М.В. Бундин

ОПЫТ ПРАВОВОГО РЕГУЛИРОВАНИЯ ПРАВА НА ЧАСТНУЮ ЖИЗНЬ И ПЕРСОНАЛЬНЫХ ДАННЫХ В СОЕДИНЕННЫХ ШТАТАХ АМЕРИКИ

Аннотация. *В статье анализируется опыт США в области защиты права на неприкосновенность частной жизни и защиты персональной информации. Исследуются содержание и исторические предпосылки принятия основных нормативно-правовых актов федерального законодательства, регулирующих вопросы защиты частной жизни и персональных данных, обрабатываемых федеральными государственными органами, а также практика Верховного Суда. Делается вывод о существовании уникального «американского» подхода к защите персональных данных, в сравнении с «европейской моделью», основанной на положениях Директивы ЕС 95/46/ЕС, которая также легла в основу российского законодательства о персональных данных. Формулируются достоинства и недостатки «американского» подхода.*

Ключевые слова: *сравнительное правоведение, права человека, зарубежное законодательство и практика, информационные системы персональных данных, персональные данные, право на неприкосновенность на частной жизни, информационная безопасность личности, компьютерные технологии, оператор данных, конфиденциальность*

США уже давно известны, как страна, где право на уважение частной жизни получило широкое признание, учитывая также, что и сам термин «частная жизнь» или «право на частную жизнь», во многом, появились, как интерпретация термина «right to privacy», введенного в употребление американскими юристами еще в 1890 году. Именно в этом году американские адвокаты Самуэль Уоррен и Луи Брандейс опубликовали в журнале Harvard Law Review статью «The Right to Privacy»[1], в которой обосновали необходимость судебной защиты частной жизни от вторжения подобно тому, как защищается доброе имя от клеветы и навета. В течение долгого периода американской истории, именно понятие «privacy» (прайваси) — становится ключевым словом-концептом для всей американской системы права. Первоначально данная концепция затрагивала лишь достаточно ограниченные аспекты частной жизни, подлежащие защите на основании текста 4-ой поправки к Конституции США, однако, благодаря гибкости и уникальным способностям к «адаптации» американского конституционного права количество правомочий постоянно возрастало. В частности, термин «прайваси» эволюционировал от защиты права на неприкосновенность жилища и тайны переписки до защиты телефонных переговоров, электронных и иных сообщений, т.е. до так называемых «privacy rights» — дословно «права на частную жизнь» (речь идет о целой группе правомочий, охватываемых или включаемых в право на частную жизнь). Аналогичные мнения высказываются и российскими авторами, которые часто в понятие «право на частную жизнь (неприкосновенность частной жизни)» вкладывают целый спектр различных правомочий[2].

Развитие компьютерных технологий обработки информации, где США является одним из бесспорных лидеров в настоящее время, привело к неизбежному вопросу о необходимости защиты «права на частную жизнь», в условиях автоматизированной обработки информации о физических лицах в электронных базах данных. Такой феномен получил в США свое название — «electronic privacy», и на сегодняшний момент он является объектом пристального изучения[3]. Следует отметить, что такого понятия как «персональные данные» или (personal data), которое получило широкое распространение во многих англоязычных странах,

[1] Brandeis Louis & Warren Samuel," The Right to Privacy," // 4 Harvard Law Review 193-220 (1890-91). [Электронный ресурс] URL: http://faculty.uml.edu/sgallagher/Brandeisprivacy.htm (дата обращения: 15.01.2012).

[2] См., к примеру: Бачило И.Л., Лопатин В.Н., Федотов М.А. Информационное право. СПб.: Изд. «Юридический центр Пресс», 2005. С. 220; Головкин Р.Б. Правовое и моральное регулирование частной жизни в современной России: Дис. ... д-ра юрид. наук: 12.00.01 Н.Новгород, 2005. С. 117; Баранов В.М. Категория «частная жизнь» // Право граждан на информацию и защита неприкосновенности частной жизни. Н.Новгород, 1999. С. 34-37.

