острова, Гернси, Израиль, Мэн, Джерси, Новая Зеландия, США, Уругвай[1]. В отношении других стран, при трансграничной передаче данных требуется предоставление соответствующего уровня защиты данных, как правило, путем заключения соответствующего соглашения. Одним из самых известных таких соглашений можно назвать Соглашение между ЕС и США о передаче персональных данных об авиапассажирах, после заключения которого уровень защиты данных об авиапассажирах из стран ЕС был признан соответствующим[2].

Пожалуй, по-прежнему достаточным своеобразием и серьезными отличительными чертами обладает механизм защиты персональных данных, предусмотренный законодательством США, причем настолько, что вполне можно говорить о другом подходе к правовому регулированию персональных данных, чем тот, который распространен в большинстве европейских государств и который заслуживает отдельного упоминания.

США уже давно известны как страна, где право на уважение частной жизни получило широкое признание и уважение, учитывая, что и сами термины «частная жизнь» или «право на частную жизнь» во многом появляются как интерпретация термина “right of privacy”, введенного в употребление американскими юристами, о чем уже ранее говорилось.

В течение долгого периода американской истории, именно понятие “privacy” (прайваси) – становится ключевым словом-концепцией для всей американской системы права. Первоначально данная концепция описывала лишь достаточно ограниченные аспекты частной жизни, подлежащие защите на основании текста 4-й поправки к Конституции США, однако, благодаря гибкости и адаптивности конституционного права количество правомочий постоянно возрастало.

---

[1] Commission decisions on the adequacy of the protection of personal data in third countries. – (http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm). – Дата обращения: 20.05.2017.

[2] The EU-U.S. Privacy Shield. – (http://ec.europa.eu/justice/data-protection/international-transfers/eu-us-privacy-shield/index_en.htm). – Дата обращения 20.05.2017.

В частности, «прайваси» в первую очередь затрагивала такие аспекты, как право на жилище, на тайну переписки, а затем и телефонных переговоров, электронных и иных сообщений, т.е. так называемых privacy rights.

Развитие компьютерных технологий обработки информации, в которых США является одним из бесспорных лидеров и в настоящее время, привело к неизбежному вопросу защиты «прайваси» (частной жизни), в первую очередь – в условиях автоматизированной обработки информации о физических лицах в электронных базах данных.

Для изучения вопроса Департаментом здравоохранения, образования и социальной защиты (Department of Health, Education and Welfare) была создана специальная комиссия по изучению вопроса, которая еще в 1973 году в своем докладе обратилась с рекомендациями к Конгрессу по принятию специального законодательства – Кодекса честной информационной практики (Code of Fair Information Practice[1]), 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

[1] FTC Fair information practice principles. – (http://inflection.com/privacy/frameworks-were-watching/ftc-fair-information-practice-principles). – Дата обращения 20.05.2017.

обеспечить достоверность персональных данных, а также принять меры к предотвращению их ненадлежащего использования.

Кроме этого, специальный доклад содержал рекомендации для организаций, ведущих обработку персональной информации о необходимости защиты последней, а также о необходимости ежегодного опубликования сведений о базах данных и содержащейся в них информации.

Большая часть положений доклада легла в основу принятого год спустя Акта о защите частной жизни 1974 года (The Privacy Act of 1974[1], далее – Акт).

История принятия этого документа стала компромиссом между двумя законопроектами, которые появились одновременно, один в Палате представителей, а другой – в Сенате. Отличались они в основном порядком возмещения вреда, причиненного субъекту данных. Законопроект Сената в этом отношении был более суров, и для возмещения вреда было достаточно лишь установления факта нарушения, тогда как законопроект Палаты представителей предусматривал возможность возмещения лишь в том случае, если будет доказано, что нарушения были умышленными и грубыми. В итоге смешанная комиссия пришла к общему мнению, согласовав общий текст будущего закона, который предусматривал, что для отдельных нарушений требовалось доказывать их преднамеренный характер для получения возмещения. В остальном – положения двух законопроектов были практически идентичны и легли в основу принятого Акта.

Сам Акт является интересным документом для изучения и в полной мере характеризует своеобразность американского подхода к правовому регулированию обработки персональной информации, в связи с чем автору видится логичным рассмотреть его положения более детально.

