ПОЛИС

Электронная библиотека
Гражданское общество в России

С. В. Бондаренко

Социальный контроль в информационном обществе (как государство и коммерческие структуры собирают персональную информацию о гражданах)

Электронный ресурс

URL: http://www.civisbook.ru/files/File/Bondar_soz.pdf

Перепечатка с сайта центра «Стратегия»
http://strategy-spb.ru

С. В. Бондаренко

Социальный контроль в информационном обществе (как государство и коммерческие структуры собирают персональную информацию о гражданах)

Как известно, «прозрачность» является одним из условий противодействия коррупции. Вместе с тем неконтролируемый общественными структурами сбор персональной информации о гражданах и иных акторах может иметь негативные последствия для демократии. Было бы ошибкой считать, что «информационное» общество является синонимом «демократического» общества. Собранная государством персональная информация может использоваться не только для разоблачения коррупционеров, но и для противодействия борьбе с коррупцией.

«Всевидящее око «Большого брата» следит за вами...». Эта знаменитая фраза из романа Оруэлла несет в себе предупреждение, что любопытствующий глаз, возможно, наблюдает за вашими действиями. В настоящей статье автор предпринял попытку обозначить формы и методы осуществления социального контроля, как за рубежом, так и в России, предоставив читателю возможность самостоятельно сделать соответствующие практические выводы из представленной информации.

Исторические корни организации социального контроля

Без использования принципа историчности невозможно понять гносеологическую историю того или иного феномена, существующего в социальной жизни общества. Существует точка зрения, в соответствии с которой организация социального контроля, как, к примеру, отмечала американский исследователь Джоэл Ковел (Joel Kovel), «неотъемлемо связанна с развитием технологий» [1].

Проблема использования для организации социального контроля технических средств, не нова и волнует власть предержащих с момента возникновения государства как социального института. В этой связи полезно помнить о том, что ещё в 1787 году английский философ Джереми Бентам (Jeremy Bentham) в своей работе «Panopticon; or The Inspection House» утверждал, что для осуществления эффективного социального контроля необходимо убедить людей в том, что они находятся под наблюдением в любое время суток [2]. При этом подразумевалось, что контроль должен осуществляться, в том числе и над теми, кто сам осуществляет функции контроля.

В своей работе Джереми Бентам предложил, говоря современным языком универсальную модель социального контроля, применимую как для тюрем, так и для фабрик, школ и иных социальных учреждений. Речь при этом шла об организации непрерывного автоматического контроля со стороны государства за своими согражданами. Образ, предложенный Бентамом, назвался Паноптикумом (Panopticon) и представлял собой здание круглой формы с рядом индивидуальных ячеек, расположенных вокруг стоящей в центре здания инспекционной башни. При этом каждая из ячеек была освещена, в то время как центральная башня маскировалась для того, чтобы иметь «возможности для наблюдения», не будучи при этом замеченной со стороны наблюдаемых. Для Бентама Паноптикум был архитектурной метафорой, позволяющей осуществить обобщение одной из сторон социальной жизни общества.

Современное общество, по определению французского философа Мишеля Фуко (Michel Foucault), это «система индивидуализации и постоянного документирования действий индивидов» [3]. При этом центральная башня Паноптикума Джереми Бентама, как метафора осуществления социального контроля, с каждым годом всё меньше и меньше соответствует современным реалиям. В наши дни уже не репрессивные структуры, а идеология, как утверждал известный

французский социолог Пьер Бурдье, образно говоря «структурирует структуры». В свою очередь современный британский исследователь Дэвид Лейг (David Leigh) предложил метафору «идеальной формы бюрократической утопии: должностное лицо невидимо и при этом гражданин раздет донага» [4].

Важную роль в вопросах организации социального контроля и сбора информации о гражданах играют компьютеры и телекоммуникационные сети. Начиная с середины 90-х годов XX века, правительства разных стран мира, осознав факт перерастания глобальных компьютерных сетей из маргинальной стадии в стадию быстрорастущей социальной общности и фактор экономического развития, стали разрабатывать, а также применять на практике в национальных сегментах киберпространства различные меры социального контроля. Кроме того, правительства стали в некоторых случаях претендовать на выполнение функций социального контроля не только в национальном, но и в международном масштабе.

Теракты 11-го сентября 2001 года, в вопросах использования компьютерных сетей для контроля над поведением граждан, стали своеобразным рубежом для многих государств. Герберт Маркузе (Herbert Marcuse), задолго до событий 11-го сентября 2001 года и последующего за ним во многих демократических странах отхода от приоритетности прав человека над всеми другими правами, очень точно подметил одну из важнейших особенностей современной цивилизации. «Современная эпоха, - писал Маркузе, - склонна к тоталитарности даже там, где она не произвела на свет тоталитарных государств» [5]. В конце XX и начале XXI века информационная открытость государственных институтов в демократических странах стала сочетаться с осуществлением тотального контроля над поведением граждан [6].

Государство как субъект социального контроля

В зависимости от типа социального устройства общества мы можем вести речь как о преимущественно однонаправленных процессах осуществления социального контроля (характерных для тоталитарных государств), так и двунаправленных процессах (типичных для демократических стран). Тоталитарные государства, используя все доступные им средства, в том числе и телекоммуникационные технологии, стремятся знать всё о своих гражданах, при этом ни в коей

мере не желая делиться с гражданами информацией о работе государственного аппарата.

В демократических странах ситуация с социальным контролем не слишком отличается от положения дел в тоталитарных государствах, разве что уровень доступности информации о происходящих в обществе процессах выше. Автор настоящей работы берет на себя смелость утверждать, что, начиная со второй половины 90-х годов XX века, прослеживается общемировая тенденция, в соответствии с которой правительства самых разных стран мира с каждым годом все шире использует компьютерные технологии для осуществления контроля над поведением своих граждан. Причем эта тенденция справедлива как в отношении демократических, так и в отношении тоталитарных обществ.

Благодаря активности структур гражданского общества, в демократических государствах регулярные попытки чиновников поставить под контроль частную жизнь граждан, периодически наталкиваются на сопротивление общественности [7]. То есть, говоря о демократических государствах, мы можем вести речь не только о том, что те или иные действия по осуществлению социального контроля направлены от государства к гражданам (однонаправленные процессы), но и о процессах воздействия граждан на государственные структуры (двунаправленные процессы). Результатом двунаправленных процессов является общественное согласие в отношении приемлемости тех или иных форм социального контроля поведения акторов.

Еще одним проявлением роли общественности в западных странах является активность СМИ в освещении процессов осуществления государственными и иными структурами социального контроля. Однако больше всего разговоров на указанную проблематику заинтересованные читатели могут обнаружить в сети Интернет [8]. «Субкультура Интернета как субкультура любого сообщества просто не может существовать без соответствующих слухов, сплетен и преданий. «Страшные истории о Большом Брате» — одна из самых популярных тем для обсуждения, так сказать, в кулуарах (открытые форумы, чаты, гневные и туманные высказывания так называемой Интернет-общественности)» [9].

Ряд зарубежных авторов, в частности Стив Леви (Steven Levy) [10], В. Ж. Ром (W.G. Rohm) [11], В. Швартау (W. Schwartau) [12], Кэсс Р. Сюнстайн (Cass R. Sunstein) [13] и другие, документально доказывают причастность военных, спецслужб и транснациональных корпораций к развитию сети Интернет. Несмотря на широкую распространённость в

сетевом социуме указанной точки зрения, документально подтверждённых оснований, позволяющих утверждать, что какая-либо национальная или международная организация единолично осуществляет функции глобального социального контроля компьютерных сетей, в настоящее время нет. Что отнюдь не препятствует практике сбора информации на национальном уровне соответствующими спецслужбами.

Важно отметить тот факт, что технологии, используемые для осуществления контроля над поведением пользователей в компьютерных сетях, носят секретный характер. К примеру, в Великобритании указанные технологии и оборудование, которые используются полицией для анализа получаемых в ходе наблюдения интернет-данных, держатся в таком строгом секрете, что криминальные дела могут прекращаться, дабы предотвратить их разглашение.

Государство может осуществлять функции социального контроля в киберпространстве как в пассивной форме (принимая законы и применяя меры нормативного регулирования по отношению к деятельности провайдеров), так и в активной форме - самостоятельно осуществляя контроль и регулирование входящего в страну трафика путем установки соответствующих фильтров.

С точки зрения информирования гражданина об осуществлении над его интеракциями социального контроля, указанная социальная функция может осуществляться в двух формах: открыто декларируемой и скрытой. В первом случае пользователя могут либо специально предупреждать о том, что получаемые от него данные могут использоваться по усмотрению владельцев посещаемых актором информационных ресурсов. При этом на актора возлагаются обязанности по использованию, к примеру, компьютерных сетей только для совершения определенных действий.

Во втором случае, при использовании скрытых форм социального контроля до определенного момента актор может и не подозревать, что все его коммуникационные взаимодействия находятся под контролем со стороны третьих лиц. В последнем случае в большинстве случаев речь идет о случаях исполнения соответствующими государственными структурами действующего законодательства по контролю над информационными взаимодействиями.

Аргументы для оправдания сбора персональной информации

Сторонники сбора персональной информации о гражданах используют самую разную аргументацию для оправдания собственной деятельности. Когда же люди узнают, какой объем подробной личной информации о них может быть собран, у них неизбежно возникают сильные негативные реакции. Рассмотрим на примерах наиболее типичные аргументы сторонников сбора персональной информации о частной жизни граждан и начнем с исторического экскурса.

