными площадками для обмена данными конфиденциального характера.

В последнее время усилилась критика в адрес государственных органов США за необоснованное и непропорциональное с точки зрения национальной безопасности использование телекоммуникационных средств для вторжения в личную жизнь граждан и иностранцев.

Например, по итогам конкретного судебного процесса НПО «Американский союз за гражданские свободы» (АСГС) добилось

рассекречивания данных о требованиях Министерства юстиции США к телекоммуникационным компаниям сообщать о телефонных звонках абонентов стационарной и мобильной связи (при помощи определителя – *trapandtracedevices*). Выяснилось, что в 2009-2011 гг. общее число таких запросов возросло на 60% (с 23,5 тыс. в 2009 г. до 37,6 тыс. в 2011 г.). Причем за этот же период количество объектов слежки увеличилось в три раза (до 47 тыс. человек), что, как подсчитали правозащитники, превышает аналогичный показатель за все годы администрации Дж.Буша.

Резко выросло и число требований к телекоммуникационным корпорациям предоставлять федеральным правоохранительным органам, полиции штатов и графств данные о местонахождении, электронной корреспонденции и интернет-трафике пользователей. По сведениям НПО, в 2011 г. американские компании получили более 1,3 млн. таких запросов (рост на 361% по сравнению с 2009 г.).

Правозащитники выяснили, что одна из крупнейших компаний - AT&T - получает в день более 700 запросов и выставляет правоохранительным агентствам счет 50-70 долл. США за каждую информацию о контактах абонентов. Отказы редки, в основном вызваны тем, что мелкие телекоммуникационные компании не справляются с наплывом полицейских запросов.

Спецслужбы преимущественно интересуются данными о местоположении абонентов и их международных звонках. Отслеживание перемещений посредством американской системы геолокации (GPS) признано менее затратным, чем классическое прослушивание телефонных разговоров.

По оценкам АСГС, речь идет о беспрецедентном вторжении в частную жизнь граждан под предлогом защиты национальной безопасности. Правозащитники сетуют, что существующее законодательство и судебная практика не предоставляют добропорядочным гражданам достаточных гарантий невмешательства в их частную жизнь.

Верховный суд США в 1979 г. постановил (по делу «Смит против Мэриленда»), что четвертая поправка к конституции США защищает содержание телефонного разговора, но гарантии неприкосновенности личных сообщений не распространяются на информацию о том, с кем и когда говорил абонент и где в момент разговора он находился.

Наибольшую озабоченность правозащитников вызывает тот факт, что спецслужбы не обязаны обращаться в суд за ордером на получение данных о телефонных разговорах и электронных сообщениях граждан. По сложившейся практике, закрепленной в Федеральном законе 1986 г. «О защите электронной переписки», в суд направляется уведомление о намерении следить за конкретным абонентом. К тому же правоохранительные органы не указывают, собирают ли они личные данные

в рамках расследования конкретного дела, и не отчитываются перед судом о том, как использовалась полученная информация.

АСГС считает, что профильное законодательство необходимо модернизировать и поддерживает усилия законодателей (в т.ч. когрессмена-демократа Дж.Надлера) по внесению поправок в устаревший закон 1986 г. В частности, правозащитники требуют от всех федеральных ведомств (а не только Минюста, как это происходит сейчас), а также правоохранительных органов штатов и графств отчитываться перед конгрессом об использовании личной информации граждан, причем делать это публично, а не под грифом «секретно», публикуя регулярные доклады в Интернете.

ВЕЛИКОБРИТАНИЯ

Согласно законодательству Великобритании (The Protection of the Children Act, Sexual Offences Act 2003) запрещается копирование на компьютер, распространение, публикация и реклама непристойных фотографий или псевдофотографий с изображением ребенка до 18 лет. Эти действия караются заключением на срок до 10 лет.