Первое, что стоит упоминания, – это сфера действия Акта, которую можно назвать достаточно ограниченной. Акт, в частности, предоставлял

[1] The Privacy Act of 1974 (Pub. L. 93–579, 88 Stat. 1896, enacted December 31, 1974, 5 U.S.C. § 552a). – (https://www.gpo.gov/fdsys/pkg/STATUTE-88/pdf/STATUTE-88-Pg1896.pdf). – Дата обращения 20.05.2017.

права в сфере обработки персональной информации, включая право на судебную защиту, исключительно гражданам и постоянным резидентам. Однако положения Акта применялись исключительно в отношении федеральных правительственных агентств, за исключением 7-го раздела касательно номера социальной защиты (Social Security Number – SSN), применяемого в отношении федеральных, местных органов власти и органов власти штатов. Номер социальной защиты может быть предоставлен исключительно на основании федерального закона, в котором в обязательном порядке указывается, является ли такое сообщение SSN добровольным или обязательным. Впрочем, это никак не мешало штатам принимать специальное законодательство, которое бы предусматривало правила обработки персональной информации органами штатов и местными органами власти, помимо положений 7-го раздела Акта. Таким образом, различные федеральные агентства, подчиняющиеся федеральному правительству, в полной мере попали под действие положений Акта, среди них стоит назвать: почта США, департамент образования, Федеральное бюро расследований и многие другие. Еще одним ограничением стало упоминание в тексте рассматриваемого закона понятия “system of records” – «система записей/файлов», которая определялась как любая совокупность записей/файлов, где информацию об индивиде можно было получить по его имени или индивидуальному идентификатору, что исключало применение закона к базам данных, устроенным по иным принципам доступа, но которые также могли содержать информацию персонального характера.

В Акте прямо была закреплена обязанность федеральных агентств ежегодно публиковать сведения о своих базах данных в Федеральном регистре. В рамках такой публикации в обязательном порядке было необходимо указать цель использования базы данных и порядок обращения в агентство заинтересованных лиц в целях предоставления письменных данных, заключений или обоснований. Кроме этого, любые значительные изменения в порядке ведения базы данных должны быть заблаговременно

рассмотрены Комитетом по государственным операциям Палаты представителей, Комитетом по государственным делам Сената, а также Кабинетом по управлению и бюджету, которые проводят оценку с точки зрения возможного или предполагаемого ущерба правам индивида предлагаемых изменений.

Права субъекта данных (любого физического лица) предусматривали право на доступ к информации о нем. Субъекту при этом предоставляется право знакомиться и делать копии информации о себе, а также требовать внесения изменений в случае неточности или ошибок.

Основное требование к операторам данных (федеральных агентств) 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, к которым подразделом b было отнесено:

1) раскрытие данных служащему агентства, который ведет их обработку и которые ему необходимы для реализации его должностных обязанностей;

2) раскрытие в соответствии с требованиями Акта о свободе информации (Freedom Information Act[1]);

3) раскрытие в соответствии с «обычной практикой» (routine use);

4) раскрытие для Бюро переписи населения США (US Census Bureau[2]) для осуществления переписи населения;

5) раскрытие по заранее полученному запросу в целях статистических исследований, при условии передачи обезличенных данных (без идентифицирующей личность информации);

6) передача записей (данных) в администрации национальных архивов и записей в качестве записи/файла, имеющей историческую ценность;

[1] The Freedom of Information Act (FOIA) (5 U.S.C. § 552). – (https://www.gpo.gov/fdsys/pkg/STATUTE-80/pdf/STATUTE-80-Pg250.pdf). – Дата обращения 20.05.2017.
[2] US Census Bureau. – (https://www.census.gov/).

7) передача записей в целях осуществления уголовного и гражданского правосудия;

8) раскрытие в целях защиты жизни и здоровья лица, при условии сообщения ему о факте раскрытия его данных;

9) раскрытие информации Конгрессу или его комитетам, подкомитетам;

10) раскрытие Генеральному аудитору (Comptroller General[1]) для осуществления деятельности Генерального счетного комитета (the General Accounting Office);

11) раскрытие на основании решения суда (судебного приказа);

12) раскрытие информации о потребителе в соответствии с требованием специального закона.