Проблема выбора оптимальной модели организации социального контроля волнует человечество не одну сотню лет. К примеру, в начале XIX века в связи с ростом численности пролетариата во Франции резко возросла преступность. В ответ на рост преступности государство поспешило создать многочисленные отряды полиции. Когда же к 1810 году преступность по той же причине возросла и в Великобритании (вдобавок выяснилось, что полиции в стране нет), правившие в то время консерваторы вообще не стали создавать дополнительные антикриминальные структуры. «Люди смирились с беспорядком, сочтя это платой за свободу». В те годы британский философ Джон Уильям Уорд писал: «У парижан блистательная полиция, но они дорого платят за этот блеск. Пусть уж лучше каждые три-четыре года полудюжине мужчин сносят голову на Ратклиф-роуд, чем сносить домашние обыски, слежку и прочие ухищрения Фуше» [14].

В XXI веке авторы идей о сборе персональной информации приводят весьма экстравагантные аргументы. К примеру, чтобы не нарушать права человека... в Великобритании в 2000 году узаконили чтение чужих писем. Министр электронной коммерции и мелкого предпринимательства этой страны (Patricia Hewitt) объявила, что в целях повышения эффективности труда и для проверки деятельности своих сотрудников в рабочее время, начальство сможет просматривать их электронную почту и прослушивать телефонные разговоры.

В оправдание действий правительства министр подчеркнула, что решение было принято именно для обеспечения соблюдения прав человека. «Есть пределы, которые нельзя преступать, - сказала она, - например, прослушивание личных телефонных разговоров из неоправданного скабрезного интереса». По словам министра, руководители, так или иначе, перлюстрируют корреспонденцию своих

подчиненных, введение же четких правил досмотра и прослушивания предотвратит эти злоупотребления [15].

Существуют аргументы в защиту усиления сбора персональной информации, основанные на необходимости учета требований научно-технического прогресса и, соответственно, облегчения жизни граждан. Так, бывший генеральный советник Министерства торговли США Эндрю Пинкус (Andrew Pincus) утверждает, что опасения в отношении вмешательства в частную жизнь угрожают фрагментацией глобального рынка электронной торговли. По его словам, величайшей проблемой обеспечения жизнеспособности глобальной системы электронной торговли является нахождение путей стирания национальных границ в вопросах неприкосновенности частной жизни. По словам Пинкуса, применение закона о неприкосновенности частной жизни могло бы повлечь за собой трагические последствия для электронной торговли. Этот закон, по его мнению, подавляет творческие подходы к решению проблемы [16].

Среди аргументов внедрения тех или иных форм социального контроля есть и «стремление обеспечить регулирование дорожного движения»... Так, к примеру, в Финляндии в 2003 году была создана принципиально новая служба слежения за интенсивностью движения. Традиционно для этих целей использовались видеокамеры или специальные датчики, с помощью которых ведется подсчет количества автомобилей, проезжающих через данный участок дороги в единицу времени. Основным недостатком указанных систем было то, что они не всегда позволяют отслеживать в реальном времени движение на участках большой протяженности.

Новая система основана на подсчете не самих автомобилей, а подключенных к киберпространству сотовых телефонов, имеющихся у водителей и пассажиров. На автодороге через каждые 4,5 км устанавливаются датчики, отслеживающие изменение положения в пространстве сотовых телефонов. На основе информации от этих датчиков система определяет среднюю скорость движения транспортных средств и общую загруженность автотрассы.

Исходя из полученных данных, производится расчет ориентировочного времени движения по маршруту и предсказывается образование автомобильных пробок. Поскольку осуществление социального контроля в данном случае основано анализе изменения в пространстве сотовых телефонов, измерить реальное количество

транспортных средств затруднительно, поскольку в некоторых машинах, например автобусах, могут находиться десятки пассажиров и, соответственно, система будет идентифицировать автобус как несколько десятков отдельных машин. Решить указанную проблему возможно в сочетании с другими техническими средствами контроля.

Приводить аргументацию сторонников усиления социального контроля можно долго. Гораздо важнее понять направление движения общества. В реалиях экономически развитых стран, экономические рычаги воздействия и невозможность индивидам выживать вне обустроенных технологиями ареалов приводят к формированию ощущения бархатных репрессий, осуществляемых исключительно в интересах социума. Касаясь последней формы организации социального контроля, Роб Фиксимер пишет о том, каким образом в демократических странах государство ненавязчиво подвёдет своих граждан к необходимости её осуществления: «Реалии таковы, что добровольная общенациональная идентификация со временем неизбежно войдёт в нашу жизнь. Устав от бесконечных очередей в аэропортах, на мостах и в туннелях, не желая постоянно таскать с собой горы самых разных документов - от кредитных карточек до паспортов, американцы, в конце концов, сами потребуют этого» [17].

Поскольку в современных европейской и североамериканской социальных моделях именно человек является основной ценностью, соответственно государственные службы ведут сбор персональной информации исключительно в целях обеспечения безопасности граждан. В свою очередь, правозащитники убеждены в том, что это только одна из целей и на самом же деле государство ставит во главу угла установление тотального контроля над поведением населения.

Какую именно информацию собирают о гражданах

Ответ на поставленный вопрос на удивление прост - любую доступную информацию, в том числе извлекаемую при часто совершаемых операциях, таких, как оформление коммунальных платежей, подписки на газеты и журналы, благотворительные пожертвования, уплата налогов и сборов, переписка по электронной почте, покупка продуктов и т.д. и т.п. Из всех получаемых данных складывается немыслимо детальная картина жизни личности.

Для того чтобы хотя бы и косвенным образом представить масштабы сбора персональной информации в США, воспользуемся примером, приведённым Председателем высшей квалификационной коллегии судей России Валентином Кузнецовым в интервью газете «Газета». Касаясь проверки в США биографических данных кандидата на должность судьи, Кузнецов сказал: «ФБР представляет подробную информацию на кандидата в триста страниц. Они опрашивают его соседей, коллег, продавцов магазинов, где кандидат в судьи покупает одежду, официантов в ресторанах, где он обедает. Досье занимают целые тома» [18].

Сегодня возможности телекоммуникационных сетей используются для контроля над полнотой и своевременностью уплаты гражданами налогов [19], законностью нахождения в стране иностранцев [20] и решения многих других общенациональных проблем. То, что раньше могло вызывать негодование граждан, сталкивающихся с фактами грубого сбора информации о гражданах со стороны не слишком умелых чиновников, сегодня делается абсолютно незаметно и с большей эффективностью, поскольку базы данных позволяют накапливать неограниченные объемы информации и истребовать её практически мгновенно.

Кроме того, государственные и коммерческие структуры разрабатывают различные электронные системы позволяющие осуществлять контроль над передвижением граждан. К таким формам социального контроля относятся «электронные паспорта» [21], системы контроля местонахождения индивидов [22] и транспортных средств 23], не говоря уже об обширных базах данных, формируемых силовыми и налоговыми ведомствами. При этом контроль над передвижением акторов может осуществляться как на уровне отдельных территориальных образований, так и в масштабах страны.

К примеру, 19 августа 2003 года правительство Москвы утвердило программу по созданию «системы навигации и телематики для городского управления и населения». Власти собираются из космоса следить за работой городских служб, за передвижением транспорта и перевозкой грузов, а также за состоянием зданий и улиц. Основные декларируемые цели программы - повышение уровня безопасности населения и эффективности работы городских систем быстрого реагирования в условиях чрезвычайных ситуаций, улучшение качества транспортного обслуживания. Утверждается, что с помощью этой системы город получит

возможность с точностью до нескольких метров определять расположение стационарных и подвижных объектов, в том числе конкретных людей. Система спутниковой навигации и телематики будет внедрена в систему жилищно-коммунального хозяйства. Электронными маячками оснастят всех дворников, электриков, сантехников и других рабочих. Так диспетчеры смогут узнать о местонахождении каждого из них и, соответственно, снижать зарплату, если рабочий решил задержаться в какой-то из квартир после устранения неисправности. Датчиками оснастят коллекторы, трубопроводы и инженерные системы в жилых домах, а также чердаки и подвалы [24].

Так на практике происходит увеличение доступной государству информации о каждом из индивидов и... тем самым нарушения права на приватность (privacy) частной жизни. В экономически развитых странах компьютерные базы данных уже содержат значительные объёмы самой разнообразной информации о каждом из граждан. Соответственно знание коммуникативной истории человека и его генетических особенностей, даёт возможность манипулировать им на любом адекватном уровне.

В настоящее время только отказ от пользования глобальными компьютерными сетями может и то, лишь в частичной мере, уберечь актора от нахождения под наблюдением [25]. Подчеркнем, что в данном случае речь идет лишь о частичном освобождении от социального контроля. Дело в том, что государственные институты собирают данные на граждан и распространяют собранную информацию по своим сетям Интранет за счет сбора данных о налоговых платежах, финансовых транзакциях, наблюдения с помощью вэб-камер, анализа информации об акторе, распространяемой по компьютерным сетям его родными, знакомыми, сослуживцами, а также из иных источников.

Тот факт, что отпечатки пальцев каждого человека уникальны, правоохранительные органы используют для опознания преступников давно. Оказывается, форма лица, радужная оболочка глаза, манера речи - сугубо индивидуальны и могут быть использованы для установления личности. Использование компьютерных программ для определения внешних данных или особенностей поведения называется «биометрикой».

Однако именно громадные объемы информации в цифровой форме, которые окажутся потенциально доступными спецслужбам, служат гарантией отсутствия тотального контроля. Как говорят хладнокровные наблюдатели, тотальная перлюстрация частной корреспонденции была вполне возможна веке в XVIII, но вряд ли осуществима в веке XXI-м,

когда количество писем превысило любые мыслимые возможности силовых структур читать их.

Кроме технических аспектов, препятствующих полномасштабному анализу информационных потоков, существуют и накладываемые на процедуры хранения и обработки информации [26] экономические ограничения [27]. Вместе с тем необходимо отметить и тот факт, что указанные выше технологии могут поставлять наряду с объективной и сфальсифицированную информацию, доказать факт наличия которой весьма и весьма сложно ввиду «непрозрачности» самих систем сбора персональной информации.