[3] См. об этом сайт Информационного центра компьютерной прайваси (Electronic Privacy Information Center). [Электронный ресурс]: URL: http://epic.org (дата обращения: 15.01.2012).

таких как Великобритания[4], Австралия[5], Канада[6] в законодательстве и практике в США не используется. Для обозначения данных в самых различных случаях применяется термин «record»[7], который можно интерпретировать как «запись/файл», содержащие информацию об индивиде (в основном, по-видимому, идет речь о сведениях, сохранившихся после взаимодействия органа публичной власти и индивида).

Для изучения вопроса о защите частной жизни индивида в условиях развития новых компьютерных технологий Департаментом здравоохранения, образования и социальной защиты (Department of Health, Education and Welfare) была создана специальная комиссия, которая еще в 1973 году в своем докладе обратилась к Конгрессу с рекомендациями по принятию специального законодательства — Кодекса честной информационной практики (Code of Fair Information Practice)[8], основанного на следующих принципиальных положениях:

– отсутствие баз персональных данных, существование которых скрывается или является секретным;
– предоставление индивиду права знать какая информация содержится о нем в базе данных и как она используется;
– предоставление права индивиду воспрепятствовать использованию информации, полученной с определенной целью, в других целях, или передаче другим лицам без его согласия;
– индивид должен иметь право требовать внесения изменений, исправлений или дополнения информации о нем, в случае ее недостоверности;
– организация, осуществляющая создание, поддержание, использование и распространение персональных данных должна обеспечить достоверность персональных данных, а также принять меры к предотвращению их ненадлежащего использования.

Кроме этого в специальном докладе рекомендовалось для организаций, ведущих обработку персональной информации, осуществлять защиту последней, а также ежегодного опубликовывать сведения о базах данных и информации в них содержащейся. Следует отметить близость этих принципов с принципами, закрепленными в ряде европейских документов, таких как Конвенция Совета Европы о защите личности в связи с автоматизированной обработкой данных[9] или Директива Европейского парламента и Совета ЕС 95/46/ЕС[10], принятых существенно позднее.

Большая часть положений доклада легла в основу дальнейшего развития законодательства о частной жизни и защите данных, которое в США значительно отличается для публичного и частного сектора экономики. Наиболее урегулированными признаются отношения связанные с защитой персональной информации в публичной сфере на основе принятого в 1974 Акта о защите частной жизни (The Privacy Act — далее Акт)[11], ставшего одним из первых в своем роде.

Главной отличительной особенностью этого документа является сравнительно узкая сфера его действия. В первую очередь он затрагивает исключительно обработку персональной информации о гражданах и постоянных резидентах правительственными агентствами США, на которую распространяется требования «честной информационной практики». Исключение составляют положения 7 раздела, относимые также к деятельности властей штатов и местных органов власти. С другой стороны Акт применим в равной степени как к исполнительным органам власти (исполнительным правительственным агентствам), так и к органам управления вооруженными силами (военным агентствам), а также к независимо управляемым агентствам и к контролируемым государством корпорациям. Следовательно, в этом ряду можно упомянуть не только «типичные» правительственные агентства, такие как, например, Департамент образования или здравоохранения, но и вооруженные силы, Федеральное бюро расследования (ФБР), а также Почтовую службу Соединенных штатов. Не являются исключением в этом ряду Конгресс и Канцелярия Президента Соединенных Штатов. В дополнении к этому сферу действия Акта сужает и его применение только к «системам записей» («systems of records» — т.е. к информационным системам, содержащих персональную информацию), которые позволяют получить доступ к файлу с персональной информацией по имени лица или другого персонального идентификатора.

---

[4] Data protection Act of 1988 [Электронный ресурс]: URL: http://www.opsi.gov.uk/acts/acts1998/ukpga_19980029_en_1 (дата обращения: 15.01.2012).

[5] Privacy Act of 1988 [Электронный ресурс]: URL: http://www.austlii.edu.au/au/legis/cth/consol_act/pa1988108/ (дата обращения: 15.01.2012).

[6] Privacy Act [Электронный ресурс]: URL: http://www.statcan.ca/english/about/privact.htm (дата обращения: 15.01.2012).