При раскрытии персональной информации агентства должны вести ее учет, т.е. хранить в течение не менее 5 лет информацию: о времени запроса; субъекте, который ее запросил, включая его контактную информацию; описание переданной информации. Субъект данных вправе ознакомиться с такой учетной записью, за исключением информации по запросам, связанным с осуществлением правосудия.

Качество и объем информации, содержащейся у агентства (оператора), регулировались путем установления принципов достоверности информации, а также принципа минимального объема информации, который необходим для реализации законной деятельности агентства, т.е. только необходимая и относящаяся к делу информация (relevant and necessary). Сверх этого было разрешено осуществлять сбор информации только в том случае, если недостаточность информации может негативно отразиться для индивида (по ограничению прав, интересов, преимуществ). В таких случаях агентства вправе собирать всю доступную информацию непосредственно от индивида. Положения Акта также предусматривали возможность сопоставления,

[1] The Comptroller General of the United States. – (http://www.gao.gov/cghome/index.html). – Дата обращения 20.05.2017.

объединения данных агентствами при условии письменного соглашения, которое должно быть сообщено Комитету по государственным делам Сената и Комитету по государственным операциям Палаты представителей, а также находиться в публичном доступе. В соглашении в обязательном порядке предусматриваются: цель и орган, который будет ответственен за объединение данных; ожидаемые результаты и обоснование необходимости объединения баз данных; описание данных, которые будут объединяться. В каждом агентстве, которое собирается участвовать в программе сопоставления и объединения данных, Акт требовал создания специального органа (Data Integrity Board), который бы следил за исполнением соглашений об обмене и сопоставлении данных, их соответствием законодательству.

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 в него 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.

Как видно из анализа рассматриваемого документа, становится очевидным, что он распространяется на достаточно узкий круг отношений, связанных с обработкой персональной информации, к тому же содержит некоторые положения, которые не всегда гарантируют адекватную защиту прав индивида. В частности, вызывает опасения применение Акта исключительно к базам данных, организованным по имени индивида, особому номеру, фотографии, что на момент его принятия в 1974 году могло гарантировать адекватную защиту. Тогда как сейчас, в условиях формирования информационных систем с самыми различными вариантами их организации и поиска в них персональной информации, такое положение

можно охарактеризовать как не совсем удачное и ограничивающее сферу его действия.

По мнению части авторов[1], особую озабоченность вызывает присутствие в числе исключений возможности раскрытия данных в рамках «обычной практики» (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.

На основании изложенного нетрудно сделать вывод о том, что Прайваси Акт регулирует только отношения по обработке данных правительственными агентствами, т.е. органами государственной власти, однако это не означает, что в США отсутствуют нормы, которые регулируют вопросы защиты прав индивида при обработке его данных в частном секторе экономики. В этом заключается еще одно существенное отличие американского подхода к регулированию обработки персональных данных.

Все дело в том, что в остальных случаях в США доминирует так называемый отраслевой подход к правовому регулированию обработки данных, а некоторые авторы даже называют его скорее практикой ad hoc[2]. 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 реализации законодательства о защите данных:

– Департамент юстиции – в сфере осуществления правосудия;

---

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

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

– Департамент здравоохранения и социальной защиты – в сфере здравоохранения и социальной защиты;
– Федеральное банковское агентство – в банковской и финансовой сфере;
– Федеральная торговая комиссия – в сфере торговли.

При этом такой перечень нельзя назвать исчерпывающим, учитывая, что существует специальное регулирование для некоторых других отраслей, равно как 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[1].

Особым образом 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 прайваси в финансовой сфере (The Right to Financial Privacy Act 1978[2]) и Акт о защите прайваси в электронных коммуникациях (The Electronic Communication Privacy Act 1986[3]), где намеренно используется именно указанный термин применительно к обозначению индивидов, и это не является исключением[4].

В целом американское законодательство в области защиты прав потребителей при обработке их персональной информации достаточно избирательно.

---

[1] Report on the Cross-Boarder Enforcement of the Privacy Laws / OECD. – 2006. – P. 13–14.
[2] The Right to Financial Privacy Act of 1978 (RFPA; codified at 12 U.S.C. ch. 35, § 3401 et seq.). – (https://www.gpo.gov/fdsys/pkg/STATUTE-92/pdf/STATUTE-92-Pg3641.pdf). – Дата обращения 20.05.2017.
[3] The Electronic Communications Privacy Act of 1986 (ECPA) (18 U.S.C. § 2510 et seq.). – (https://www.gpo.gov/fdsys/pkg/STATUTE-100/pdf/STATUTE-100-Pg1848.pdf). – Дата обращения 20.05.2017.
[4] Автор намеренно использует термин «прайваси» в обоих случаях, так как само содержание указанных актов не позволяет использование другого термина, поскольку названные документы в большей степени посвящены ограничению вмешательства государства в указанные сферы, нежели обеспечению неприкосновенности частной жизни в целом.