Как это делается на практике

Использование автоматизированных систем сбора и обработки информации о гражданах не является прерогативой эпохи компьютеров. К примеру, уже в фашистской Германии существовала электромеханическая система, предназначенная для автоматизации хранения и обработки персональной информации обо всех гражданах страны. А в США общенациональные номера социального страхования были введены ещё в 1935 году и для обработки информации применялись электромеханические системы.

Уже в 2002 году в США началось создание глобальной системы анализа личной информации о гражданах этой страны [28], собираемой из всех доступных информационных источников. «В БД системы будут храниться сведения о банковских транзакциях, покупках в э-магазинах, водительских лицензиях, медицинских записях, э-переписке, путешествиях по Сети и любых других действиях, фиксируемых в компьютерных системах страны. В перспективе TIA призвана объединить все базы данных коммерческих и государственных структур, что позволит аналитикам выявлять типовые шаблоны действий, свойственные нарушителям законов, а ФБР - пользоваться этими шаблонами для дистанционной слежки» [29].

Согласно данных, полученных американским исследователем Е.С. Миллером (E.S. Miller), Федеральное бюро расследований США в рамках программы «Carnivore», ещё с середины 90-х годов XX века осуществляет слежку за электронными почтовыми отправлениями граждан своей страны. Автоматизированная система Carnivore, называемая также DCS1000, записывает все электронные коммуникации подозреваемого. Со

временем программа «Carnivore» стала контролировать не только электронную почту, но и интеракции, осуществляемые в чатах, электронные доски объявлений, а также коммуникативные взаимодействия, осуществляемые в одноранговых сетях [30]. Селекция информации в программе «Carnivore» ведется автоматически по ключевым словам.

С технической точки зрения, используемые при этом программные артефакты, относятся к «специализированным анализаторам» (сниферам). Такого рода программные артефакты используют не только спецслужбы, но и коммерческие компании, осуществляющие контроль над соблюдением внутренних правил коммуникативных взаимодействий или для администрирования сети.

При этом чаще всего анализируются источник коммуникативного послания, получатель и тип коммуникации (электронная почта, осуществление покупок через сеть Интернет и т.д.). Гражданский контроль над осуществлением программ социального контроля типа «Carnivore» фактически отсутствует, хотя в демократических странах должен быть частью государственного устройства. Тем не менее, возможности противодействия указанным технологиям существуют [31].

Существующие законодательные ограничения на сбор персональной информации фактически носят концептуальный характер и отнюдь не препятствуют разработке и реализации на практике тех или иных форм программных средств осуществления социального контроля в соответствующем масштабе. В частности, для мониторинга глобальных информационных потоков, специальные службы используют так называемые технологии «информационной проходки» (data mining) [32], а также их разновидности (text mining, audio mining, web mining и т.д.), позволяющие проводить отбор и предварительный анализ контента по ключевым сочетаниям символов или звуковым отпечаткам голоса [33].

Современные технологии «информационной проходки» основаны на переработке информации с целью поиска шаблонов (паттернов) неочевидных закономерностей, характерных для каких-либо фрагментов неоднородных многомерных данных. Эти технологии используются не только для осуществления социального контроля, но и в научных целях при решении задач по выявлению закономерностей в больших объемах информации.

Российский исследователь Сергей Арсеньев так описывает историю появления технологий «информационной проходки»: «В 1990-х годах

стали появляться первые программные продукты, позволявшие обрабатывать большие объемы исторических данных с целью извлечения из них ранее неизвестных, нетривиальных, практически полезных знаний, помогающих принимать правильные решения. Эти технологии углублённого анализа данных получили название data mining (букв. «добыча, разработка данных»). Интересно, что к моменту их появления уже был наработан почти весь необходимый математический аппарат. Data mining является синтетической областью, и в его основе лежат как статистика, так и принципы самообучающихся программ, эвристики. Все эти компоненты связаны в единое целое, дабы избавить людей от трудоёмких расчётов. Data mining предполагает значительную автоматизацию вычислений и передачу бизнес-аналитикам лишь тех тактических и стратегических вопросов, которые не могут быть решены без участия человека» [34].

Без использования указанных программных артефактов спецслужбы не способны были бы справиться с резко возросшими объемами эмпирических данных. Человеческий мозг не приспособлен для восприятия больших массивов разнородной информации и, в лучшем случае, индивид способен уловить две-три взаимосвязи даже в небольших выборках. Накопление данных за определенные периоды позволяет с помощью компьютерных систем проводить их ретроспективный анализ, направленный на выявление трендов и скрытых закономерностей в длинных временных рядах.

Вместе с тем необходимо отметить, что возможности технологий далеко не всегда позволяют выбрать необходимые данные из хаоса информации. Дело в том, что в настоящее время соотношение между неструктурированной информацией (прежде всего графических документов, текстов, звука, видео и т.д.) и структурированной информацией, то есть информацией представленной в цифровой форме составляет порядка 80:20 [35]. Безусловно, указанный факт затрудняет анализ уже имеющейся информации.

Россия: эволюция систем сбора персональной информации о гражданах

Сегодня в нашей стране 8 министерств и ведомств ведут сбор персональной информации о гражданах. Ранее разрозненные базы данных объединяются в общегосударственную интегрированную систему.

К примеру, в 2004 году МВД РФ планирует завершить создание единой интегрированной базы данных, в которую будут занесены все имеющиеся сведения о российских паспортах, когда-либо выдававшихся или считающихся утраченными на территории страны [36]. Таким образом, в ходе прошедшего обмена паспортов впервые в истории современной России была создана соответствующая федеральная база данных.

Министерство по налогам и сборам еще в 2002 году обнародовало информацию о возможностях созданного в недрах этого ведомства единого государственного реестра налогоплательщиков (ЕГРН). Реестр призван сделать налогоплательщиков абсолютно прозрачными для налоговых органов. Новое в системе – возможность оперативно получать графики взаимосвязей любых российских налогоплательщиков.

Любой налоговый инспектор, имеющий удаленный доступ к федеральной базе ЕГРН со своего рабочего места, сможет просмотреть все зафиксированные для заданного налогоплательщика дочерние структуры и пересечения учредителей, главных бухгалтеров, директоров и других сотрудников. Об ответственности сотрудников МНС за утечку конфиденциальной информации речи практически не идет.

Пока у МНС есть программы, рассчитанные на обработку только структурированной информации, то есть информации о налогоплательщике, имеющейся у налоговых органов. В будущем планируется разработать программное обеспечение, позволяющее обрабатывать неструктурированную информацию, то есть данные, полученные от сторонних организаций: загсов, таможенных служб, паспортно-визовых служб, коммунальных организаций и прочих владельцев баз данных, в которые включена информация о гражданах [37].

В настоящее время разработан проект Федерального Закона «О государственном регистре населения РФ». Государственный регистр населения, в котором будет содержаться многочисленная информация о гражданах, планируется формировать как территориально-распределенную базу данных. Так, в Государственный реестр включается следующая документированная информация: фамилия, имя, отчество; дата и место рождения; пол; гражданство; адрес места жительства; вид и реквизиты документа (наименование, серия, номер, дата и место выдачи); сведения об отце, матери, супруге и детях, включающие фамилию, имя,

отчество, дату и место рождения, гражданство; даты регистрации по месту жительства и даты убытия к другому месту постоянного проживания.

Уже сегодня в России существуют обширные базы данных генетической информации, а в Министерстве внутренних дел страны готовится проект закона о генетическом паспорте для идентификации личности. Новая технология идентификации личности основывается на том, что сочетание отрезков хромосомной спирали для каждого человека индивидуально [38]. Массовому внедрению технологии препятствуют лишь относительно высокая стоимость проведения анализов, доходящая до 100 долларов США.

Кроме того, создаются системы видеонаблюдения (видеослежки), информация с которых поступает в соответствующие спецслужбы. К примеру, в 2002 году все центральные вокзалы Москвы были оборудованы системами видеонаблюдения. Так, в середине 2002 года на Казанском вокзале функционировало 74 портативных телекамеры, на Курском - 68. С их помощью круглосуточно под наблюдением находятся все помещения - залы ожидания, кассовые залы, платформы, пути. Аналогичные системы планировались к установке на центральных вокзалах Курска, Орла, Брянска и Смоленска.

Еще один достаточно показательный пример. В Ростове-на-Дону в 2003 году на Главном железнодорожном вокзале была установлена новая цифровая система видеонаблюдения, включившая в свой состав 33 видеокамеры и 7 мониторов. Утверждается, что видеонаблюдение - антитеррористическая мера. Старая вокзальная система включала восемь аналоговых видеокамер и не позволяла записывать изображение, при этом с помощью этой системы не было выявлено ни одного преступника!.. Журналист Юлия Уракчеева пишет: «Новые цифровые камеры... умеют увеличивать изображение и фотографировать любого посетителя вокзала. Полученный портрет нетрудно проверить по базе данных милиции. Цифровые регистраторы запишут изображение на жесткий диск, чтобы хранить как минимум в течение недели» [39].

Указанные примеры массового внедрения систем видеонаблюдения можно приводить достаточно долго. При этом особую тревогу в вопросах защиты прав граждан на неприкосновенность частной жизни вызывают семь аспектов внедрения систем видеонаблюдения (видеослежки):

- обмен данными между разными системами видеонаблюдения;

· корреляция получаемой в процессе видеонаблюдения (видеослежки) информации с банками биометрических данных и отпечатков пальцев;

· использование систем распознавания голоса;

· внедрение систем, которые позволяют автоматически создавать изображения;

· использования систем идентификации по внешнему виду (эти системы могут автоматически относить человека к определенной категории по ряду внешних признаков);

· возможность автоматического определения маршрута следования и предсказания поведения человека в ближайшем будущем;

· принятие автоматических решений на основе информации, собранной о человеке [40].