Также, с целью пресечения оборота непристойной информации (включая порнографию) среди детей в Великобритании действует «Свод правил новых форм контента» (Code of Practice on New Form of Content), согласно которому все операторы мобильной связи ответственны за предустановку на мобильных телефонах фильтрационного программного обеспечения, блокирующего доступ к потенциально опасным для детей материалам.

На данный момент в Великобритании разрабатывается законопроект «Об информации, передаваемой по каналам связи» (Communications Data Bill), обязывающий компании-провайдеры хранить «до востребования» в своих архивах личные данные клиентов, включая их переписку по электронной почте и в социальных сетях, историю посещения сайтов и поисковых запросов. Такая информация должна будет предоставляться по запросу правоохранительным органам без судебной санкции.

Национальная «горячая линия» по мониторингу нелегального интернет-контента «Фонд Наблюдения за сетью Интернет» (Internet Watch Foundation, IWF) на регулярной основе формирует и обновляет «черный список», который направляется интернет-провайдерам. Те, в свою очередь, информируют специальные подразделения полиции, в частности национальный отдел по борьбе с преступностью (National Crime Squad, NCS). С момента своего создания Фонд удалил более 26 тыс. изображений детской порнографии с британских серверов и оказал помощь полиции в возбуждении уголовных дел.

В Министерстве внутренних дел на регулярной основе проводятся совещания с представителями интернет-компаний, в том числе управляющих структур таких социальных сетей, как Twitter, Facebook, LinkedIn. На указанных совещаниях обсуждаются преимущественно вопросы предотвращения использования Интернета террористическими, экстремистскими организациями. По рекомендациям правоохранительных органов и спецслужб интернет-провайдеры держат под особым контролем страницы в социальных сетях, принадлежащие наиболее активным членам мусульманской общины пакистанского и бангладешского происхождения и Британской национальной партии.

Отдельные компании, в частности Twitter и Facebook уже проинформировали британские спецслужбы о том, что они располагают программными и техническими возможностями для тотального отслеживания циркулирующей на данных ресурсах информации.

Деятельность британских госорганов по мониторингу информационного пространства тесно координируется ими с ЦРУ и АНБ США, австралийскими, канадскими и новозеландскими спецслужбами.

ФРГ

Регулирование интернет-пространства в ФРГ осуществляется на основе законов «О телекоммуникационных данных» и «Об ограничении тайны переписки, почтовых и телефонных сообщений». В январе 2012 г. на 4 года был продлен срок действия пакета антитеррористических законов от 2002 г., которые дают спецслужбам широкие полномочия по мониторингу Интернета.

Государственная политика по защите молодежи от негативного воздействия СМИ основывается на законах «О распространении материалов вредных для молодежи» (Act To Regulate The Dissemination of Writings and Media Contents Harmful to Young Persons) от 1953 г. и «О барьерах в Интернете» от 2009 г. Оба закона предполагают составление списка запрещенных материалов, распространяемых с помощью электронных средств. Нарушение закона наказывается денежным штрафом или лишением свободы. В 2005 году в данный список было внесено 650 порнографических, прославляющих насилие и «крайне правых» сайтов.

Германские Интернет-компании на добровольной основе фильтруют интернет-сайты на основе списка, который составляется Федеральным департаментом по вредным для молодежи медиаресурсам (Federal Department for Media Harmful to Young Persons).

В практическом плане контроль за содержанием информационного пространства в ФРГ ведет ряд специальных подразделений. Так, при

Объединенном антитеррористическом центре ФРГ в Берлине действует совместное Интернет-бюро, осуществляющее целевой мониторинг киберпространства.

С 1 апреля 2012 г. на базе федерального ведомства по защите информационных технологий в Бонне действует национальный центр по борьбе с киберпреступностью. Одной из задач центра является оперативная оценка содержания интернет-ресурсов, в том числе социальных сетей.