В качестве наиболее «урегулированных сфер» можно назвать: финансовую сферу[1], медицинские услуги[2], услуги по кредитованию[3], услуги видеопроката[4], кабельное телевидение[5], «онлайн» деятельность детей до 13 лет[6], образовательные услуги[7], регистрация транспортных средств[8], телемаркетинг[9].

Значительную роль в регулировании вопросов защиты частной жизни в США, включая защиту персональных данных, играют решения Верховного суда, основанные на толковании 4-й 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[10]. В 2001 году Верховный суд признал отсутствие нарушений Акта о семейных образовательных правах и частной жизни и 4-й поправки Конституции в случае выставления рейтинга учащихся и его оглашения вслух[11].

Многие вопросы в области регулирования обработки данных разрешаются на основе саморегулирования, т.е. на основе внутренних

---

[1] The Right to Financial Privacy Act of 1978 (RFPA; codified at 12 U.S.C. ch. 35, § 3401 et seq.). – (https://www.gpo.gov/fdsys/pkg/STATUTE-92/pdf/STATUTE-92-Pg3641.pdf). – Дата обращения 20.05.2017.

[2] The Health Insurance Portability and Accountability Act of 1996 (Pub. L. No. 104–191). – (https://www.gpo.gov/fdsys/pkg/PLAW-104publ191/html/PLAW-104publ191.htm). – Дата обращения 20.05.2017.

[3] The Fair Credit Reporting Act of 1970 (Pub. L. No. No. 91-508 (1970)). – (https://www.gpo.gov/fdsys/pkg/STATUTE-84/pdf/STATUTE-84-Pg1114-2.pdf). – Дата обращения 20.05.2017.

[4] The Video Privacy Protection Act (Pub. L. No. 100-618 (1988)). – (https://www.gpo.gov/fdsys/pkg/STATUTE-102/pdf/STATUTE-102-Pg3195.pdf). – (дата обращения 20.05.2017).

[5] The Cable Communications Policy Act of 1984 (Pub. L. No. 98-549 (1984)). – (https://www.gpo.gov/fdsys/pkg/STATUTE-98/pdf/STATUTE-98-Pg2779.pdf). – Дата обращения 20.05.2017.

[6] The Children's Online Privacy Protection Act of 1998 (COPPA) (Pub. L. No. 105-277 (1998)). – (https://www.gpo.gov/fdsys/pkg/PLAW-105publ277/html/PLAW-105publ277.htm). – Дата обращения 20.05.2017.

[7] The Family Educational Rights and Privacy Act of 1974 (FERPA or the Buckley Amendment) (Pub. L. No. 93-380 (1974)). – (http://www.legisworks.org/GPO/STATUTE-88-Pg484.pdf). – Дата обращения 20.05.2017.

[8] The Driver's Privacy Protection Act of 1994 (Pub. L. No. 103-322 (1994)). – (https://www.gpo.gov/fdsys/pkg/USCODE-2011-title18/pdf/USCODE-2011-title18-partI-chap123-sec2721.pdf). – Дата обращения 20.05.2017.

[9] The Telephone Consumer Protection Act of 1991 (Pub. L. No. 102-243 (1991)). – (https://www.gpo.gov/fdsys/pkg/USCODE-2011-title47/pdf/USCODE-2011-title47-chap5-subchapII-partI-sec227.pdf). – Дата обращения 20.05.2017.

[10] Reno v. Condon, 528 U.S. 141 (2000). – (https://supreme.justia.com/cases/federal/us/528/141/case.html). – Дата обращения 20.05.2017.

[11] Owasso Independent School District v. Falvo, 534 U.S. 426 (2001). – (https://supreme.justia.com/cases/federal/us/534/426/case.html). – Дата обращения 20.05.2017.).