[7] См. об этом The Privacy Act of 1974 [Электронный ресурс]: URL: http://www.usdoj.gov/oip/privstat.htm (дата обращения: 15.01.2012).

[8] [Электронный ресурс]: URL: http://epic.org/privacy/consumer/code_fair_info.html (дата обращения: 15.01.2012).

[9] Конвенция Совета Европы о защите личности в связи с автоматизированной обработкой данных от 28 января 1981 г. [Электронный ресурс]: URL: http://conventions.coe.int/Treaty/EN/Treaties/Html/108.htm (дата обращения: 15.01.2012).

[10] URL: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:NOT (дата обращения: 15.01.2012).

[11] URL: http://epic.org/privacy/consumer/code_fair_info.html (дата обращения: 15.01.2012).

На основании положений Акта, субъекту данных (любому физическому лицу) предоставляется право на доступ к информации о нем, при этом он вправе ознакомиться с ней и делать копии, а также требовать внесения изменений в случае неточности или ошибки. Ответ на обращение индивида должен быть получен от агентства в течение 10 рабочих дней и может быть обжалован вышестоящему должностному лицу, обязанному в течение 30 рабочих дней принять окончательное решение, которое в свою очередь может быть обжаловано в суд.

Основное требование к операторам данных (федеральным агентствам) на основании Акта можно изложить, как запрет их раскрытия (disclosure) — передачи третьим лицам или неопределенному кругу лиц, т.е. сохранения их конфиденциальности за исключением прямо предусмотренных 12 случаев-условий (например, раскрытие данных служащему, ведущему обработку, раскрытие на основании Акта о свободе информации (Freedom of Information Act[12]), раскрытие в интересах правосудия, обеспечения применения гражданского или уголовного закона, передача данных в Национальный архив и т.д.). В случае раскрытия данных обязательно ведение учета кому и когда они были переданы, включая информацию об органе и должностном лице, которым переданы были сведения. Данные учета подлежат обязательному хранению в течение 5 лет или в пределах срока обработки персональной информации в зависимости от того, что дольше по срокам, и должны быть доступны для ознакомления субъекту данных.

Информационные системы федеральных агентств по общему требованию должны содержать минимальный объем информации об индивиде — т.е. только «необходимые и относимые к делу» данные. В случае, если использование данных может затронуть реализацию основных прав и свобод, то агентство не вправе собирать больше информации, чем оно могло бы получить от индивида непосредственно. При сборе данных непосредственно от индивида необходимо указать на правовое основание таких действий, а также на суть последующих операций с данными, включая возможные действия по их раскрытию.

Во избежание формирования «скрытых» баз данных в Акте прямо закрепляется обязанность федеральных агентств публиковать детальные сведения о своих базах данных и любых изменениях в них в Федеральном регистре. Существенные же изменения в информационных системах, содержащих базы персональных данных, должны быть предварительно сообщены Комитету по Государственной делам Палаты представителей и Комитету по государственным делам Сената, а также в Управление по бюджету и финансам.

Значительная часть положений Акта посвящена вопросу объединения или соотнесения баз данных правительственными агентствами. По общему правилу такие действия прямо запрещаются, если только они не предусмотрены в рамках специального соглашения между агентствами об обмене информацией, содержащейся в базах данных с персональной информацией, при условии его опубликования и сообщения Комитету по Государственной деятельности Палаты представителей и Комитету по государственным делам Сената. Соглашения об обмене данными включают в обязательном порядке: наименование правительственных агентств, которые будут осуществлять соотнесение или обмен данных; законное обоснование таких действий; ожидаемые результаты и цели; порядок извещения субъектов данных, чьи права могут быть затронуты; указание на то какие именно данные будут объединены или подвергнуты сверке/соотнесению; положение, позволяющее Генеральному контролеру производить мониторинг правильности выполнения условий соглашения. Максимальный срок действия указанных соглашений не может превышать 18 месяцев, но есть возможность их обновления.