В России информацию о гражданах собирали всегда и в отличие от западных стран еще пытались ограничивать доступ к соответствующим знаниям о технологиях социального контроля. Причем приведенный тезис относится не столько к временам СССР, а уже и к новейшей истории. Несколько лет назад даже делались попытки ввести официальный допуск к пользованию Интернетом и уголовную ответственность за несанкционированный выход в сеть, однако все ограничилось внедрением систем СОРМ.

Система оперативно-розыскных мероприятий на сетях документальной электросвязи (СОРМ) действует в России с тех же самых пор, с каких начал распространяться Интернет. Указ Президента РФ «Об упорядочении организации и проведения оперативно-розыскных мероприятий с использованием технических средств» № 891 был подписан 1 сентября 1995 г. Опубликовали же его в открытой печати только в 1999 г., когда особым распоряжением Президента с него был снят гриф «Для служебного пользования». Этим указом контроль почтовых отправлений, телеграфных и иных сообщений возлагается на ФСБ. В частности, в трехмесячный срок со дня подписания указа органам было предложено заключить соглашение «о порядке организации и проведения оперативно-технических мероприятий, связанных с подключением к станционной аппаратуре объектов связи». В применении к интернет-провайдерам это означает требование установить на их оборудовании технические средства контроля над передачей информации.

20 января 1997 г. ФСБ утвердила «Соглашение между Министерством связи Российской Федерации и Федеральной службой безопасности Российской Федерации по вопросу внедрения технических средств системы оперативно-розыскных мероприятий на сетях электросвязи России». Этим актом операторам связи (в частности, провайдерам) предписывалось «предусматривать поставку станционной части СОРМ и программного обеспечения, дополнительного оборудования для передачи данных между станционной частью СОРМ и пунктом управления ФСБ России». Значит, провайдеры сами, на собственные свои средства обязывались устанавливать прослушивающие устройства на аппаратуру — в противном случае им просто отказывали в выдаче лицензии.

Новые требования к обеспечению провайдерами канала прослушивания абонентов за свой счет стали называть СОРМ–2 в отличие от прежнего постановления, регулировавшего только доступ сотрудников ФСБ к аппаратуре. «Технические требования к СОРМ на сетях документальной электросвязи» были разработаны группой специалистов из Госкомсвязи России, ФСБ России, ЦНИИС и Главсвязьнадзора под руководством Ю. В. Златкиса и опубликованы летом 1998 г.

Такое положение дел узаконил и Приказ Минсвязи РФ от 25 июля 2000 г. № 130 «О порядке внедрения системы технических средств по обеспечению оперативно-розыскных мероприятий на сетях телефонной, подвижной и беспроводной связи и персонального радиовызова общего пользования», подписанный лично министром РФ по связи и информатизации Л. Д. Рейманом. Однако Приказ Минсвязи РФ от 25 октября 2000 г. № 185 «О внесении изменения в приказ Минсвязи России от 25.07.2000 № 130», действующий и по сегодняшний день, отменил правомочность важнейшего пункта предыдущего Приказа, пункта 2.6:

«2.6. Учитывать, что передача в правоохранительные органы информации об оказанных абоненту услугах связи осуществляется в порядке, определенном Федеральным законом «Об оперативно-разыскной деятельности».

Ответственность за соблюдение законности при организации и проведении оперативно-розыскных мероприятий в соответствии со статьей 22 Федерального закона «Об оперативно-розыскной деятельности» несут руководители органов, осуществляющих оперативно-розыскную деятельность.

Информация об абонентах, в отношении которых проводятся оперативно-розыскные мероприятия, а также решения, на основании которых проводятся указанные мероприятия, операторам связи не предоставляются».

Поспешное изменение нормативного акта было вызвано тем, что журналист из Санкт-Петербурга Павел Нетупский выступил с иском о его не конституционности. Верховный Суд России признал 25 сентября 2000 г. пункт 2.6 этого постановления незаконным. Теперь сотрудники ФСБ обязаны ставить провайдера в известность о том, чей именно интернет-трафик или телефонный разговор их интересует, а также предъявлять решение суда или санкцию прокурора на осуществление собственно прослушивания. Таким образом, бесконтрольного надзора со стороны ФСБ за всеми подряд российскими пользователями Паутины удалось избежать.

Таким образом, ФСБ добралось и до интернет-провайдеров. В частности, они могут потребовать с провайдеров обеспечить их возможностью контроля за любыми передаваемыми через них данными, в том числе и с помощью электронной почты. Не секрет, что в лицензиях провайдеров всегда присутствовала фраза: «Сеть должна отвечать эксплуатационно-техническим требованиям по обеспечению и проведению оперативно-розыскных мероприятий в соответствии с законом "Об оперативно-розыскной деятельности (ОРД) в РФ». Согласно официальным данным в нашей стране в 2001 году операторами связи было выявлено надзорными органами нарушений условий лицензии в части СОРМ 720 при общем количестве лицензий в 7969, а в 2002 году уже 1329 при общем количестве лицензиатов 9138 [41]. Таким образом, операторы связи в любой момент могут лишиться права заниматься предоставлением услуг связи, а значит, понесут невосполнимые убытки и потеряют возможность осуществлять свой бизнес. Вряд ли стоит комментировать то, как послушно операторы выполняют все требования контролирующих органов.

Марат Хайрулин пишет в «Новой газете»: «...когда заходит речь о системах СОРМ, бизнесмены из сферы высоких технологий утверждают, что их установка проводится совершенно безо всяких лицензий и соблюдения законодательных норм. Например, ранее, до введения в действие СОРМ-2, сотрудникам управления «Р» для прослушки того или иного сотового телефона нужно было прийти к оператору с санкцией. Так вот теперь этого совершенно не требуется - в смысле куда-то ходить.

Любая прослушка может осуществляться де-факто, напрямую, из хорошо всем известного здания на Ленинградском проспекте. Иди проконтролируй их: все засекречено, потому как борьба с терроризмом.

Прибавьте ко всем этим кошмарам ту программу, которую «эровцы» внедряют последний год всем крупным провайдерам. Программа эта призвана следить за всеми «мейлами». То есть если в вашем электронном послании затесалось нехорошее слово, то вы автоматически становитесь объектом пристального внимания со стороны управления «Р». И все, как всегда, без специального закона, без соответствующего думского обсуждения, тайком от собственных граждан» [42].

Коммерческие акторы, осуществляющие сбор персональной информации

Как уже отмечалось выше, сбор персональной информации о пользователе может осуществляться разным образом. Технические средства ИКТ для анализа поведение акторов в киберпространстве достаточно развиты. Акторами, заинтересованными в дальнейшем развитии социотехнических систем социального контроля, функционирующих в киберпространстве, являются:

- государственные структуры;
- коммерческие фирмы, осуществляющие разработку, производство и реализацию указанных систем;
- коммерческие фирмы, заинтересованные в сборе информации о посетителях тех или иных информационных ресурсов, размещенных в глобальных компьютерных сетях;
- руководители предприятий и организаций, в целях уменьшения непроизводительных потерь рабочего времени и непроизводительного использования телекоммуникационного оборудования и иные акторы.

К числу акторов, использующих на легитимных основания социотехнические системы контроля поведения пользователей в киберпространстве, могут быть отнесены: государственные структуры, которые в потенциале могут осуществлять абсолютный контроль на информационными ресурсами в киберпространстве, подпадающими под их национальную юрисдикцию, а также владельцы информационных

ресурсов в отношении принадлежащих им технических и программно-технологических артефактов.

В некоторых случаях, устанавливаемых соответствующими нормативными актами, владельцами социотехнические системы контроля, могут быть правообладатели объектов интеллектуальной собственности, чьи права нарушаются акторами, осуществляющие интеракции делинквентного характера (в качестве примера можно привести владельцам фонограммных и иных компаний, чьи произведения незаконно тиражируются и распространяются в глобальных компьютерных сетях). Таким образом, в вопросах контроля над поведением пользователей в киберпространстве интересы государства и интересы крупных монополий зачастую смыкаются.

Операции с персональными данными стали большим бизнесом как для ориентированных на получение прибыли фирм, так и для негосударственных организаций, включая политические партии. Тот факт, что во многих странах мира государственные институты не предпринимают мер по предотвращению сбора маркетинговыми компаниями информации о поведении в сети акторов, путем скрытого размещения на компьютере пользователей соответствующих файлов (cookies), является не просто нежеланием учитывать общественное мнение, но в первую очередь стремлением приучить большую часть пользователей к новой форме социального контроля. По оценкам экспертов, большой коммерческий потенциал в сетях сотовой связи имеют услуги контроля над месторасположением детей, получившие название семейных [43].

В целом ряде стран (Китай, Куба и др.) контроль над содержанием переписки в целях недопущения передачи по электронной почте антиправительственных и иных нарушающих закон сообщений, обязаны в соответствии с законом осуществлять провайдеры. Принятое 30 мая 2002 года решение Европейского парламента позволяет правоохранительным органам заниматься мониторингом электронной почты частных лиц.

С августа 2002 года в Великобритании вступил в силу закон, принятый еще в 2000 году, обязывающий компании-провайдеры телекоммуникационных услуг устанавливать слежку в Интернете за своими пользователями. Согласно закону, телекоммуникационные компании обязаны начать сбор данных о своем клиенте в течение 24 часов после извещения полиции о том, что органы правопорядка нуждаются в информации такого характера. Теоретически это означает

возможность сбора всей информации о человеке, доступной методами, аналогичными методам телефонного прослушивания. В настоящее время специальная аппаратура слежения позволяет установить круглосуточный контроль над одним из каждых десяти тысяч пользователей. Собранная информация обо всех интернет-адресах, которые посещались подозреваемым, электронных письмах и даже телефонных разговорах должна передаваться в правоохранительные органы.