корпоративных норм и рыночной целесообразности[1], что существенным образом сказывается на уровне защиты данных и сохранения их конфиденциальности и приводит к существованию своего рода рынка данных об индивиде, о котором он может и не знать. 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 впоследствии изъята из оборота под давлением потребителей[2].

Подводя итог анализу зарубежной и международной практики, можно условно выделить два основных подхода (модели) правового регулирования персональных данных – *европейский* и *американский*.

Основными и наиболее характерными чертами первой модели следует признать:

1) признание за индивидом неотъемлемого права контролировать обработку информации о себе, как части «информационной самоидентификации» личности в демократическом обществе;

2) наличие специального закона, устанавливающего общие требования к обработке персональных данных в частной и публичной сфере, т.е. установление общего режима конфиденциальности, заключающегося в особом режиме доступа к ним и их распространения, преимущественно с согласия индивида;

3) наличие единого, независимого уполномоченного органа по контролю над соблюдением законодательства о персональных данных (специальная комиссия или омбудсмен), который полномочен самостоятельно рассматривать жалобы граждан;

---

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

[2] Cadoux, L. La Vie Privée: un Avenir sous Haute Surveillance / L. Cadoux // Liberté d'Expression et Nouvelles Technologies. – Paris: IQ Collectif, 1998. – P. 121

4) использование механизмов саморегулирования в частной сфере в качестве дополнительного (субсидиарного).

В качестве несомненных положительных черт такого подхода следует признать ориентацию на приоритет прав личности, признание защиты персональных данных в качестве одной из сторон прав и свобод человека, в связи с чем он более ориентирован на государственное регулирование обработки персональных данных, независимо от сферы ее осуществления и установление гарантий прав субъекта.

Отрицательными чертами в таком случае стоит признать тот факт, что часто гармонизация законодательства о персональных данных оставляет существенное «поле для маневра» для государств-участников ЕС, что иногда приводит к существенным расхождениям в его содержании.

Для *американского* похода, напротив, характерно:

1) использование категории «прайваси» для частной и публичной сферы для ограничения вмешательства государства и его органов в частную жизнь индивида;

2) отраслевой подход к правовому регулированию вопросов защиты данных о физических лицах, где наиболее урегулированной сферой на уровне законодательства является «публичная сфера (сфера государственного управления)» и отсутствует единый документ, устанавливающего единые принципы защиты данных для частной и публичной сфер экономики;

3) преобладание в частном секторе (в экономике) рыночных механизмов регулирования 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 единого 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.

Существенный недостаток данного подхода во многом очевиден – это ориентация на рыночные механизмы регулирование в частной сфере, что не лучшим образом гарантирует защиту прав субъекта данных, поскольку, вне всякого сомнения, в случае противоречий индивиду будет гораздо сложнее противостоять частным компаниям, а также требовать от них информирования об использовании данных о себе в отсутствие законодательно закрепленной обязанности. К примеру, деятельности специализированных агентств, предоставляющих информацию о кредитных историях, урегулирована, тогда как компании, занимающиеся адресным (прямым) маркетингом, не связаны в аналогичном случае какими-либо правилами. Положительной чертой в этом походе является как раз «специальный», или даже в некоторой степени «адресный», подход к регулированию защиты прав субъекта, учитывающий специфику той или иной отрасли экономики, государственного управления, в том числе и при установлении средств судебной защиты, поскольку в каждом случае обычно упоминается размер или порядок определения размера возмещения в гражданском судопроизводстве и размеры уголовного наказания за возможные нарушения.

Говоря о распространенности названных выше подходов среди государств мира, можно сказать, что *европейский* получил более широкое распространение и в настоящий момент это порядка 50 государств Совета Европы, расположенных на европейском континенте, а также Канада, Аргентина, Австралия, Новая Зеландия, Южная Корея, Буркина Фасо.

Американский подход менее распространен и помимо самих Соединенных Штатов Америки аналогичным образом «отраслевое»

регулирование обработки персональных данных характерно для Японии, Парагвая, Тайваня, Тайланда[1].

[1] Параскевов, А.В. Сравнительный анализ правового регулирования защиты персональных данных в России и за рубежом / А.В. Параскевов, А.В. Левченко, Ю.А. Кухоль // Политематический сетевой электронный научный журнал Кубанского государственного аграрного университета. – Краснодар: КубГУ, 2015. – № 110. – С. 866–894.