Для защиты прав индивида Актом установлена гражданская и уголовная ответственность за нарушения отдельных его положений. В частности, гражданская ответственность предусмотрена за необоснованный отказ индивиду в доступе к файлу/записи или во внесении туда необходимых изменений и в некоторых иных случаях. Уголовная ответственность предусмотрена за умышленные: раскрытие персональной информации, несообщение о создании баз данных с персональной информацией, необоснованный запрос персональной информации по ложному основанию и т.д.

Особо стоит отметить положения 7 раздела Акта, который применим, как уже говорилось и в отношении властей штатов и местных органов власти, касающегося вопросов использования номера социального страхования (social security number — SSN, далее SSN). Такое внимание обусловлено тем, что SSN уже давно используется как федеральными, так и региональными органами власти в качестве универсального идентификатора, и далеко не всегда в целях решения вопросов о предоставлении социальной помощи или аналогичных услуг. Федеральные агентства, равно как власти штатов и местные органы, не вправе требовать от индивида предоставления SSN в обмен на получение возможности реализации своего права, свободы или получении иной выгоды. Исключение составляют случаи, когда это прямо предписано федеральным законодательством, а также, если информационные системы были созданы еще до вступления Акта в силу, т.е. до 1 января 1975 г. Любое требование, адресованное индивиду, указать свой номер социального страхования должно сопровождаться разъяснениями, является ли пре-

[12] URL: http://www.usdoj.gov/oip/ (дата обращения: 15.01.2012).

доставление добровольным или обязательным, какими законодательными нормами оно предусмотрено и каковы цели его дальнейшего использования.

Оценивая в целом содержание положений Акта, стоит отметить некоторые его существенные недостатки, которые не ограничиваются сравнительно узкой сферой его применения — только в отношении федеральных органов власти. К таким недостаткам можно отнести, в частности, применение Акта только в отношении информационных систем, позволяющих вести поиск информации об индивиде по имени или по иному персональному идентификатору, что выводит из под его действия целый ряд баз данных с иной логической структурой организации информации, где, несомненно, также может содержаться значительный объем персональной информации.

По мнению части авторов[13], особую озабоченность вызывает присутствие в числе исключений возможность раскрытия данных в рамках «обычной практики» (т.н. «routine use disclosure»), которая часто очень широко трактуется правительственными агентствами. Сам Акт определяет это как возможность раскрытия данных в целях сопоставимых/схожих с целями, определенными при их сборе. Такое положение дел ведет к указанию федеральными агентствами самых общих целей при сборе информации о гражданах и оставляет им значительное пространство для возможных злоупотреблений.

Совсем иное положение дел в частном секторе, где при регулировании отношений по обработке персональных данных в США доминирует так называемый «отраслевой» подход, называемый некоторыми авторами, практикой ad hoc[14]. Не случайно, что в своем отчете о принятых мерах на национальном уровне в рамках ОЭСР Соединенные Штаты заявили сразу четыре органа, уполномоченных в сфере контроля за реализацией законодательства о защите данных:

1. Департамент юстиции — в сфере осуществления правосудия;
2. Департамент здравоохранения и социальной защиты — в сфере здравоохранения и социальной защиты;
3. Федеральное банковское агентство — в банковской и финансовой сфере;
4. Федеральная торговая комиссия — в сфере торговли.

При этом такой перечень нельзя назвать исчерпывающим, учитывая, что существует специальное регулирование для некоторых других отраслей и наличие в каждом таком случае специально уполномоченного органа по контролю, а равно учитывая, что штаты также вправе принимать собственные законы о защите данных и учреждать контролирующие органы[15].

Следует подчеркнуть, что законодательство и практика в США подходит в целом к регулированию обработки персональных данных в частном секторе, рассматривая в основном ее с позиции защиты конкуренции и прав потребителей, неслучайно употребляя вместо термина «субъект персональных данных» или «индивид», понятие «потребитель (consumer)». В качестве примера можно привести Акт о защите частной жизни в финансовой сфере (The Right to Financial Privacy Act 1978[16]) и Акт о защите частной жизни в сфере электронной коммуникации (The Electronic Communication Privacy Act 1986[17]), где намеренно используется именно такой термин применительно к обозначению индивидов и это не является исключением[18].