Поскольку интернет-кафе могут использоваться в своих целях представителями криминальных сообществ, владельцы кафе по указанию властей организуют негласный контроль над деятельностью посетителей. С этой целью на предназначенных для общего доступа компьютерах устанавливаются специальные программы, которые отслеживают перемещение пользователя по виртуальному пространству, запоминают, какие тексты вводил посетитель с клавиатуры, а также блокируют доступ к сайтам определенных тематических категорий. А для того, чтобы однозначно идентифицировать личность посетителей интернет-кафе, может вводиться обязательная регистрация для всех посетителей с фиксацией паспортных данных [44].

Особый вопрос связан с регламентацией действий в киберпространстве сотрудников предприятий и организаций. Прежде чем служащему будет разрешен доступ в киберпространство, осуществляемый со служебных компьютерных терминалов, он должен выразить согласие соблюдать правила, регламентирующих те или иные действия.

Указанная норма имеет не только юридический смысл, но и служит профилактике делинквентного поведения - после знакомства с установленным порядком пользования компьютерными сетями, пользователи осознают, что все их действия регистрируются и за возможные нарушения к ним на законном основании могут быть применены дисциплинарные санкции. Исследования показывают, что сам факт декларирования социального контроля над коммуникацией сотрудников, резко снижает количество случаев нарушения трудовой дисциплины.

Контроль над перепиской по электронной почте может осуществлять как по решению руководства компании, так и быть обязательной мерой в соответствии с нормами национального законодательства [45]. В некоторых странах мира контроль над перепиской служащих не имеет политической или антикриминальной подоплеки, а является частью корпоративной культуры, нацеленной на

эффективное использование режима рабочего времени. Так, американцы с большой ответственностью относятся к контролю над использованием служащими своего рабочего времени, в том числе и за правильностью использования корпоративной электронной почты [46].

При этом контроль может осуществляться не только в отношении текстовых сообщений, но и в отношении характера пересылаемых графических файлов. С этой целью системный администратор заносит образцы разрешенных и запрещенных изображений в специальную базу образов, а компьютерная программа анализа сообщений электронной почты в процессе работы сравнивает передаваемые файлы с данными базы. Указанные возможности помогают блокировать передачу изображений, нарушающих политику безопасности, и защитить компанию от таких рисков, как утечка ее секретов, снижение производительности труда сотрудников и увеличение трафика электронной почты за счет несанкционированной пересылки графических файлов [47].

Как отмечалось выше, наряду со сбором информации спецслужбами, касающейся безопасности государства и общества, существует большое количество самых разнообразных акторов. осуществляющих сбор и классификацию так называемой «деловой информации» [48]. Такого рода информация, будучи обработанной, становится неоценимым активом для достижения коммерческих или политических целей.

К примеру, в США уже несколько лет рекламные щиты, установленные вдоль автодорог, оборудуются специальными устройствами, которые позволяют определить, какие радиостанции слушают проезжающие мимо автомобилисты. Существуют технические средства, позволяющие составлять всеобъемлющие досье о том, какие лекарства принимают люди, какую одежду носят, какие книги читают, какие продукты питания потребляют, а также о привычках и предпочтениях их детей.

Зачастую люди даже не знают о том, что в принадлежащих им вещах установлены системы наблюдения. Заранее принося извинения за слишком подробное объяснение, автор, тем не менее, считает необходимым проиллюстрировать приведенный тезис достаточно показательным примером. Многие люди слышали о самописцах, устанавливаемых в самолетах и вертолетах - так называемых «черных ящиках», записывающих данные за последние минуты полета

потерпевшего аварию воздушного судна. Эти аппараты сохраняют важную информацию, которая может помочь специалистам найти причину произошедшей катастрофы.

Но немногие знают о специальном модуле воздушной подушки, который устанавливается в миллионах легковых автомобилей и грузовиков, производившихся с девяностых годов прошедшего столетия корпорациями «Дженерал моторс» и «Форд». Модуль представляет собой компьютер, размером с пачку сигарет. Основное назначение этого модуля - управление работой, так называемой ограничительной системы, то есть системы безопасности срабатывания воздушных подушек и правильной работы ремней безопасности». При этом данные, записанные компьютерным модулем подушек безопасности автомобиля, могут служить в качестве доказательств со стороны обвинения в случае судебного разбирательства.

Компьютерный модуль подушек безопасности может следить и записывать различную информацию. Этот прибор фиксирует скорость автомобиля в момент аварии, его ускорение, а также сам факт столкновения. Прибор фиксирует также, в каком положении на момент аварии находилась педаль газа, использовал ли водитель тормоза, были ли пристегнуты ремни безопасности и так далее. Грамотные следователи не мудрствуя лукаво, просто подсоединяются к компьютерному модулю автомобиля и скачивают необходимую им информацию.

Подобные примеры нарушения права на неприкосновенность частной жизни даже в демократических странах не единичны. Гарриет Пирсон (Harriet Pearson), которая занимается проблемами неприкосновенности частной жизни в компании «Ай-Би-Эм» (IBM) на одной из пресс-конференций в 2000 году привела такой факт: компания «Ай-Би-Эм» работает с данными в 130 странах мира, многие из которых в эпоху Интернета не имеют даже элементарных законов о неприкосновенности частной жизни. «Ясно одно - никто не хочет никому причинить вред» [49], - продекламировала представитель одного из гигантов мирового компьютерного бизнеса.

Самое интересное, что на той же пресс-конференции, представитель одной из компаний венчурного бизнеса фактически не согласилась со столь простодушным подходом. Тара Лемми (Tara Lemmey), заявила, что ей часто приходится иметь дело с инцидентами, связанными с «утечкой данных». Утечка из той или иной компании конфиденциальной информации о ее клиентах нередко вызвана

«нежеланием думать». «Компании никогда не просчитывают всех последствий соблюдения прав на информацию и методов сбора информации», - сказала она. По словам Тары Лемми, вопросы, связанные с управлением данными, стали настолько сложными, что «всю картину целиком не может увидеть ни один человек» [50].

Практика сбора персональной информации и декларации политиков

В любой демократической стране задача закона, регулирующего функционирование средств связи, - создать надежную систему защиты таких естественных прав человека, как, скажем, право на неприкосновенность личной жизни, тайну переписки. И нельзя не признать, что такая система защиты в демократических странах давно разработана и уже давно действует.

Директива Европейской комиссии о неприкосновенности частной информации, вступившая в законную силу в 1998 году запрещает передачу персональных данных в не входящие в состав Европейского союза страны, не выполняющие европейский стандарт «адекватной» защиты частной информации. Ещё в 2000 году на страницах западной прессы появлялись статьи о принципиальных расхождениях во мнениях между США и Европейским союзом по вопросу о неприкосновенности частной жизни.

Евросоюз принял закон о неприкосновенности частной жизни, тогда как США предпочитают проводить политику отраслевого саморегулирования. В результате определенного компромисса в 2000 году Евросоюз принял предложенные США так называемые «директивы по защите данных». Эти директивы разъясняют, как американские компании решают проблему конфиденциальности получаемых из Европы данных, и носят добровольный характер. Европейские компании вправе отказаться вести дела с теми американскими компаниями, которые не придерживаются этих директив.

В США закон охраняет неприкосновенность персональных данных только в некоторых областях человеческой деятельности, к которым относится некоторые виды финансовой информации, а также информация, касающаяся здоровья. В Соединенных Штатах Америки фирмы и другие организации могут целенаправленно собирать информацию, чем они и занимаются, чтобы потом использовать ее вновь,

покупать и продавать, накапливать в компьютерных системах и обменивать.

От данных, которыми обладает, которые контролирует и хочет продать или обменять какая-либо американская компания, могут в действительности в значительной мере зависеть ее доходы и биржевая капитализация. А поскольку все это происходит легально, описанная здесь нами информация, касающаяся частной сферы, не имеет никакой правовой защиты.

В США государство ориентируется в этих вопросах на саморегулирование, осуществляемое бизнес-сообществом. Тремя важнейшими рекомендациями государства бизнесу являются: информирование, согласие и доступ. Однако это только рекомендуемые способы действий. Американское правительство лишь недавно приступило к изучению вариантов возможных законов о частной сфере.

Полной противоположностью этой практике является отношение к персональной информации в Европе. Европейское сообщество оказывало содействие политике защиты частной сферы, которая неукоснительно соблюдает неприкосновенность информации, касающейся личной жизни человека. Если дать самое простое определение, то отдельная личность в Европе автоматически считается обладателем всей информации, относящейся к ней самой, и любое использование этой информации возможно только в результате открыто одобренной и открыто санкционированной операции.

Серьезную опасность представляет и бесконтрольное распространение персональной генетической информации. Международная декларация о генетических данных человека была принята на в 2003 году на 32-й сессии Генеральной конференции ЮНЕСКО. В декларации отмечается, что процесс сбора информации о генах населения Земли необходимо подвергнуть строгому этическому контролю, чтобы избежать злоупотреблений. К сожалению, до практических действий в этом направлении еще далеко, а это означает, что распространение указанной информации в настоящее время находится вне правового поля.

Государственные структуры, ответственные за реализацию политики защиты права на неприкосновенность частной жизни

Исторически, борьба за защищенность информационных коммуникаций была начата, как это ни забавно, в Америке во время «сухого закона». Полиция прослушивала телефон одного из торговцев спиртным и на основе полученных данных построила свое обвинение. Алкогольный спекулянт обратился в суд, который признал правомочность действий полиции, поскольку почта ею не просматривалась. Именно на этом процессе судья Луис Брэндейс произнес свою знаменитую речь в защиту частной информации. В результате в 1934 году Конгресс США принял федеральный закон, признающий право на тайну коммуникаций «в полном объеме».

