**П.А. Шариков***

# КОНФИДЕНЦИАЛЬНОСТЬ ИНФОРМАЦИИ И ПОЛИТИКА НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ: АМЕРИКАНСКИЙ ДИСКУРС В XXI ВЕКЕ**

*Федеральное государственное бюджетное учреждение науки «Институт Соединенных Штатов Америки и Канады Российской академии наук»*
*123995, Москва, Хлебный пер., 2/3*

Бурное развитие информационных технологий, наблюдаемое со второй половины XX в., к началу XXI столетия приобрело такие масштабы, что по праву стало называться информационной революцией и отразилось буквально на всех сторонах общественной жизни, в том числе международных отношениях. Однако, как и в случае с любым подлинно революционным явлением, в полной мере оценить его воздействие, характер и тем более последствия в настоящий момент в высшей степени проблематично. С этой точки зрения особый интерес представляет опыт Соединенных Штатов Америки как страны, одной из первых вступившей в «информационную эпоху» и, как следствие, успевшей накопить определенную практику регулирования информационной сферы в новых условиях. В центре внимания американских исследователей и политиков оказалась проблема поиска баланса между гарантиями конфиденциальности личной информации и задачами обеспечения национальной безопасности. В статье изучена эволюция подходов к данной проблеме администраций У. Клинтона, Дж. Буша-мл. и Б. Обамы. Особое внимание уделено сравнительному анализу двух ключевых документов, которые регулировали вопросы защиты персональных данных в контексте информационной безопасности, — законов «Патриот» и «О свободе». Подробно рассмотрены обстоятельства, причины и предпосылки принятия этих нормативных актов. Автор отмечает, что если закон «Патриот», наделявший специальные службы широчайшими правами и полномочиями в отношении доступа к личной информации американских и иностранных граждан, был рассмотрен и утвержден в рекордные сроки по горячим следам терактов 11 сентября 2001 г., то обсуждение закона «О свободе», спровоцированное разоблачениями

* *Шариков Павел Александрович* — кандидат политических наук, руководитель Центра прикладных исследований Института США и Канады РАН; доцент кафедры региональных проблем мировой политики факультета мировой политики МГУ имени М.В. Ломоносова (e-mail: pasha.sharikov@gmail.com).

** Исследование подготовлено при финансовой поддержке РГНФ, проект № 15-37-01203.

бывшего сотрудника Агентства национальной безопасности Э. Сноудена, затянулось и даже стало предметом полемики в рамках предвыборной кампании 2016 г. По мнению автора, в настоящий момент в американской политике в отношении информационной сферы в целом и проблемы защиты конфиденциальной информации в частности возобладала тенденция к ограничению государственного вмешательства и повышению прозрачности деятельности спецслужб.

***Ключевые слова:*** Соединенные Штаты Америки, США, национальная безопасность, информационная безопасность, конфиденциальная информация, закон «Патриот», закон «О свободе», закон «Об иностранной разведке», PRISM, массовый сбор данных, «пакет Яровой», Э. Сноуден.

Стремительное развитие информационных технологий, потребительской электроники и интернета во второй половине XX — начале XXI в. сделало вопросы регулирования сферы информации приоритетом государственной политики. Происходящие в обществе под влиянием информационной революции изменения даже натолкнули ряд философов на мысль о вступлении человечества в новый период своей истории — информационную эпоху. Фундаментальные трансформации современного социума ученые объясняли по-разному. С помощью таких понятий, как «постиндустриальное общество» [Белл, 2004], «общество знаний» [Drucker, 1996], «информационная эпоха» [Кастельс, 2000], «третья волна» [Toffler, 1984], «новое индустриальное общество» [Gailbraith, 1967] и др., выдающиеся мыслители и экономисты XX в. так или иначе стремились ухватить и описать одну и ту же особенность сегодняшнего мира.

В эпицентре внимания ученых оказались Соединенные Штаты Америки, где проявления информационной революции наиболее существенны. Информация стала новым локомотивом американской экономики, коммерческое значение информационных ресурсов[1] заметно возросло. При этом известный отечественный исследователь американской политической мысли Э.Я. Баталов отмечает, что «попытки теоретического осмысления внедрения ИКТ в политику и их влияния на демократический процесс пока отстают от практики — и в Соединенных Штатах, и в остальном мире. Что касается серьезных теорий или целостных концепций, то их пока вообще нет» [Баталов, 2010: 360]. Однако очевидно, что формирование информационного общества, развитие киберпространства в США оказывают влияние на эволюцию американской политической идеологии, а традиционные для Соединенных Штатов идеи

[1] Под информационными ресурсами в целом автор понимает физически осязаемую технологическую инфраструктуру и смысловое содержание, создаваемое и передаваемое с ее помощью.