В целом американское законодательство в области защиты прав потребителей при обработки их персональной информации достаточно избирательно. В частности специальное законодательное регулирование предусмотрено для следующих сфер: финансовую сферу[19], медицинские услуги[20], услуги по кредитованию[21], услуги видеопроката[22], кабельное телевидение[23], «он-

---

[13] Коровяковский Д.Г. Российский и зарубежный опыт в области защиты персональных данных // Национальные интересы: приоритеты и безопасность. 2009. № 5. С. 49-50.

[14] Reidenberg Joel R. Privacy Protection and the Interdependence of Law Technology and Self-Regulation//Variations sur le Droit de la Société de l'Information. Bruylant.: Bruxelles, 2001. C. 128.

[15] Report on the Cross-Boarder Enforcement of the Privacy Laws. OECD, 2006. [Электронный ресурс]: URL: http://www.oecd.org/sti/security-privacy (дата обращения: 15.01.2012). С. 13-14.

[16] URL: http://www.fdic.gov/regulations/laws/rules/6500-2550.html (дата обращения: 15.01.2012).

[17] URL: http://cpsr.org/issues/privacy/ecpa86/ (дата обращения: 15.01.2012).

[18] Прим.: Автор намеренно использует термин прайваси в обоих случаях, т.к. само содержание указанных актов не позволяет применение другого термина, поскольку речь идет в большей степени об ограничении вмешательства государства в указанные сферы, нежели обеспечению неприкосновенности частной жизни в целом.

[19] Right to Financial Privacy Act, Pub. L. No. 95-630 (1978). [Электронный ресурс]: URL: http://www.fdic.gov/regulations/laws/rules/6500-2550.html (дата обращения: 15.01.2012).

[20] The Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191. [Электронный ресурс]: URL: http://aspe.hhs.gov/admnsimp/pl104191.htm (дата обращения: 15.01.2012).

[21] Fair Credit Reporting Act, Pub. L. No. 91-508 (1970). [Электронный ресурс]: URL: http://www.ftc.gov/os/statutes/fcra.htm (дата обращения: 15.01.2012).

[22] Video Privacy Protection Act, Pub. L. No. 100-618 (1988). [Электронный ресурс]: URL: http://www.accessreports.com/statutes/VIDEO1.htm (дата обращения: 15.01.2012).

[23] Cable Privacy Protection Act, Pub. L. No. 98-549 (1984). [Электронный ресурс]: URL: http://epic.org/privacy/cable_tv/cpa.html (дата обращения: 15.01.2012).

лайн» деятельность детей до 13 лет[24], образовательные услуги[25], регистрация транспортных средств[26], телемаркетинг[27].

Значительную роль в регулировании вопросов защиты частной жизни в США, включая защиту персональной информации, играют решения Верховного суда, основанные на толковании 4-ой поправки Конституции. Такие решения принимаются достаточно часто и, как правило, носят казуальный характер. В частности, Верховный суд рассматривал вопрос о данных владельцев транспортных средств, признав их коммерческий характер и возможность регулировать их обработку федеральным правительством[28]. В 2001 г. Верховный суд признал отсутствие нарушений Акта о семейных образовательных правах и частной жизни[29] и 4-ой поправки Конституции в случае выставления рейтинга учащихся и его оглашения вслух[30].

Многие вопросы в области регулирования обработки данных решаются на основе саморегулирования, т.е. на основе внутренних корпоративных норм и рыночной целесообразности[31], что существенным образом сказывается на уровне защиты данных и сохранения их конфиденциальности, что приводит к формированию своего рода рынка данных об индивиде, о котором он может и не догадываться. В качестве одного из ярких примеров можно назвать наличие самостоятельного и весьма прибыльного рынка информации о гражданах-потребителях о чем можно судить на основании ставшего широко известным дела Lotus, когда информация (CD-диск) об образе жизни около 20 миллионов американских семей, стала предметом продажи и распространения и была в последствии изъята из оборота под давлением потребителей[32].