Соблюдению прав пользователей посвящено ряд директив ЕС, соответствующие правила оговариваются и в ряде общеевропейских договоров и хартий, например в Европейской хартии основных прав. Все страны - члены ЕС к 2002 году привели свои государственные законы в соответствие с нормами Директивы о конфиденциальности. В каждой стране, входящей в ЕС, сейчас действует комиссар по контролю над защитой личной тайны, а также национальное агентство с аналогичными функциями. Однако во многих странах работа агентств налажена плохо. Чиновники, которые должны контролировать соблюдение прав на конфиденциальность, чаще всего жалуются на отсутствие финансирования и на огромный объем работ [51].

В США до терактов 11 сентября 2001 года американское правительство мало вмешивалось в систему контроля над обеспечением прав граждан на конфиденциальность. Действия правительства в этом направлении ограничивались сферой финансовых услуг, информации, касающейся здравоохранения, и защитой частной жизни детей. Но уже тогда официальные лица заявляли, что участие правительства в решении этих вопросов будет расширяться.

Россия в 2001 году присоединилась к Конвенции о защите личности в связи с автоматической обработкой данных. Эта Конвенция является первым обязывающим международным инструментом, защищающим человека от несоблюдения прав, которое может сопровождать сбор и обработку персональных данных, и одновременно стремящимся регулировать передачу персональных сведений за границу.

Ограничения прав, заложенных в Конвенции, возможны только когда затронуты особо важные интересы (государственная безопасность, оборона и т. д.). Страны, подписавшие Конвенцию, обязались предоставлять гарантии в том, что касается сбора и обработки персональных данных, а также запрещать обработку данных о расе, политических взглядах, здоровье, религии, половой жизни и других сведениях без соответствующих юридических оснований. Конвенция также дает право человеку знать, что информация о нем или о ней хранится в соответствующих государственных организациях и, если необходимо, подкорректировать ее.

На практике же, Европейский Союз делает шаги к созданию общеевропейской идентификационной карточки. К 2008 году будут введены новые карточки с микрочипами, на которых будут записаны биометрические и персональные данные. Предполагается, что новая карточка будет по размеру такой же, как нынешние кредитные карточки.

Страховые медицинские полисы, которые сегодня присутствуют среди документов почти любого путешественника, уже в обозримом будущем будут заменены на единую карточку медицинского страхования (European Health Insurance Card). Впоследствии эта карточка заменит и другие документы медицинского характера, которые необходимо оформлять для проживания в других странах (не только для кратковременных поездок).

Первый этап программы начнется 1 июня 2004 года. Каждая страна может сама сделать выбор, будут ли на карточке записаны фотографии, отпечатки пальцев, биометрические данные (например, касающиеся радужной оболочки глаз). Вся эта информация будет размещаться на «национальной» стороне карточки, другая сторона будет общей. Вероятно, каждая карточка будет иметь встроенный микрочип.

О роли НКО в вопросах защиты неприкосновенности частной жизни

Говоря о роли НКО в вопросах защиты неприкосновенности частной жизни в первую очередь необходимо указать на две основные функции – просветительскую [52] и экспертную. Для осуществления просветительской функции необходимы знания существа происходящих процессов, навыки работы с масс-медиа и населением. Для реализации

экспертной функции необходимы специалисты высокой квалификации и источники информации.

Зарубежными правозащитниками в указанной сфере уже накоплен определенный опыт. Так, начиная с 1998 года, когда Privacy International (http://www.bigbrotherawards.org/) впервые выступила с идеей провести церемонию «Награды Большого брата», сложилась целая международная традиция присуждения «премий» нарушителям прав граждан на неприкосновенность частной жизни. К сегодняшнему дню в 15 разных странах прошло более 40 церемоний.

Правозащитные организации предупреждают, что объявленный властями США «крестовый поход против терроризма» и попытки усилить контроль над перемещением данных в Интернете существенно ограничат права простых людей и мало скажутся на деятельности экстремистов, полагающихся в основном на весьма примитивные способы передачи информации. Как утверждает Брайан Гладман, бывший технический директор НАТО, ныне - советник Фонда по исследованиям в информационной политике: «Мы готовимся к высокотехнологичной войне, но уже ясно, что террористы используют очень простые методы. В сети так мало закодированных сообщений, что любое применение кодировщиков сразу же становится заметным» [53].

Защитники сетевой свободы из групп Electronic Frontier Foundation и Electronic Privacy Information Center призывали своих сторонников давить на парламентариев с тем, чтобы не пропустить через конгресс США в спешке составленный закон о борьбе с терроризмом и им это удалось сделать. EFF указывает, что ФБР уже и так хватает полномочий для перехвата частных сообщений и слежки за гражданами. «Закон кардинальным образом изменит положение с гражданскими свободами за счет излишне широких ограничений на свободу слова и права на частную жизнь в США и за их пределами», - предупредил EFF {54].

Государство во всех странах с большим нежеланием допускает представителей общественности к какой-либо информации, касающейся функционирования специальных систем сбора информации о гражданах. ФБР под напором общественности решила разделить ответственность - с согласия Департамента юстиции США спецслужба передала свое детище на исследование нескольким независимым организациям, взяв с них подписку о неразглашении кодов программы. Вчера представители Иллинойского отделения Института технологических исследований заявили о том, что система автоматического прочитывания электронной

почты программы Carnivore делает именно то, что было объявлено представителями ФБР.

Не все правозащитные организации согласились с указанным выводом. Так, организация EPIC (Electronic Privacy Information Center - Центр по защите электронной информации), проанализировав новые результаты исследований, заявила о том, что намерения ФБР в данной области постоянно расширяются. Представитель EPIC заявил: «Заместитель директора ФБР сказал Конгрессу, что программа не может хранить не фильтрованные данные, но вот уже успешно испытывается система записи «сырой» информации. Оказывается, Carnivore гораздо мощнее, чем предполагалось» [55].

Участник EDRI, организация Privacy International, и юридическая фирма Covington & Burling опубликовали в 2003 году юридическое заключение, из которого следует, что обязательное требование хранить данные о клиентах (идея, популярная сегодня в ЕС) - незаконно. Речь при этом шла, прежде всего, о «рамочной» директиве ЕС об обязательном хранении коммуникационных данных.

В указанном юридическом заключении сказано: «Режим обязательного сохранения данных, предусмотренный Директивой, сегодня реализуется в разных странах - членах ЕС, однако этот режим незаконен. Статья 8 Европейской Конвенции о защите прав человека гарантирует каждому право на уважение его/ее частной жизни. Исключение делается лишь в некоторых случаях. Инициатива ЕС и последовавшие за ней изменения в национальных законах нарушают это право, так как режим хранения данных приводит к созданию информационных баз о действиях частных лиц. Это не что иное, как вторжение в частную жизнь каждого европейского пользователя коммуникаций и не укладывается в те «некоторые случаи», о которых идет речь в статье 8 Конвенции - она не соответствует закону и не является необходимой в демократическом обществе».

Далее в документе говорится: «Сбор данных о неопределенном круге лиц противоречит самым главным принципам: люди должны знать об условиях, на которых государство может вести слежку, с тем, чтобы они могли не совершать действий, создающих предпосылки для слежки. Более того, требование о хранении данных совершенно неадекватно задачам правоохранительных органов. Исходя из практики Европейского Суда по правам человека, такое непропорциональное вторжение в

частную жизнь не является необходимостью в демократическом обществе».

В резолюции 428 Консультативной Ассамблеи Совета Европы (раздел С), в которой сформулированы два правила:

· в случае противоречия между правом на свободу информации и на уважение частной жизни, приоритет отдается последнему;

· частная жизнь общественных деятелей должна защищаться, как и частная жизнь других граждан, за исключением случаев, когда она может оказать воздействие на общественно-значимые события.

Размах протестов общественности ограничивается тем, что отдельный гражданин знает об истинном объеме вторжения в свою частную сферу. Действующие ныне в Соединенных Штатах Америки законы практически не позволяют выяснить, что известно об индивидууме, кто владеет этой информацией, и как она, возможно, используется.

Не исключено, что уже в ближайшие годы мы станем свидетелями диктатур нового типа, основанных на квалифицированном использовании возможностей, предоставляемых новыми технологиями для целей политической коммуникации и социального контроля. К примеру, в Китае, как пишет французский автор Пьер Аски (Pierre Haski): «Охота на интеллектуалов, публикующих в Интернете призывы к политическим реформам, идет полным ходом. Эта невидимая борьба между демократической интеллигенцией и «киберполицией», постоянно совершенствующей свои методы, контрастирует с экономической открытостью и либеральным имиджем, который хочет обрести китайский режим. Китай, активно развивающий информационные технологии, стоит на первом месте по количеству осужденных за интернет-публикации» [56].

Вместе с тем практика свидетельствует о том, что всякий раз, когда режим внедряет в практику работы спецслужб новый метод технического контроля, какие-нибудь хакеры или «хактивисты» взламывают соответствующие системы или находят иные способы противодействия в течение весьма непродолжительного времени. Кроме того, существует огромное количество кодирующих программ. Под контролем остаются только несведущие в технологиях граждане.

Ответственность за обеспечение сохранности персональной информации

Во всех нормативных актах говорится об ответственности государства за утечку и неправомерное использование персональных данных. Однако на практике государство практически не несёт никакой ответственности за возможные утечки персональной информации. В демократических странах в условиях рыночных отношений возникает проблема краж компьютерных баз данных, содержащих персональную информацию, с целью дальнейшего коммерческого распространения информации, собранной государственными (муниципальными) организациями и бизнес-структурами.