ФРАНЦИЯ

15 февраля 2011 Конституционным Советом Франции принят закон «О безопасности Интернета» (LOPPSI-2), направленный на обеспечение внутренней безопасности страны. Закон, в частности, предусматривает введение следующих мер регулирования и контроля сети:

- осуществление обязательной фильтрации сети Интернет для пресечения распространения детской порнографии на основании составляемых МВД Франции совместно с общественными организациями «черных списков», а также незамедлительного блокирования ресурсов по представлению МВД Франции (без необходимости представления судебного решения);

- введение уголовной ответственности за кражу и использование персональных данных в сети Интернет (лишение свободы на срок до 1 года и денежный штраф);

- легализацию удаленной установки полицейскими подразделениями на компьютеры лиц, подозреваемых в совершении преступлений, специальных программ, позволяющих регистрировать и передавать в полицию данные о действиях, совершаемых пользователями персональных компьютеров (только по решению суда).

Для борьбы с терроризмом в Интернете в составе МВД Франции по работе на каналах электронных коммуникаций функционирует специализированное подразделение - «кибер-патруль». Представителям этой структуры разрешено участвовать под вымышленными именами в интернет-форумах и социальных сетях, поддерживать электронные контакты с лицами, подозреваемыми в подстрекательстве к терроризму. Цель таких контактов - установление личности подозреваемых и сбор доказательной базы для последующего судебного процесса. Сотрудники «кибер-патруля» освобождены от уголовной ответственности за свою профессиональную деятельность в рамках расследования по уголовному делу или исполнения следственного поручения.

ИТАЛИЯ

На данный момент Министерство юстиции Италии разрабатывает законопроект «О прослушивании», который предусматривает нормы контроля за интернет-сайтами и блогами. В документе предлагается ввести жесткие санкции в отношении информационных сайтов или блогов, которые распространяют заведомо ложные сведения. В частности, предусматривается, что администратор сайта или блоггер должны будут в течение двух суток убрать опротестованный материал и дать по нему соответствующее опровержение - в ином случае нарушителям грозит крупный штраф.

АВСТРАЛИЯ

Несмотря на то, что закона, позволяющего запрещать пользователям доступ к отдельным ресурсам сети Интернет, в Австралии до сих пор не принято, австралийская Комиссия по средствам массовой информации и коммуникациям (АСМА) осуществляет ограничение доступа к интернет-ресурсам. С 2007 г. АСМА ведет список запрещённых сайтов, который регулярно пополняется. Комиссия требует от провайдеров блокировать сайты, входящие в её «чёрный список», а против пользователей и ресурсов, размещающих ссылки на сайты из этого списка, заводятся судебные дела. При этом

содержание самого списка является закрытой информацией, так что пользователи и владельцы ресурсов не имеют возможности официально ознакомиться с его содержанием.

КАНАДА

В Канаде в соответствии с уголовным кодексом список блокируемых материалов (в основном порнографического характера с участием несовершеннолетних) формируется по результатам судебной экспертизы. Оборот списка осуществлялся в рамках юрисдикции правоохранительных и судебных органов власти страны.

Блокирование зарубежных интернет-ресурсов, расположенных вне юрисдикции канадских правоохранительных органов осуществляется в рамках проекта «Cleanfeed/Канада» («Чистая связь»), реализованного в ноябре 2006 г, при содействии ведущих провайдеров Канады.

Аналитики cybertip.ca(данный портал, созданный Канадским центром по защите детей, принимает сообщения пользователей о ресурсах, содержащих детскую порнографию) оценивают сообщения от жителей Канады о нахождении в сети подобного рода сайтов и сообщают о возможном нарушении закона соответствующим правоохранительным органам. Ссылка, которую аналитики расценивают, как заслуживающую блокирования, вносится в «чёрный список» системы «Cleanfeed».

ЯПОНИЯ

В Японии принят специальный законодательный акт, затрагивающий Интернет -«Закон о формировании условий для безопасного пользования интернетом несовершеннолетними» от 2008 г. Им предусматривается запрет на размещение материалов, содержащих подстрекательство к совершению противоправных действий, порнографию, сцены жестокости и насилия. Владельцам интернет-сайтов вменяется в обязанность осуществлять самоцензуру.