Стоит отдельно упомянуть законодательные изменения, касающиеся защиты частной жизни, принятые после печальных событий 11 сентября 2001 г. Следствием указанных событий стало существенное расширение полномочий спецслужб, правоохранительных и правоприменительных органов, что нашло свое закрепление в так называемом «Патриотическом Акте 2001 года» (Полное название — Акт об единении и укреплении Америки, путем принятия соответствующих мер, необходимых для противодействия терроризму[33]). Принятие указанного акта было осуществлено в предельно краткие сроки, практически без каких либо проволочек. Вступление его в силу серьезным образом изменило действие целого спектра нормативных актов (в качестве примера можно назвать: Статут о связи, Акт о защите частной жизни в финансовой сфере, Акт о защите частной жизни в сфере электронных коммуникаций, Акт об агентствах кредитных историй, Акт о банковской тайне и др.), ограничивающих возможности органов власти контролировать действия граждан. Большая часть внесенных изменений существенным образом упростило работу спецслужбам по установлению специальных технических устройств, осуществляющих перехват информации о коммуникационных соединениях, информации о времени, адресате и отправителе сообщения, и некоторые другие сведения. До Патриотического Акта использование специальных электронных технических средств наблюдения было возможным только с разрешения суда и исключительно при наличии существенных правовых оснований (предположение о совершении тяжкого преступления, предусмотренного специальным перечнем; обоснованного предположения о том, что будет перехвачена информация о совершенном или совершаемом преступлении; средства коммуникации в достаточной степени используются подозреваемым, в том числе для совершения правонарушения). Кроме этого такое разрешение всегда было ограниченно во времени, в противном случае доступ к содержанию сообщений был бы незаконным, а любое доказательство, полученное в нарушении выше названного порядка было бы «неприемлемым» для суда. Судебная санкция имела также огра-

---

[24] Children's Online Privacy Protection Act, Pub. L. No. 105-277 (1998). [Электронный ресурс]: URL: http://www.ftc.gov/ogc/coppa1.htm (дата обращения: 15.01.2012).

[25] Family Educational Rights and Privacy Act, Pub. L. No. 93-380 (1974). [Электронный ресурс]: URL: http://epic.org/privacy/education/ferpa.html (дата обращения: 15.01.2012).

[26] Drivers Privacy Protection Act, Pub. L. No. 103-322 (1994). [Электронный ресурс]: URL: http://www.accessreports.com/statutes/DPPA1.htm

[27] Telephone Consumer Protection Act, Pub. L. No. 102-243 (1991). [Электронный ресурс]: URL: http://epic.org/privacy/telemarketing/ (дата обращения: 15.01.2012).

[28] Reno v. Condon, 528 U.S. 141 (2000). [Электронный ресурс]: URL: http://www.usdoj.gov/osg/briefs/1999/3mer/2mer/98-1464.mer.aa.html

[29] Family Educational Rights and Privacy Act, Pub. L. No. 93-380 (1974). [Электронный ресурс]: URL: http://epic.org/privacy/education/ferpa.html (дата обращения: 15.01.2012).

[30] Owasso Independent School District v. Falvo, 534 U.S. 426 (2001). [Электронный ресурс]: URL: http://www.law.com/regionals/ca/opinions/feb/001073.shtml (дата обращения: 15.01.2012).

[31] Reidenberg Joel R. Privacy Protection and the Interdependence of Law Technology and Self-Regulation//Variations sur le Droit de la Société de l'Information, Bruylant. Bruxelles, 2001. C. 131.

[32] Cadoux Louise La Vie Privée : un Avenir sous Haute Surveillance // Liberté d'Expression et Nouvelles Technologies, IQ Collectif. Paris, 1998. C. 121

[33] Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 26, october 2001. [Электронный ресурс]: URL: http://epic.org/privacy/terrorism/hr3162.html (дата обращения: 15.01.2012).