Анатолий Левенчук, координатор московского правозащитного проекта «Московский Либертариум», главным недостатком концентрации баз данных в руках государства считает опасность злоупотребления со стороны государственных чиновников частной информацией, которая будет собрана в одну базу данных. «Нет оснований считать, что чиновники - более честные люди, чем все прочие, - говорит Левенчук. - Мы сегодня часто видим, что базы данных частных компаний можно купить на рынках» [57].

Поскольку правовой режим, к примеру, телефонно-адресных баз данных, практически ни в одной стране мира не определён и этим в своих интересах пользуются лица, исповедующие идеологию девиантного поведения. Приведём несколько примеров, связанных с российской действительностью. В мае 2001 года из челябинского центра СПИДа была украдена база данных на всех ВИЧ инфицированных Южного Урала. Медики высказывали опасения в отношении возможности использования в корыстных целях полученной преступниками информации. В мае 2003 года газета «Коммерсантъ» писала о том, что неизвестными лицами распространяются компакт-диск с информацией по состоянию на конец 2002 года о четырех с половиной миллионах абонентов компаний сотовой связи Санкт-Петербурга. В предлагавшейся преступниками базе данных был возможен поиск по номеру телефона, фамилии абонента, номеру его паспорта, прописке и по контактным телефонам [58].

По электронной почте совершенно открыто предлагается, в частности, база данных по всем экспортно-импортным операциям, осуществленным в России в 2002 году. Речь при этом идет о полной информации, содержащейся в грузовых таможенных декларациях: данные

о покупателе, поставщике, коде товара по ТН ВЭД, количестве, массе, стоимости, номере ГТД, дате сделки, банках обслуживающих сделку, таможенном терминале и т.д. (около 100 полей декларации).

Подобные примеры можно приводить достаточно долго, гораздо важнее тот факт, что, несмотря на пиаровские акции по задержанию «оборотней» в погонах, практически никто из допущенных к конфиденциальным базам данных чиновников не был задержан. И это притом, что похищенные базы данных могут использоваться и во вред интересам государства, путём воздействия на чиновников, ответственных за принятие тех или иных решений. К примеру, имеют место случаи социального протеста в форме сбора персональных данных и их дальнейшего разглашения с целью проявления несогласия с планами правительства по предоставлению специальным службам свободного доступа к персональной информации граждан.

Так, в США двое исследователей из Массачусетского технологического института, обеспокоенные созданием правительственной системы тотального слежения TIA (Total Information Awareness, служба Тотального информационного мониторинга), разработали интернет-сервис, позволяющий вести досье на государственных чиновников. На сервере www.opengov.media.mit.edu публикуется общая информация о чиновниках. После этого любой пользователь глобальных компьютерных сетей сможет добавлять к этой информации известные ему сведения, результаты наблюдений за официальными лицами. Причем достоверность публикуемой информации проверяться не будет. Новая служба получила название Службы мониторинга действий правительства (Government Information Awareness, GIA). Принцип работы программных артефактов, используемых в проекте GIA аналогичен принципам работы интернет-служб индексирования поисковых машин. Кроме того, специальная компьютерная программа передает на сервер проекта изображения политиков, появляющихся на одном из кабельных телеканалов. Щелкнув на таком изображении, любой пользователь сможет получить о чиновнике всю необходимую информацию [59].

Еще один пример. Журналист газеты «San Francisco Weekly» Мэтт Смит (Matt Smith) в одном из своих материалов в 2002 году опубликовал личную информацию Джона Пойнтдекстера (John Poindexter), разработчика программы тотальной слежки в США. Пойндекстер работал директором Управления по сбору информации Агентства перспективных

исследований Министерства обороны (Information Awareness Office) [60]. Опубликованная информация включала домашний телефон чиновника и фотографии его дома в штате Мэриленд. По утверждению журналиста, вся эта информация была получена им из открытых источников. Смит заявил, что таким образом он хотел продемонстрировать несогласие с планами правительства дать секретным службам свободный доступ к персональной информации граждан. «Пойнтдекстер намерен собирать данные о простых американцах, затем эта информация, вероятнее всего, попадет и к другим организациям, которые станут использовать ее в своих интересах, почему бы не повернуть эту систему против него самого?, - сказал Смит, - К тому же, это даст возможность моим читателям еще раз задуматься над обсуждаемой проблемой» [61].

Приведенные примеры показывают не только масштабы распространения систем социального контроля, отсутствие на практике ответственности чиновников за ее несанкционированную утечку, объемы собираемой спецслужбами персональной информации, но и возможности баз данных как для борьбы с коррупцией, так и для шантажа тех, кто на практике готов противостоять коррупционным проявлениям.

Вместо заключения

Для оправдания усиления социального контроля, государством (как субъектом организации социального контроля), используется различная аргументация, однако чаще всего разговор идёт о необходимости усиления безопасности граждан. Выдающийся американский политический деятель Франклин Делано Рузвельт в свое время пророчески заметил: «Люди, отказывающиеся от свободы в пользу безопасности, недостойны ни того, ни другого».

P.S. В соответствии с п.2. ст. 23 Конституции РФ каждый имеет право на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений. Нарушение этого принципа возможно только на основе мотивированного решения суда.

---

1. Kovel J. Against the State of Nuclear Terror. -L.: Pan. 1983. P. 76.

2. Bentham J. Works. (Eds). Bowring. -Endinburgh: William Tait. 1843.

3. Foucault M. Discipline and Punish: The Birth of the Prison. - Harmondsworth: Penguin. 1979. P. 250.

4. Leigh D. The Frontiers of Secrecy: Closed Government in Britain. -L.: Junction Books. 1980. P. 218.

5. Маркузе Г. Эрос и цивилизация. Одномерный человек: Исследование идеологии развитого индустриального общества. / Пер. с англ. -М.: ООО «Издательство АСТ», 2002. С. 9. Выходные данные оригинального издания на английском языке: Marcuse H. Eros and Civilization. -N.Y.: Vintage, 1955.

6. К примеру, в США в штате Южная Каролина действует закон «Об образовательных стандартах». Местные законодатели внесли в него пункт, который обязывает компьютерных специалистов, занимающихся ремонтом компьютеров и поддержкой их систем, сообщать в полицию о случаях обнаружения детской порнографии на компьютерах своих клиентов.

7. Если в западных странах уважение к частной жизни как элемент политической культуры имеет относительно большую историю, то в странах с переходными экономиками (к которым относится и Россия), государство не привыкло считаться с правами личности. Соответственно, социальные ценности уважения к неприкосновенности частной жизни, ещё только должны быть закреплены в законе, морали и в общественном сознании.

8. Достаточно широко известна своеобразная форма выражения философского концепта «отрицание отрицания» по отношению к социальному контролю поведения индивида: «Если у вас паранойя, это не значит, что за вами не следят».

9. Панишев А. Глобальная слежка: человек под прицелом // ПЛ Компьютеры, 2001, № 10. С. 48-58.

10. См. Levy S. Hackers: Heroes of the Computer Revolution. -N.Y.: Penguin. 2001.

11. См. Rohm W.G. The Microsoft File: The Secret Case Against Bill Gates. -N.Y.: Random House. 1998.

12. См. Schwartau W. Information Warefare: Cyberterrorism: Protecting Your Personal Security in the Electronic Age. -N.Y.: Thunder's Mouth Press. 1996.

13. См. Sunstein C.R. Republic.com. -New Jersy: Princeton University Press. 2001.

14. Цит. по: Ортега-и-Гассет Х. Восстание масс. / Ортега-и-Гассет Х. Избранные труды. Пер. с исп. / Сост., предисл. и общ. ред. А.М. Руткевича. 2-е изд. -М.: Издательство «Весь мир», 2000. С. 116.

15. Цит. по: Eaglesham J. Companies free to snoop on staff // Financial Times, 2000, 3 October.

16. Цит. по: Kurata P. Privacy Intrusions Seen to Threaten Growth of E-Commerce (Former Commerce official warns against over-regulation) // Washington File, 2000, 29 September.

17. Фиксимер Р. Смиритесь: национальные идентификаторы на подходе // PC WEEK RE, 2002, № 7 (325). С. 22.

18. Цит. по: Михайлина Ю. Кандидатов в судьи проверяют милиция и ФСБ. Председатель высшей квалификационной коллегии судей Валентин Кузнецов - ГАЗЕТЕ // Газета, 2003, 21 июля.

19. Возможности созданного в 2002 году Министерством по налогам и сборам России единого государственного реестра налогоплательщиков позволяют собрать данные о финансовой деятельности всех физических и юридических лиц страны.

20. В США действует режим обязательной передачи таможне данных о пассажирах, прибывающих в эту страну, включая религиозную

принадлежность, предпочтения в еде, номера кредитных карточек и т.д. А с июля 2002 года в этой стране внедрена информационная система контроля над студенческими обменами и приезжающими студентами (Student Exchange and Visitor Information System, SEVIS). С помощью этой системы около учебные заведения страны передают по сети Интернет в Службу иммиграции и натурализации США (INS) данные о своих иностранных студентах в случае, если те не смогли поступить в ВУЗ, покинули его или были отчислены. Вопрос достоверности информации о лицах, въезжающих в США по учебным визам, приобрел актуальность после терактов 11 сентября 2001 года. В ходе их расследования выяснилось, что один из угонщиков самолетов, Хани Ханжур (Hani Hanjour) для въезда в Америку воспользовался студенческой визой. Официально он находился в США с целью изучения английского языка, однако в школе, где проходили занятия, ни разу не появлялся.

21. К примеру, в Бирме в августе 2002 года была введена система электронных паспортов. Уже существующие бумажные паспорта снабжаются микрочипами, на которых записывается информация о владельце паспорта, в том числе его фотография и отпечатки пальцев, представленные в цифровой форме. Правозащитники опасаются, что власти используют систему, чтобы следить за оппозиционными лидерами.