НОРВЕГИЯ

В Норвегии не существует специального законодательства, регулирующего Интернет. Защита от злоупотреблений свободой слова, в том числе в интернете, предусмотрена статьями уголовного кодекса, а также законом «О защите персональных данных», законом «Об авторском праве на творческие произведения».

Норвежские власти проводят активный мониторинг сети с целью выявления страниц, содержащих детскую порнографию. С 2004 г. провайдеры в сотрудничестве с полицией составляют «чёрный список» нелегальных ресурсов и применяют к ним блокирующий фильтр.

Задача по мониторингу деятельности клиентов местных операторов сотовой связи и интернет-провайдеров решается также посредством сбора и накопления спецслужбами оперативно-значимой информации, как напрямую от поставщиков услуг, так и при помощи специальных программно-аппаратных средств. Указанные меры безопасности предпринимаются норвежскими властями на фоне отсутствия возможности анонимного использования проводного Интернета и средств сотовой связи. Все контракты на оказание соответствующих услуг заключаются только при предоставлении клиентом подробных сведений о себе.

ФИНЛЯНДИЯ

Закон «О мерах, препятствующих распространению детской порнографии» от 2006 г. предоставляет полиции Финляндии право составлять список сайтов, содержащих детскую порнографию и направлять его провайдерам. Речь идет о возможности закрытия доступа только к иностранным интернет-ресурсам. Однако решение о закрытии доступа к сайтам принимает непосредственно провайдер.

В 2008 г. в Финляндии имел место резонансный случай закрытия сайта сторонника свободы в Интернете, на котором размещались критические статьи в отношении указанного закона.

БЕЛЬГИЯ

В Бельгии существует целый ряд законов, ограничивающих свободу слова в информационном пространстве: «О борьбе с проявлениями расизма», «Об ответственности за отрицание холокоста», «О борьбе с дискриминацией», «О террористической деятельности». На их основе бельгийские спецслужбы проводят плотный мониторинг контента бельгийского сегмента глобальной сети с целью выявления элементов, способных нанести ущерб национальной безопасности.

НИДЕРЛАНДЫ

Борьба с противоправным контентом ведется на основе обычного административного и уголовного законодательства. Так, по решению суда, нарушитель, разместивший информацию в Интернете (например, порнография или оскорбление королевы), а также провайдер могут быть обязаны удалить информацию.

ДАНИЯ

Вопросы неправомерного использования информационного пространства в Дании регулируются в соответствии с положениями национального уголовного кодекса. Отдельные его положения наделяют правоохранительные органы полномочиями требовать по решению суда от поставщиков информационных услуг хранить до трех месяцев персональные данные пользователей и информацию о передаваемых электронных

сообщениях.

В Дании ведется активная борьба с нарушениями в области авторских прав в Интернете. Так, в 2010 г. Верховный суд Дании обязал провайдеров блокировать доступ к сайтам, которые содержат или имеют ссылки на материалы, нарушающие авторские права.

ЧЕХИЯ

В Чехии регулирование вопросов использования интернет-пространства осуществляется на основе закона «Об аудиовизуальных медиа-услугах». Указанный закон содержит ограничения распространения информации, влияющей на подсознание, способствующей разжиганию ненависти по половому, языковому, расовому признаку, по причине вероисповедания, политических или иных убеждений. Интернет-услуги, содержащие, прежде всего, порнографический контент и демонстрацию насилия, могут быть доступны, только если их содержание не могут наблюдать дети и молодежь. За нарушение этих требований предусмотрен штраф в размере порядка 100 тысяч долларов.

ВЕНГРИЯ

Порядок размещения информации в Интернете в Венгрии регулируют два основных нормативных акта: закон «О некоторых вопросах оказания коммерческих услуг с использованием электронных средств, а также услуг, связанных с функционированием

информационного общества» от 2001 года и закон «Об электронной связи» от 2003 года. Законодательно интернет в Венгрии не относится к СМИ.