демократии, либерализма, индивидуализма обусловили отношение к информационным ресурсам как к частной собственности.

В этой связи одним из ключевых становится вопрос, кто должен обеспечивать конфиденциальность и неприкосновенность персональной информации. С одной стороны, традиционно эту функцию выполняло государство [Рогов, 2005: 6]. Исторически это было связано с необходимостью содержать вооруженные силы и поддерживать правопорядок. В XXI в. задача обеспечения безопасности не потеряла актуальности, но при этом заметно трансформировалась, охватив в том числе информационную сферу. Защита информации стала рассматриваться как одна из важнейших функций государственных органов.

С другой стороны, охрана персональных данных — прерогатива их владельца. Количество и характер информации, требующей защиты, всегда индивидуальны. Каждый субъект права самостоятельно определяет, в отношении каких сведений необходимо обеспечить конфиденциальность, а главное — какими средствами. Более того, в силу динамики развития информационных технологий в современном мире объем частной информации постоянно увеличивается, и требуются все новые способы ее защиты. Государство при этом выступает лишь как один из субъектов поддержания безопасности и не несет непосредственной ответственности за неприкосновенность информации своих граждан. При таком подходе доступ, например, специальных служб или правоохранительных органов к персональным данным является нарушением конфиденциальности и требует соблюдения специальной юридической процедуры.

В целом именно поиск баланса между защитой частной информации и обеспечением безопасности лежал в основе эволюции американской политики в информационной сфере вообще и в отношении проблемы охраны персональных данных в частности. С развитием информационных технологий и повсеместным распространением интернета в американском обществе противоречие между двумя описанными подходами только обострилось.

С середины 1990-х годов многие исследователи обращали внимание на эту дилемму. Как отмечает сотрудник факультета права Джорджтаунского университета Мэри де Роса, «недоверие к сильному государству всегда являлось частью американского наследия. Во многом в силу этого недоверия американцы в большей степени, по сравнению с гражданами других стран, противятся идее о необходимости предоставлять персональные данные государственным органам. Они опасаются того, что государство использует эту информацию не по назначению» [De Rosa, 2003].

Вместе с тем, как утверждает Бенджамин Уиттс, сотрудник Института Брукингса, сама идея конфиденциальности информации «устарела и не соответствует требованиям современного глобализирующегося мира, окутанного информационной сетью» [Wittes, 2011: 2]. Он отмечает, что понятие «конфиденциальность информации» (*privacy*) всегда крайне тяжело поддавалось юридическим определениям. При этом данная проблема усилилась многократно в результате распространения сведений о каждом из нас и появления возможности анализировать разнообразную частную информацию систематически в режиме реального времени.

О необходимости усиления государственного контроля над персональными данными еще до террористических атак 11 сентября писал американский исследователь Амитай Этциони. В книге «Границы частной информации» ('The limits of privacy') он обращал внимание на то, что «гарантия конфиденциальности информации — привилегия» [Etzioni, 2000]. Понятия «безопасность», «общественный порядок» он относил к категории «общего блага» (*public good*), при этом неприкосновенность личных сведений, разумеется, ученый причислял к разряду «индивидуальных благ». В конце XX в., по его мнению, благодаря распространению информационных технологий безопасность частной информации вошла в противоречие с интересами общества. Основная идея книги А. Этциони заключалась в том, что существовавшие (на конец 1990-х годов) нормы гарантии конфиденциальности не отвечали общественным интересам. По его мнению, к персональным данным государство будет относиться «ответственно», поэтому никаких опасений быть не должно.

Сотрудница юридического отдела американского Конгресса Джина Мари Стивенс отмечала, что «личная информация, анализ которой может быть полезен при разработке превентивных действий, содержится во множестве частных и государственных баз данных. Среди них есть финансовые организации (банки, казино, брокерские фирмы), образовательные, а также туристские и медицинские учреждения, ветеринарные клиники, производители средств и услуг связи» [Stevens, 2003: 3].

Однако абсолютное большинство американских экспертов сошлись во мнении, что конфиденциальность информации необходимо сохранять, а государственный контроль над этой сферой несовместим с идеалами свободы [Lessons from identity trail, 2009: 124]. Как утверждают исследователи, доступ третьих лиц к персональным данным, скорее всего, повлечет за собой их разглашение, что, естественно, нанесет ущерб владельцу информации.

