

Угроза неприкосновенности частной жизни: надзор как первое ограничение

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

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

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

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

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

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

Право оставаться неидентифицированным в процессе коммуникации

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

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

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

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

Любая попытка государства ограничить свободу слова может быть объявлена незаконной как противоречащая Конституции. Ограничения свободы слова могут быть незаконными в силу размытости своих формулировок, что способно оказать парализующее воздействие на свободу слова; из-за широкого толкования законов, запрещающих как защищаемую, так и не защищаемую свободу слова; установления априорных ограничений на свободу слова; регулирования содержания слова при отсутствии узкоспециальной задачи, стоящей перед государством, и менее суровой ограничительной альтернативы; при этом постановления, принуждающие к слову, не разрешены. Запрет на принуждение к слову был использован для отмены законов, обязывающих людей раскрывать свою идентичность³⁹.

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

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

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

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

В 1958 г. Верховный Суд поддержал право Национальной ассоциации содействия прогрессу цветного населения (NAACP) не раскрывать списки членов недружественному ей правительству штата Алабама⁴⁰.

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

В своем решении по делу «Тэлли против штата Калифорния»⁴¹ судебная коллегия записала:

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

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

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

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

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

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

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

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

В этом случае решение Верховного Суда гласило, что нет оснований считать, что текст сообщения содержал ложную, вводящую в заблуждение или клеветническую информацию. В решении Суда⁴² говорилось:

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

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

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

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

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

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

Самым последним по времени судебным решением на данную тему стало решение по делу «Сторожевая башня Библии против Страттона» (*Watchtower Bible v. Stratton*) в июне 2002 г. Суд вынес следующее постановление⁴³:

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

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

Что касается Интернета, то правительства часто пытались требовать от граждан идентификации личности для предоставления им права высказывать свое мнение. В 1996 г. органы законодательной власти штата Джорджия приняли закон, запрещающий анонимные и псевдонимные высказывания в онлайн-режиме. ACLU предупредил о неконституционном характере данного закона, поскольку он накладывал ограничения на контент в части выражения мнения в компьютерных сетях⁴⁴. Суды согласились, что закон чрезмерно широко и нечетко трактовал этот вопрос и накладывал ограничения на контент в нарушение Конституции.

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

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

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

намерение обмануть или обман уже имел место. Поэтому этот законодательный акт можно применять к широкому спектру случаев передачи информации, которые «ложно идентифицируют» отправителя, но при этом не являются «мошенническими» в значении уголовного кодекса⁴⁵.

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

Поддержка права анонимного доступа и отход от него

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

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

Те же идеи стояли за решением суда:

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

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

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

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

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

Однако анонимность пользователей не идет дальше провайдеров интернет-услуг. Неудивительно, что режим Мои (Moi) в Кении регулярно требовал от провайдеров предоставлять списки своих абонентов; что пользователи интернет-кафе в Бирме должны регистрироваться и указывать свои паспортные данные и адреса; что Южная Корея предложила установить порядок, по которому национальные паспортные данные должны быть предоставлены до того, как человек получит право размещать свои сообщения на «досках объявлений» общественных организаций; что пользователи в Италии должны безо всяких оснований предъявлять паспорта в интернет-кафе; что растущее беспокойство вызывает закон, требующий установки систем наблюдения в интернет-кафе одного из городков Калифорнии⁴⁷. Полиция Индии требует от властей штата Махараштра установить порядок, по которому Интернет-кафе могут получить лицензии только после установки фильтров на программном обеспечении; помимо этого, все посетители должны будут в обязательном порядке заполнять длинные анкеты с указанием своих адресов, номеров телефонов и других данных, а также предъявлять удостоверения личности с фотографией⁴⁸. Установление идентичности пользователей услуг интернет-провайдеров и разглашение этой информации вызывает все больше и больше вопросов.

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

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

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

пользователей достигло 500 000, а в день обрабатывалось более 7000 сообщений, сервис был закрыт⁴⁹. Полиция Финляндии предъявила Хельсингиусу ордер на обыск в связи с расследованием заявления, поступившего от Церкви сайентологов, обвинявшей Хельсингиуса в использовании anon.penet.fi для разглашения частной информации, взятой из компьютеров церкви, и размещении ее на сайте alt.religion.scientology в USENET.

22 августа 1996 г. окружной суд г. Хельсинки вынес постановление, обязывающее г-на Хельсингиуса передать полиции электронный адрес отправителя⁵⁰. В качестве обоснования причины вынесения данного постановления суд привел пример, что свидетель не имеет права уклоняться от предоставления информации в ходе судебного заседания, что сообщения, о которых идет речь, были направлены в общедоступную сеть, и что публичные сообщения не защищены законом. Хельсингиус отверг данное требование, заявив, что конфиденциальность почтовых отправок, телефонных разговоров и других личных сообщений защищена Конституцией Финляндии и не может быть нарушена в ходе предварительного расследования мелкого правонарушения, коим являлось выдвинутое против него обвинение в нарушении авторского права. На основании решения окружного суда, после пяти обысков, которые проводила полиция в связи с поступлением новых обвинений в нарушении авторских прав и сообщений, содержащих оскорбления в адрес официальных лиц других стран, Хельсингиус был вынужден закрыть свой сервис⁵¹.

Определенную роль в этом решении сыграл страх быть обвиненным в преступлении. The London Observer цитировала консультанта ФБР, который сказал, что до 90% детской порнографии, которую он нашел в Интернете, проходила через римейлер Хельсингиуса⁵². После

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

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

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

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

расследования, проведенного финской полицией, обвинение Observer оказалось беспочвенным – за год до статьи в Observer полиция подтвердила, что деятельность римейлера была ограничена, и передача изображений была запрещена. Римейлер также обвиняли в том, что им часто пользовались криминальные лица из России⁵³. Под натиском всех этих обвинений сервер был закрыт, несмотря на то, что он использовался одной британской организацией для предотвращения суицида отчаявшихся людей, не желающих раскрывать свои имена⁵⁴.

Ограничение свободы слова за счет введения массового надзора

Личность пользователей раскрывается все чаще. Во многих странах мира суды выносили постановления, обязывающие раскрывать личность людей, помещающих объявления в Интернете, людей, осуществляющих электронные рассылки, и рядовых пользователей. Авторское право, предписывающее предоставлять информацию о предполагаемых пользователях файлов, усугубляет ситуацию в сфере защиты неприкосновенности частной жизни человека. На сегодняшний день музыкальная и звукозаписывающая отрасль в США выдала более 2400 повесток⁵⁵.

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

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

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

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

виняют в участии в незаконном анонимном общении в Интернете. Особенность ситуации в том, что, поскольку анонимное слово находится под защитой конституции, повестка в суд по поводу выдачи информации об абоненте подпадает под иммунитет при условии соответствия установленным требованиям. Возможно, что установление личности этих людей плохо скажется на анонимности общения: интернет-пользователи будут знать, что их смогут идентифицировать люди, способные ложно обвинить их в нарушении закона, даже не имея намерения затевать судебный процесс⁵⁶.

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

Доступ к данным о трафике представляется проблематичным с позиций защиты неприкосновенности частной жизни. По мнению группы экспертов Еврокомиссии по неприкосновенности частной жизни и защите данных⁵⁷, информация о трафике и современные коммуникационные инфраструктуры становятся все более деликатной сферой.

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

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

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

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

Этот рост данных фактически усугубляется по причине принятия определенных законов.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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