Интернет-ресурс может быть заблокирован по решению МВД или суда с целью воспрепятствовать распространению вредоносного контента, в частности, создающего угрозу внутренней безопасности страны путем разжигания расовой, религиозной вражды, межнациональной розни, подрыва общественного порядка и обороноспособности государства, а также пропагандирующего детскую порнографию и т.п.

Венгерские провайдеры обязаны сотрудничать с правоохранительными органами и специальной службой национальной безопасности в сборе информации закрытого характера.

ПОЛЬША

В Польше применительно к Интернету руководствуются законами «О СМИ» и «О порядке предоставления услуг связи электронным путем». К возможным нарушениям в сфере размещения информации в глобальной сети в соответствии с гражданским и уголовным кодексами относятся: клевета, публичное распространение порочащих сведений и мошенничество.

ЛИТВА

Применяется закон «Об общественной информации» от 1996 г., в котором закреплена свобода выражения мыслей и убеждений, но также предполагается возможность ограничения этого права «для защиты конституционного уклада, здоровья, чести и достоинства, частной жизни, нравственности человека».

На основе закона «Об оперативной деятельности» от 2002 г. весьма активный мониторинг сети осуществляет Департамент госбезопасности Литвы (ДГБ). В отчете этого ведомства за 2011 год приведена статистика: в 2011 г. ДГБ выполнил 412 задач по контролю информации, передаваемой в Интернете, 5119 - по получению информации об имевших место событиях в сетях электронной связи. По оценкам экспертов, Литва является лидером в ЕС в области негласного контроля за контактами граждан в Интернете.

ТУРЦИЯ

В Турции основным документом, регулирующим сферу использования Интернета, является закон «Об упорядочивании размещения информации в Интернете и борьбе с правонарушениями, совершаемыми посредством всемирной сети». В нем определены типы «нежелательной» информации и вводится ответственность за нарушение установленных норм. К запрещенному контенту относятся пропаганда терроризма, наркотиков, порнографии, в первую очередь детской, проституции, азартных игр, материалы, оскорбляющие Ататюрка.

По неофициальным оценкам, с 2007 года был заблокирован доступ более чем к 20 тысячам сайтов. В будущем руководство страны планирует ввести повсеместную фильтрацию интернет-ресурсов по ключевым словам.

ВЫВОДЫ

1. Меры, принимаемые правительствами и спецслужбами иностранных государств, по законодательному, техническому и организационному регулированию деятельности в Интернете с целью защиты своего информационного пространства, национальных интересов, обеспечения информационного суверенитета, противодействия киберугрозам, терроризму, распространению порнографии, наркотиков и т.д.

2. Выдвижение международной инициативы по выводу из-под единоличного контроля США «международной» компании-регулятора (распределителя) присвоения доменных имен в сети Интернет ICANN и создания серверных площадок, обеспечивающих функционирование Интернета, за пределами США.

3. В настоящее время из 14 глобальных узлов Интернета на планете 12 принадлежат американцам, которые к тому же через агентов влияния контролируют «независимый» Международный союз электросвязи, определяющий международные и обязательные для всех стран правила функционирования Интернета со всеми вытекающими последствиями. Данным положением вещей возмущена не только Россия, но и Китай, а также ряд крупных государств, которых сейчас американцы активно «обрабатывают», чтобы не допустить в мае с.г. консолидированного выступления по предложенной инициативе России и Китая в ООН.

4. Попытки обсуждения этих тем в российском медиа-пространстве сразу же приводят к истерике либерального лобби, «независимых» блогеров и журналистов, обвиняющих государство в попытке введения «цензуры» в Интернете и т.п., что на самом деле стимулируют по вышеуказанным причинам сами «демократичные» США.

ПРАВОВОЕ РЕГУЛИРОВАНИЕ СЕГМЕНТОВ ИНТЕРНЕТА

Информационно-аналитический доклад

© - Центр политической информации
Сведения приведены на 24 апреля 2013 года

Все права сохранены, материалы запрещено перепечатывать
и распространять в электронном или каком-либо ином виде без письменного разрешения авторов.