Угроза утраты конфиденциальности осложняется и тем, что далеко не всегда можно выяснить, кто является злоумышленником. В современном американском обществе существует высокий спрос на самые разные персональные данные. Например, Александр Никс, глава компании «Cambridge Analytics», заявляет, что его фирма закупает подобные сведения «из всех возможных источников: кадастровых списков, бонусных программ, телефонных справочников, клубных карт, газетных подписок, медицинских баз»[2]. При этом он утверждает, что изобретенный им алгоритм анализа этой информации в сочетании с маркетинговыми и прочими технологиями обеспечил победу Дональду Трампу на президентских выборах.

Эксперты Международного экономического форума указывают, что существующие «традиционные» нормы защиты персональных данных не отвечают условиям современности. «Они основаны на вычислительной архитектуре 1970-х годов, когда государство или предприятие собирало определенное количество информации для решения конкретной задачи. После ее выполнения данные уничтожались»[3]. Очевидно, что с распространением цифровых технологий, развитием глобального информационного пространства подобное обращение с информацией просто невозможно. Эти идеи разделяют и исследователи из Университета Джорджа Вашингтона, которые отмечают, что «широкое использование новых сложных технологий привело к заметному усилению контроля, осуществляемого правоохранительными органами, предоставлению правительствам беспрецедентных законодательных полномочий и технологических возможностей для массовой слежки за гражданами» [Solove, 2004: 1701].

Поскольку США — абсолютный мировой лидер по степени проникновения интернета в общество, очевидно, что данная проблема приобрела там особую актуальность, и обращение к изучению американского опыта представляет особый интерес. Несмотря на то что конфиденциальность частной информации относится скорее к вопросам внутренней политики, она имеет и определенное международное измерение. Как отмечает Збигнев Бжезинский, «одновременно обеспечивать свободу Интернета и гарантировать информационную безопасность — нелегкая задача, особенно с учетом децентрализации и быстрого развития интернет-пространства. Как

---

[2] Расследование Das Magazin: как Big Data и пара ученых обеспечили победу Трампу и Brexit // The Insider. 06.12.2016. Доступ: http://theins.ru/politika/38490 (дата обращения: 10.12.2016).

[3] Unlocking the value of personal data: From Collection to Usage // World Economic Forum. February 2013. Available at: http://www3.weforum.org/docs/WEF_IT_UnlockingValuePersonalData_CollectionUsage_Report_2013.pdf (accessed: 03.12.2016).

и в Мировом океане, обеспечение справедливого регулирования и свободы на этих просторах во многом зависит от Америки, поскольку в настоящее время Штаты контролируют большую часть доступа к киберпространству. Обеспечивая свободу Интернета, эта система, тем не менее, не запрещает отдельным государствам, например Китаю или Ирану, ограничивать своим гражданам доступ в Интернет, хотя Соединенные Штаты уже поставили себе первоочередную задачу публично выступить против подобных ограничений» [Бжезинский, 2012: 63].

Дополнительную актуальность исследованию данной проблемы придают недавние законодательные инициативы в области регулирования сферы информации, принятые в Российской Федерации. Положения «пакета Яровой»[4], вызвавшие наибольшую критику общественности, обязывают операторов связи хранить в течение полугода и предоставлять российским спецслужбам конфиденциальные данные российских граждан. Закон был принят в кратчайшие сроки вопреки мнению экспертов и представителей отрасли[5], а также правительства[6], не говоря уже о правозащитниках и средствах массовой информации. Резко негативную оценку этой законодательной инициативе дал даже Эдвард Сноуден[7], до сих пор вынужденный скрываться в России. Особое беспокойство вызывает практически единогласное мнение сторон, которое заключается в том, что принятые меры не решат проблему безопасности. С этой точки зрения интересно проанализировать опыт США, где сразу же после террористических атак в Нью-Йорке и Вашингтоне были введены чрезвычайно жесткие положения относительно полномо-

---

[4] «Пакет Яровой» получил свое название по имени депутата Государственной Думы И.А. Яровой, предложившей его к рассмотрению. На самом деле это два документа: Федеральные законы от 6 июля 2016 г. № 374-ФЗ «О внесении изменений в Федеральный закон “О противодействии терроризму” и отдельные законодательные акты Российской Федерации в части установления дополнительных мер противодействия терроризму и обеспечения общественной безопасности» (доступ: http://kremlin.ru/acts/bank/41108, дата обращения: 10.11.2016) и № 375-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации и Уголовно-процессуальный кодекс Российской Федерации в части установления дополнительных мер противодействия терроризму и обеспечения общественной безопасности» (доступ: http://kremlin.ru/events/president/news/52489, дата обращения: 10.11.2016). Оба были подписаны Президентом РФ 7 июля 2016 г.

[5] Официальная позиция РАЭК по «законопроекту Яровой» (№ 1039149-6 — второе чтение) // Российская ассоциация электронных коммуникаций. 21.06.2016. Доступ: http://raec.ru/times/detail/5225/ (дата обращения: 23.11.2016).