ниченное географическое действие, поскольку могла быть выдана только местными судебными властями в соответствии с территориальной подсудностью. Вступление акта в силу изменило некоторым образом этот порядок, приведем лишь некоторые примеры этого:

- Во-первых, Патриотический акт предоставил возможность широкого использования специальных средств регистрирующих только информацию о об акте коммуникации (время, адресат, получатель, продолжительность и иная информация о коммуникации, исключая доступ к содержанию самого сообщения), технология, которая в США получила название «pen register» или «trap and trace»[34]. Использование подобных устройств стало возможным с разрешения суда, которое основывалось на простом утверждении об уместности такого использования в интересах следствия, исходящего от соответствующего атторнея, что существенно проще, нежели стандартная процедура. Более того акт значительно расширил круг использования аналогичных устройств в отношении не только телефонной связи, но и в отношении практически всех известных разновидностей электронной коммуникации: электронная почта, навигационные данные в сети Интернет, и многие другие виды электронной связи.
- Во-вторых, Патриотический акт содержал очень важные положения относительно законности действий правоохранительных органов по перехвату электронных сообщений и иной информации о «компьютерном нарушителе», если на то получено согласие владельца или оператора «защищенного компьютера». Таким образом, указанные действия властей становились частными отношениями оператора и органа власти, т.е. вне всякого судебного контроля. В последующем это привело к использованию и внедрению ФБР технологии сбора компьютерной информации Carnivore[35], позднее переименованной в DCS-1000, которая сама по себе, как и ее использование, порождает до сих пор самые противоречивые мнения[36].
- В-третьих, с 2001 г. стало возможным выдача федеральными судами ордеров, имеющих силу на всей территории США, с одной стороны это также серьезно упростило работу правоохранительных органов и с другой стороны усложнило порядок обжалования их действий, поскольку такие действия должны быть предприняты в том же суде.

Приведенные примеры не исчерпывают перечень «законодательных новелл» в американском праве, ставших итогом печальных событий 11 сентября 2001 года, что говорит о продолжающихся изменениях действующего законодательства о защите частной жизни и доступа государства к персональным данным граждан в США. До настоящего времени было несколько попыток некоторой реформы положений Патриотического Акта, которые так и не нашли поддержку в Конгрессе[37].

Подводя итог и оценивая в целом уровень защиты прав субъекта персональных данных в США можно выделить и подчеркнуть следующие отличительные особенности, отражающие в полной мере специфику «американского» похода к правовому регулированию защиты частной жизни при обработке персональных данных:

1. Использование для правового регулирования отношений в области обработки персональных данных категорий-концептов «прайваси» (стоит отметить, что это аналогичная, но подчас не тождественная категория понятию «праву на частную жизнь») и «электронная (компьтерная) прайваси», которая в основном используется для установления пределов вмешательства, в первую очередь, государства и его органов в частную жизнь индивида;
2. Крайне избирательный, отраслевой подход к правовому регулированию вопросов защиты данных о физических лицах, где наиболее урегулированным на уровне законодательства является «публичная сфера (сфера государственного управления)» в отсутствии единого акта, устанавливающего общие принципы защиты данных, содержащих персональную информацию;

---

[34] Прим.: «pen register (дословно журнал записей)» определяется как «устройство или процесс, который записывает или декодирует информацию об электронном соединении (набранном номере или адресате, маршруте, передаваемых сигналах и сообщениях), передаваемую прибором или устройством, с которого осуществляется проводное или иное электронное соединение, при условии, что она не включает в себя само содержание передаваемого сообщения»; «trap and trace device (ловушка и след – устройство)» определяется как «устройство или процесс перехвата входящих электронных или иных сигналов (импульсов), содержащих информацию об электронном соединении (исходящем адресе (номере), получателе, маршруте, передаваемых сигналах и сообщениях) позволяющую с большой вероятностью определить источник проводного или иного электронного соединения, при условии, что она не включает в себя само содержание передаваемого сообщения» [перевод автора]. Оригинальный текст [Электронный ресурс]: URL: http://codes.lp.findlaw.com/uscode/18/II/206/3127 (дата обращения: 15.01.2012).

[35] Прим.: пер. с англ. – дословно хищник или плотоядное животное.

[36] См. об этом: URL: http://www.cybertelecom.org/security/carnivore.htm (дата обращения: 15.01.2012).

[37] См. об этом: URL: http://epic.org/privacy/terrorism/usapatriot/ (дата обращения: 15.01.2012).