22. Так в США в середине 2002 года в продажу поступили детские наручные часы, в которые встроена миниатюрная версия приемника системы глобального позиционирования GPS. «Персональный локатор» - так называется это устройство - разработано компанией Wherify Wireless. Он позволяет родителям всего за минуту узнать, где именно находится их ребенок. Контроль над процессом передвижения ребенка осуществляется с использованием сети Интернет и спутниковых технологий.

23. В качестве примера приведем Великобританию. Британское правительство намерено к 2006 году ввести систему спутникового слежения и оплаты за пользование дорогами для 450 тысяч иностранных грузовых автомобилей, въезжающих в страну, а для всех британских автомобилей - еще через несколько лет. Работа предложенной системы слежения основана на технологии, которая уже давно используется для определения местоположения автомобилей и судов с помощью искусственных спутников Земли. Новое - это ее массовое и при этом

обязательное применение. На каждом из 26 миллионов автомобилей в Британии предполагается установить специальный датчик - прикрепляемый к ветровому стеклу небольшой «черный ящик» с микрочипами, находящийся в постоянном радиоконтакте со спутником. Система может точно устанавливать, где именно находится автомобиль и, сколько он проехал за время поездки. Кроме этого компьютерная система позволит собирать и обрабатывать информацию о маршрутах поездок практически каждого владельца автомобиля. См. Костин В. Платить за дороги заставит спутник // Сайт Би-Би-Си, 2002, 27 июля, http://news.bbc.co.uk/hi/russian/sci/tech/newsid_2156000/2156522.stm.

24. См. Голунов И. Столичные власти будут следить за Москвой из космоса // Газета, 2003, 20 августа.

25. Международные террористы предпочитают пользоваться неэлектронными средствами связи. К примеру, в Афганистане сторонники Усамы бин Ладена обменивались посланиями через конных курьеров, несмотря на то, что имели возможность использования спутниковых телекоммуникационных каналов связи.

26. По данным на начало 2003 года сбор и хранение информации о поведении пользователей в глобальных компьютерных сетях обходился в 700 тысяч долларов за каждый терабайт собранных данных.

27. Речь идёт как об использовании специального программного обеспечения и специализированных протоколов передачи данных. Так, вместо TCP возможно использование протокола UDP, трафик которого трудней отследить. Кроме того, возможно использование протоколов шифрования данных. И хотя приведённые два способа известны специальным службам (и, кстати, вовсе не гарантируют анонимности), однако процесс осуществления социального контроля в компьютерных сетях они до определенной степени затрудняют и удорожают.

28. Программа, поначалу получившее название TIA (Total Information Awareness) впоследствии была трансформирована в программу Terrorism Information Awareness. (Смена названия программы произошла из-за смутившего многих слова Total). А законопослушным гражданам бояться, честное слово, совсем нечего, потому что цель TIA вовсе не

повальная слежка, а строго наоборот - слежка выборочная. Протесты Американского союза за гражданские права были услышаны, и отныне инструментарий TIA запрещено применять на американцах. Программа, утверждают официальные лица, задумана как инструмент идентификации террористов, для чего предполагается постоянное перелопачивание многих терабайт информации в поисках подозрительных транзакций, имен, обстоятельств, переговоров и прочего. Terrorism Information Awareness задумана и воплощается агентством DARPA (Defense Advanced Research Projects Agency - Агентство перспективных оборонных исследовательских разработок) - учреждением, породившим компьютерные сети.

29. Бобровский С. США начинают охоту на ведьм // PC WEEK RE, 2002, № 44. С. 47.

30. См. Miller E.S. Civilizing Cyberspace: Policy, Power and the Information Superhigway. -N.Y.: ACM Press. 1996.

31. Возможность блокирования социального контроля, осуществляемого такими системами реальна, к примеру, на это в своей статье обращает внимание Ричард Форно. См. Форно Р. Кому страшен Carnivore? // Компьютерра, 2000, № 28 (357). С. 34-35

32. Читателей, интересующихся более подробно технологиями «цифровой проходки» автор отсылает к работе: Дюк В., Самойленко А. Data Mining. -СПб: Питер, 2001. -386 с.

33. В данном случае речь идёт о том, что полученный однажды тем или иным образом «звуковой отпечаток» голоса вводится в компьютерные базы данных и впоследствии может быть использован, в частности, для идентификации пользователей, пользующихся средствами IP-телефонии.

34. Цит. по: Арсеньев С. Data mining - не панацея // Компьютерра, 2003, № 37 (512). С. 24 - 25.

35. См. Колесов А. Извлекая знания из хаоса информации // PC WEEK RE, 2003, № 43 (409). С. 40.

36. МВД России создает единую базу паспортов // Русский курьер, 2003, № 155, 25 ноября. С. 1.

37. Для реализации планов нужны немалые средства. Поэтому в 2004 г. на реализацию проектов в сфере информатизации Всемирный банк выделит $150 млн МНС РФ и $140 млн - ГТК РФ. Займы будут предоставлены под гарантии Правительства России.

38. Важно отметить и тот факт, что Россия в этом отношении повторяет путь западных стран. Так, информационные банки ДНК военнослужащих в США и европейских странах создавались еще в начале 90-х годов.

39. Уракчеева Ю. 33 глаза Главного вокзала. За людьми на перронах будут наблюдать видеокамеры // Новая городская газета, 2003, № 44 (324). С. 6.

40. Указанная проблематика в 2003 году была впервые в полном объеме рассмотрена европейскими уполномоченными по защите данных, объединенными в рабочую группу под условным названием «Article 29». Группа занималась анализом различий в законодательстве и правоприменительной практике стран-членов ЕС, возникших в период после принятия Директивы о приватности (95/46/ЕС).

41. Бугаенко В.Н. Государственный надзор за связью и информатизацией в Российской Федерации // Федеральный справочник «Связь и информатизация в России, 2002-2003 годы», 2003. С. 329.

42. Хайруллин М. Мышка-наружка // Новая газета, 2003, 10 ноября.

43. См. Николаев В. П. Позиционирование подвижных объектов в сотовых сетях: услуги и проекты // Технологии и средства связи, 2002, № 3 (30). С. 38-42.

44. Так, учёт паспортных данных посетителей интернет-кафе с 2003 года официально осуществляется в Белоруссии.

45. В США обязательному хранению подлежит переписка по электронной почте сотрудников администрации Президента. Кроме того, в соответствии с решением Комиссии по ценным бумагам (SEC) финансовые компании США обязаны хранить электронную переписку сотрудников. Меры за нарушение данного правила предусмотрены довольно жесткие. Так, в середине 2002 года за не сохранение электронной переписки были оштрафованы крупнейшие американские компании: Merrill Lynch, Goldman Sachs Group, Citigroup unit Salomon Smith Barney, Morgan Stanley, Deutsche Bank, Piper Jaffray. Сумма штрафа с каждой компании составила по 1,67 млн. долларов. См. Financial firms face fine for lost e-mail // Reuters, 2002, 2 August.

46. К примеру, в апреле 2002 года шесть государственных служащих в Вашингтоне (США) были уволены из-за неправильного использования электронной почты. Провинившиеся позволили себе через принадлежащие государству компьютерные системы отправлять электронные письма, содержащие вульгарные шутки, эротические фото и даже оговаривали планы оргий. В ходе тайного анализа 2700 почтовых аккаунтов, принадлежащих одной из государственных структур, были выявлены сотни нарушений инструкций по использованию корпоративной электронной почты. Цит. по: Washington State Fires Six for Racy E-Mails // Reuters, 2002, 26 April.

47. В качестве примера можно привести систему анализа сообщений электронной почты MAILsweeper for SMTP британской компании Clearswift (http://www.clearswift.com).

48. Burnham D. The Rise of the Computer State. -N.Y.: Random House. 1983.

49. Цит. по: Kurata P. Privacy Intrusions Seen to Threaten Growth of E-Commerce (Former Commerce official warns against over-regulation) // Washington File, 2000, 29 September.

50. Там же.

51. Викерс Б. Без права на конфиденциальность. Европейцам труднее спрятаться в Интернете, чем американцам // Ведомости, 2001, 15 февраля.

52. В качестве примера просветительской деятельности приведем деятельность общественной правозащитной организации из Санкт-Петербурга «Гражданский контроль», а также выпущенной в 2002 году межрегиональной группой «Правозащитная сеть» брошюру Сергея Смирнова. См. Смирнов С. Приватность. -М.: «Права человека», 2002. -96 с.

53. Права или спокойствие? // Всемирная служба Би-Би-Си, 2001, 21 сентября.

54. Права или спокойствие? // Всемирная служба Би-Би-Си, 2001, 21 сентября.

55. Латкин А. Сугубо научный взгляд. Ученые одобряют действия спецслужб // Известия, 2000, 23 ноября. С. 6.

56. Haski P. Cyberrйpression en Chine. Des internautes sont arrktйs pour avoir rйclamй des rйformes // Liberation, 2003, 06 novembre.

57. Цит. по: Дорохов Р. «Умные» паспорта // Ведомости, 2003, 11 июня.

58. См. Горлин Б. Вот это номер! В Петербурге украли базы данных всех телефонных операторов//Коммерсантъ, 2003, № 85 (2688). 20 МАЯ

59. См. Website turns tables on government officials // The Boston Globe, 2003. 04.07. Программа TIA была лишена финансирования из бюджета США в сентябре 2003 года.

60. Сайт Агентства в сети Интернет - http://www.darpa.mil/iao. Примечание: для пользователей из России указанный сайт не доступен.

61. Цит. по: Boutin P. Keeping Track of John Poindexter // Wired, 2002, 14 December.