[6] Глава Минкомсвязи признал, что из-за «пакета Яровой» связь может подорожать на 300% // NewsRU.com. 30.06.2016. Доступ: http://www.newsru.com/russia/30jun2016/mincom.html (дата обращения: 22.11.2016).

[7] Snowden E. Mass surveillance doesn’t work // Twitter. 25.06.2016. Available at: https://twitter.com/Snowden/status/746685673650913281?ref_src=twsrc%5Etfw (accessed: 12.11.2016).

чий специальных служб в сфере доступа к конфиденциальной информации, которые, как и «пакет Яровой» в России, мотивировались именно необходимостью повышения эффективности антитеррористических мер.

* * *

Отцы-основатели Соединенных Штатов заложили в основу государственного строя положение о том, что в случае подозрения гражданина в противоправной деятельности любые досудебные действия, связанные с доступом правоохранительных органов к конфиденциальной информации, возможны только при условии разрешения соответствующего органа, а именно судьи. Данная норма была зафиксирована четвертой поправкой к Конституции США[8]. Американским законодательством предусмотрены и соответствующие процедуры. Сбор конфиденциальных данных, таким образом, был необходим для предоставления в качестве доказательств в суде.

По мере развития информационных и телекоммуникационных технологий эта норма применялась и в отношении прочих средств связи, появлявшихся и распространявшихся в Соединенных Штатах. Спустя 200 лет после подписания Конституции информационное взаимодействие посредством цифровых технологий почти полностью заменило другие средства коммуникации.

В начале 1990-х годов, когда интернет приобрел заметное политическое значение, информационная политика Белого дома носила в целом либеральный характер. В тот период вопросам безопасности уделялось намного меньше внимания, чем сейчас. Приоритетом государства были стимулирование информационного сектора, поддержка предпринимательства в области создания глобальной информационной инфраструктуры. Данные положения были высказаны еще в ходе предвыборной кампании президента У. Клинтона. В книге «Народ прежде всего», подробно описывающей видение его администрацией своей будущей политики, этой теме было уделено особое внимание. Победа в биполярном противостоянии сравнивалась с окончанием Второй мировой войны. В связи с этим У. Клинтон предлагал «масштабный план военной конверсии, в рамках которого многие элементы информационной инфраструктуры получили бы гражданское назначение» [Clinton, Gore, 1992: 75–77].

---

[8] Конституция США. Поправка IV. «Право народа на охрану личности, жилища, бумаг и имущества от необоснованных обысков и арестов не должно нарушаться. Ни один ордер не должен выдаваться иначе, как при наличии достаточного основания, подтвержденного присягой или торжественным заявлением; при этом ордер должен содержать подробное описание места, подлежащего обыску, лиц или предметов, подлежащих аресту».

Предполагалось к 2015 г. «обеспечить каждый дом, классную комнату, лабораторию доступом к Сети». Информационные товары и услуги должны были стать локомотивом американской экономики. Судя по всему, реализация предложенной программы полностью оправдала себя и даже превзошла все ожидания.

После победы У. Клинтона на выборах 1992 г. некоторые эксперты высказывали идею о том, что технологическая повестка дня пришедшей администрации — «обеспечить Америке прорыв в новую эру»[9], причем ее реализация была поручена вице-президенту Альберту Гору. Официальные материалы Белого дома 1993 г. свидетельствуют о том, что вопросы технологической модернизации стали наиболее приоритетными[10].

В период правления У. Клинтона ведущими считались экономические, коммерческие факторы развития интернета, соответственно формировалась и государственная политика в области гарантий конфиденциальности. Доступ к частной информации разрешался правоохранительным органам в исключительных случаях и согласно специальной процедуре, предусматривавшей санкцию судебной власти для предоставления доказательств в суде.

Террористические атаки 11 сентября 2001 г. заставили американское руководство пересмотреть подходы к обеспечению национальной безопасности в сторону их общего ужесточения, в частности за счет качественного расширения полномочий специальных служб в информационной сфере. Последовавшая за этим масштабная деятельность данных структур в области доступа к конфиденциальной информации граждан в теоретическом отношении опиралась в первую очередь на принцип превентивных действий, который лег в основу Стратегии национальной безопасности 2002 г.[11]

Термин «превентивная оборона», предложенный главой Пентагона У. Перри в середине 1990-х годов [Carter, Perry, 1999], подразумевал использование средств дипломатии, международно-политического воздействия на потенциальную угрозу с тем, чтобы она не превратилась в реальную. При этом администрация Дж. Буша-мл. в Стратегии национальной безопасности оставляла за Соединен-

---

[9] Clinton to promote high technology, with Gore in charge // The New York Times. 10.11.1992. Available at: http://www.nytimes.com/1992/11/10/science/clinton-to-promote-high-technology-with-gore-in-charge.html (accessed: 12.11.2016).