3. Преобладание в частном секторе экономики рыночных механизмов и механизмов саморегулирования в вопросах защиты прав индивида, а также рассмотрение в целом проблемы регулирования обработки данных частными компаниями с позиций «добросовестной конкуренции» и «защиты прав потребителя»;
4. Отсутствие едино уполномоченного органа по контролю за соблюдением законодательства в сфере персональных данных и распределение этих функций между различными органами, в соответствии с их компетенцией и отраслевой направленностью.

Несмотря на такие значительные различия в «американском» подходе к правовому регулированию обработки персональных данных, в первую очередь от «общеевропейской» практики, ориентированной на установление единого правового регулирования для государственного и частного сектора, в условиях существования единого контролирующего органа по защите прав индивида, говорить о его неэффективности вряд ли стоит, скорее можно констатировать его своеобразие и крайне отраслевой и разобщенный характер, что, пожалуй, воспринимается как недостаток, но который обусловлен своеобразием самой системы права и законодательства в США, а не отсутствием желания гарантировать и обеспечить защиту прав личности.

Сводные доклады о состоянии выполнения государствами-участниками ОЭСР своих международных обязательств по принятию законодательных мер по защите прав субъектов персональных данных, не называют США в качестве аутсайдеров[38], как в прочем и независимые оценки со стороны международных неправительственных организаций, таких как Прайваси Интернэшнл (Privacy Inetrnational)[39].

Библиографический список:

1. Brandeis Louis & Warren Samuel," The Right to Privacy" // 4 Harvard Law Review 193-220 (1890-91). [Электронный ресурс] URL: http://faculty.uml.edu/sgallagher/Brandeisprivacy.htm (дата обращения: 15.01.2012).
2. Cadoux Louise La Vie Privée: un Avenir sous Haute Surveillance//Liberté d'Expression et Nouvelles Technologies, IQ Collectif. Paris, 1998.
3. Reidenberg Joel R. Privacy Protection and the Interdependence of Law Technology and Self-Regulation // Variations sur le Droit de la Société de l'Information, Bruylant. Bruxelles, 2001.
4. Баранов В.М. Категория «частная жизнь» // Право граждан на информацию и защита неприкосновенности частной жизни. Н.Новгород, 1999.
5. Бачило И.Л., Лопатин В.Н., Федотов М.А. Информационное право. СПб.: Изд. «Юридический центр Пресс», 2005.
6. Головкин Р.Б. Правовое и моральное регулирование частной жизни в современной России: Дис. ... д-ра юрид. наук: 12.00.01. Н.Новгород, 2005.
7. Коровяковский Д.Г. Российский и зарубежный опыт в области защиты персональных данных // Национальные интересы: приоритеты и безопасность. 2009. № 5.

References (transliteration):

1. Baranov V.M. Kategoriya «chastnaya zhizn'» // Pravo grazhdan na informatsiyu i zashchita neprikosnovennosti chastnoy zhizni. N.Novgorod, 1999.
2. Bachilo I.L., Lopatin V.N., Fedotov M.A. Informatsionnoe pravo. SPb: Izd. «Yuridicheskiy tsentr Press», 2005.
3. Golovkin R.B. Pravovoe i moral'noe regulirovanie chastnoy zhizni v sovremennoy Rossii: Dis. ... d-ra yurid. nauk: 12.00.01. N.Novgorod, 2005.
4. Korovyakovskiy D.G. Rossiyskiy i zarubezhnyy opyt v oblasti zashchity personal'nykh dannykh // Natsional'nye interesy: prioritety i bezopasnost'. — 2009. — № 5.

[38] Report on the Cross-Boarder Enforcement of the Privacy Laws, OECD 2006. [Электронный ресурс]: URL: www.oecd.org/sti/security-privacy (дата обращения: 15.01.2012).

[39] См. об этом: Сводные данные об уровне защиты права на частную жизнь в мире. [Электронный ресурс]: URL: http://www.privacyinternational.org/article.shtml?cmd[347]=x-347-559597 (дата обращения: 15.01.2012).