[10] Clinton W.J., Gore A. Technology for America's economic growth, a new direction to build economic strength. 22.02.1993. Available at: https://web.archive.org/web/20070619205603/http://www.itsdocs.fhwa.dot.gov/JPODOCS/BRIEFING/7423.pdf (accessed: 12.11.2016).

[11] National Security Strategy // The White House. Washington, D.C., 2002. Available at: https://georgewbush-whitehouse.archives.gov/nsc/nss/2002/ (accessed: 12.11.2016).

ными Штатами возможность вести и превентивные *военные* действия против потенциальной угрозы.

Сбор конфиденциальной информации в таком случае осуществлялся не в целях предоставления доказательств в суде, но для проведения специальных, в том числе военных, операций (например, таких как задержание С. Хуссейна или ликвидация У. бен Ладена). Деятельность спецслужб при этом распространялась не только на граждан США, но и на всех пользователей основных американских провайдеров телекоммуникационных услуг (Microsoft, Google, Apple, Facebook, Skype и др.). Очевидно, что при соблюдении «традиционной» юридической процедуры (разрешение судьи или прокурора) решить поставленные задачи, связанные с проведением превентивных действий в отношении подозреваемых, было бы невозможно.

Принцип «превентивной обороны», принятый на вооружение сразу же после террористических атак, впервые был формально закреплен в законе «Патриот» 2001 г.[12] Подготовка и принятие одного из самых масштабных законодательных актов в сфере национальной безопасности Соединенных Штатов заняли всего 45 дней после трагических событий в Нью-Йорке и Вашингтоне.

В этой связи многие специалисты отмечали, что «после каждой террористической атаки законодательные инициативы, ранее не имевшие шанса на успех, предлагались вновь. Конечной целью проводимой политики было усиление государственных полномочий в сфере доступа к конфиденциальной и частной информации» [Digital privacy, 2008: 410].

Закон «Патриот» представлял собой комплекс мер, направленных на противодействие террористической угрозе на территории США и за рубежом. Этот документ, в частности, предусматривал меры наказания в отношении лиц и организаций, предоставляющих террористам финансовые средства. Законом была усилена защита границ США, предполагались депортация и наказание иностран-

[12] В российской литературе название этого закона переводят по-разному, наиболее часто встречающиеся переводы — «Закон о патриотизме», «Закон по борьбе с терроризмом», однако USA PATRIOT Act — аббревиатура, расшифровка которой звучит как «Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001», дословно на русский язык это можно перевести как «Закон об объединении и укреплении Америки через обеспечение адекватными инструментами, необходимыми для перехвата и предотвращения терроризма». В данной работе на русском языке используется обозначение «закон “Патриот”». См. подробнее: H.R.3162 — Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001 // Library of Congress. Available at: https://www.congress.gov/bill/107th-congress/house-bill/3162/actions (accessed: 13.11.2016).

цев, подозреваемых в террористической деятельности на территории Америки. Согласно поправкам, внесенным в уголовное законодательство, вводилось уголовное наказание за новый вид преступлений — террористические атаки на транспортной инфраструктуре, применение биологического оружия, предоставление убежища и иной поддержки террористам и т.д.[13]

Наибольшее возмущение общественности вызвали положения закона «Патриот», связанные с расширением полномочий американских спецслужб в области доступа к конфиденциальной информации. Американский союз защиты гражданских свобод, крупнейшая в США правозащитная организация, неоднократно выступал с заявлениями о несоответствии положений принятого документа Конституции Соединенных Штатов. На каждом этапе рассмотрения законопроекта Конгрессом союз направлял в Сенат и Палату представителей письма с просьбами пересмотреть решение о принятии закона[14]. Мнение правозащитников, однако, не было услышано, и закон «Патриот» был принят 26 октября 2001 г.

Согласно разделу 215, вызвавшему наибольшие разногласия в обществе, «американские спецслужбы имеют право получать только телефонную “метаинформацию”, т.е. с какого и на какой номер, откуда и когда осуществлялся звонок, но не содержание самого телефонного разговора»[15]. Данная норма действовала лишь в отношении американцев, однако борьба с террористической угрозой подразумевала необходимость анализа конфиденциальной информации и иностранных граждан.

Для ее получения в США существовала другая нормативная база — закон «Об иностранной разведке»[16], действовавший с 1978 г.

---

[13] Подробный юридический анализ положений закона «Патриот» был выполнен Исследовательской службой Конгресса: Doyle C. The USA PATRIOT Act: A legal analysis // Congressional Research Service. Available at http://fas.org/irp/crs/RL31377.pdf (accessed: 10.10.2016).

[14] Letter to Congress urging changes in provisions of anti-terrorism legislation // American Civil Liberties Union (ACLU). 02.10.2001. Available at: https://www.aclu.org/letter/letter-congress-urging-changes-provisions-anti-terrorism-legislation (accessed: 12.11.2016); Letter to the House urging them to vote ‘No’ on the PATRIOT Act // ACLU. 12.10.2001. Available at: https://www.aclu.org/letter/letter-house-urging-them-vote-no-patriot-act (accessed: 12.11.2016); Letter to the Senate urging rejection on the final version of the USA PATRIOT Act // ACLU. 23.10.2001. Available at: https://www.aclu.org/letter/letter-senate-urging-rejection-final-version-usa-patriot-act (accessed: 12.11.2016); Letter to the House urging rejection on the final version of the USA PATRIOT Act // ACLU. 23.10.2001. Available at: https://www.aclu.org/letter/letter-house-urging-rejection-final-version-usa-patriot-act (accessed: 12.11.2016).

[15] USA PATRIOT Act. Available at: https://www.gpo.gov/fdsys/pkg/PLAW-107publ56/pdf/PLAW-107publ56.pdf (accessed: 10.10.2016).

[16] Foreign Intelligence Surveillance Act (FISA), 1978. Available at: https://it.ojp.gov/PrivacyLiberty/authorities/statutes/1286 (accessed: 12.10.2016).

История его принятия заслуживает отдельного внимания в контексте изучаемой проблематики. В 1975 г. в результате расследования Конгресса о деятельности Агентства национальной безопасности выяснилось, что «АНБ фактически незаконно перехватывало международные сообщения в течение 20 лет. При этом сотрудники Агентства не получали ни ордера судьи, ни другого разрешения на доступ к тайне переписки» [Klosek, 2007: 38]. Закон «Об иностранной разведке» был призван подвести законодательную базу под деятельность АНБ. Согласно разделу № 702 этого нормативного акта условием получения разрешения на доступ к конфиденциальной информации иностранных граждан было наличие весомых доказательств того, что подозреваемый занимается террористической или иной антиамериканской деятельностью. Эти доказательства тщательно документировались, а разрешение не нарушало четвертую поправку к Конституции США. Если полученная информация не представляла ценности для американских спецслужб, она подлежала уничтожению[17].

В ходе реформы законодательной базы в контексте борьбы с терроризмом в 2001 г. в закон «Об иностранной разведке» были внесены поправки, регламентировавшие доступ к персональным данным посредством цифровых технологий, а также упрощалась процедура получения разрешения, едва ли вообще без участия специальных судов. Нола Бреглио из Йельского университета отмечала, что с принятием закона «Патриот» «во всех случаях, связанных с иностранными агентами, следователи уже не соблюдали нормальные процедуры криминального делопроизводства» [Breglio, 2003].

Следует отметить, что Верховный Суд США не давал заключения по положениям закона «Патриот» о доступе к электронным сообщениям на стадии обсуждения [Sottiaux, 2008: 303]. Только спустя год после принятия этого законопроекта, 10 сентября 2002 г., в юридическом комитете Сената США прошли слушания, посвященные анализу результатов практического применения данного документа. Председатель комитета сенатор Патрик Лихи, ссылаясь на заключение Министерства юстиции США, заявил, что изменения в законе «Об иностранной разведке» позволяют американским специальным службам получать доступ к конфиденциальной информации иностранцев и даже американских граждан в обход четвертой поправки к Конституции[18]. По его мнению, после событий

[17] NSA fact sheet on Section 215 of the PATRIOT Act // National Security Agency. Available at: https://fas.org/irp/news/2013/06/nsa-sect215.pdf (accessed: 12.10.2016).

[18] The USA PATRIOT Act in Practice: Shedding Light on the FISA Process. Hearing before the Committee on the Judiciary. 10.09.2002. Available at: http://fas.org/irp/congress/2002_hr/091002transcript.html (accessed: 22.10.2016).

2001 г. закон «Об иностранной разведке» более не выполнял своих первоначальных функций.

Судебный ордер по-прежнему требовался для получения персональных данных американских и иностранных граждан при подозрении их в совершении преступления — при этом заводилось уголовное дело. Однако если лицо подозревалось в террористической деятельности, то участия судебных органов не требовалось. Реализация принципа «превентивных действий» была просто несовместима с обычной работой судов и уголовным делопроизводством. Спустя десятилетие благодаря разоблачениям Э. Сноудена выяснилось, что соответствующие структуры обладали серьезными технологическими инструментами сбора конфиденциальной информации.

Таким образом, для упреждения теракта и принятия превентивных мер на этапе планирования террористических действий американские спецслужбы могли получить практически любые данные о собственных или иностранных гражданах. На основе таких сведений, как, например, история просмотра интернет-сайтов, запрошенные издания в библиотеках, наименование оплаченных товаров через платежные системы и др., можно было составить исчерпывающее представление о любом человеке. Генри Киссинджер в своей книге о новом мировом порядке назвал подобную деятельность «опережающей аналитикой» [Киссинджер, 2015]. Идея авторов закона «Патриот» заключалась в том, что, оперативно получив информацию о человеке, который, к примеру, изучает литературу об изготовлении самодельного взрывного устройства или приобретает оружие в магазине, спецслужбы смогут упредить угрозу до того, как злоумышленник совершит задуманное. Эту точку зрения поддерживал американский исследователь Ричард Хьюбэнк, который утверждал, что «стратегическая разведка» играет особую роль в противодействии террористической угрозе в условиях развития информационного пространства. «Стратегическая разведка используется для долгосрочного планирования. Анализ информации с помощью компьютерных технологий позволяет спрогнозировать террористическую атаку и подготовить наиболее приемлемый способ противодействия и упреждения» [Hughbank, 2010: 32].

С одной стороны, подобная деятельность позволяет эффективно бороться с террористическими угрозами. С другой стороны, крайне сложно определить «грань дозволенного», объем и характер собираемой конфиденциальной информации, необходимой правоохранительным органам для принятия решения. Обладая законодательными полномочиями получать доступ к персональным данным, американские специальные службы использовали для

этого все возможные инструменты. АНБ располагало достаточно мощными технологиями, позволявшими сделать сбор частной информации по-настоящему массовым[19]. В 2014 г. научно-аналитический центр «New America Foundation» провел исследование после заявления председателя Комитета по разведке Палаты представителей США Майка Роджерса, который указал: «Программы АНБ применялись 54 раза и в каждом случае позволяли остановить и нейтрализовать террористов как на территории США, так и в Европе»[20]. Авторы исследования проанализировали дела 225 членов террористической организации «Аль-Каида», обвиненных в подготовке террористических актов в Соединенных Штатах после событий 11 сентября 2001 г. В большинстве случаев традиционные методы проведения расследований показывали наибольшую эффективность, в то время как вклад АНБ был минимален[21]. Более того, слежка за американскими гражданами вообще не дала никаких результатов.

Деятельность Агентства и других спецслужб попадала под законодательство о государственной тайне, поэтому гражданское общество не имело точного представления о масштабах их полномочий в области доступа к конфиденциальной информации. Но даже на основе открытых сведений многие эксперты били тревогу. Общественное движение «Пока не остыли чернила на тексте закона “Патриот”» (‘Before the ink was dry on the PATRIOT Act’), объединившее множество правозащитных организаций, генеральный прокурор Джон Эшкрофт и даже некоторые конгрессмены выражали протест против этого нормативного акта по причине его противоречия первой, четвертой, пятой, шестой и десятой поправкам к Конституции США [Ball, 2004: 62].

Например, журналист газеты «The New York Times» Эрик Лихтблау утверждал, что закон «Патриот» стирает юридические границы между уголовными и террористическими делами[22]. Уголовное делопроизводство направлено на то, чтобы подготовить материалы к рассмотрению в суде. Преступления, связанные с террористиче-

---

[19] Непереводимое с английского языка понятие ‘bulk data collection’ означает, что специальные службы получали доступ не к конкретной информации, а ко всему массиву данных, а впоследствии в результате анализа находили среди всего прочего именно то, что было нужно.

[20] Cahall B., Bergen P., Sterman D., Schneider E. Do NSA’s bulk surveillance programs stop terrorists? // New America. 13.01.2014. Available at: https://www.newamerica.org/international-security/policy-papers/do-nsas-bulk-surveillance-programs-stop-terrorists/ (accessed: 12.11.2016).

[21] Ibidem.

[22] Lichtblau E. U.S. uses terror law to pursue crimes from drugs to swindling // The New York Times. 28.09.2003. Available at: http://www.nytimes.com/2003/09/28/us/us-uses-terror-law-to-pursue-crimes-from-drugs-to-swindling.html?_r=0 (accessed: 12.10.2016).

ской деятельностью, были вынесены в отдельную категорию, при этом все материалы, собираемые в ходе расследования, засекречивались. По мнению американского журналиста, правоохранительные органы превышали свои полномочия и использовали их для ведения дел, не имевших отношения к терроризму.

Противники закона «Патриот» оказались даже в республиканском лагере. Так, жесткую позицию занял член Палаты представителей от штата Техас Рон Пол[23]. В октябре 2001 г. он заявлял, что окончательный текст данного документа даже не был доступен для ознакомления до процедуры голосования[24]. Этот тезис также был озвучен скандально известным режиссером и общественным деятелем Майклом Муром в документальном фильме «Фаренгейт 911».

Большое беспокойство правозащитников вызвали и обстоятельства принятия антитеррористического законодательства, прежде всего быстрота, с которой оно было проведено через Конгресс. Действительно, 19 сентября 2001 г. генеральный прокурор Дж. Эшкрофт, выступив перед парламентом, предложил необходимые меры; сенатор-демократ Патрик Лихи и член Палаты представителей республиканец Джеймс Сенсенбреннер, председатель юридического комитета, вместе с многими коллегами подготовили текст законопроекта, который 24 октября был одобрен в нижней палате 357 голосами против 66, 25 октября — в Сенате 99 голосами против 1 и подписан президентом Дж. Бушем-мл. 26 октября 2001 г.[25] Учитывая масштаб принимаемых мер, такую скорость, с которой законопроект был обсужден и рассмотрен неповоротливой американской законодательной машиной, можно считать рекордной. Профильные комитеты даже не успевали готовить заключения по тексту законопроекта, фактически вся информация об обсуждении различных положений закона «Патриот» содержится только в стенограммах заседаний.

Интересно отметить, что расширение полномочий специальных служб в сфере доступа к конфиденциальной информации граждан, вызывавшее недовольство многих представителей общественности,

---

[23] Он дважды неудачно баллотировался в президенты от Либертарианской партии. Его сын Рэнд Пол также выставлял свою кандидатуру на должность президента от Республиканской партии в 2016 г. Их позиция относительно антитеррористичекого законодательства оставалась неизменной на протяжении 15 лет.

[24] Republican representative Ron Paul of Texas. Interview by Laura Knoy on NHPR, June 5, 2007 // New Hampshire Public Radio. Available at: http://info.nhpr.org/node/13016 (accessed: 11.11.2016).

[25] H.R.3162 — Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001 // Library of Congress. Available at: https://www.congress.gov/bill/107th-congress/house-bill/3162/actions (accessed: 13.11.2016).

противоречило даже рекомендациям доклада о расследовании террористических атак 11 сентября 2001 г. В этом документе, подготовленном специальной комиссией, которая два года исследовала причины и предпосылки произошедшей трагедии, подчеркивалась необходимость соблюдения гарантий неприкосновенности частной информации[26].

Тем не менее, поскольку граждане ожидали от правительства решительных антитеррористических мер, волну общественного недовольства удалось погасить, несмотря на действия правозащитных организаций, разнообразные письма и протесты.

Можно констатировать, что в условиях крайней неопределенности и нагнетания страха перед террористической угрозой политическое руководство Соединенных Штатов смогло принять достаточно жесткие меры, направленные на контроль информационной сферы. В более спокойные времена проведение через Конгресс подобного законодательства было бы невозможно. Органы государственного управления и безопасности получали широкие полномочия в сфере доступа к конфиденциальной информации граждан, при этом механизмы и инструменты использования этих полномочий не были прописаны законодательно.

С вступлением в силу закона «Патриот» наиболее жесткая волна критики утихла. 26 октября президент Дж. Буш-мл., подписывая этот документ, заявил, что он «позволит эффективно противодействовать террористической угрозе, в результате которой уже были убиты тысячи невинных ничего не подозревающих людей. У террористов нет морали, у них нет совести, с ними невозможно вести разумный диалог»[27].

Помимо конгрессменов и представителей исполнительной власти в поддержку законопроекта высказались и некоторые эксперты исследовательских центров. Например, Пол Розенцвейг, сотрудник фонда «Heritage», неоднократно в публичных выступлениях отвечал на критику закона «Патриот». Его основные идеи были изложены в статье «Гражданские свободы и ответ терроризму» [Rosenzweig, 2004], где он утверждал, что те, кто боится усиления полномочий правительства, ошибочно предлагают запретительные меры (*prohibition*), тогда как в сложившейся ситуации необходимо

---

[26] The 9/11 Commission Report // The National Commission on Terrorist Attacks upon the United States. P. 394, 406. Available at: https://9-11commission.gov/report/911Report.pdf (accessed: 10.10.2016).

[27] Remarks by the President at Signing of the Patriot Act, Anti-Terrorism Legislation // The White House. 26.10.2001. Available at: https://georgewbush-whitehouse.archives.gov/news/releases/2001/10/20011026-5.html (accessed: 12.10.2016).

противодействовать терроризму посредством законодательных, организационных и технических решений, предусматривающих ответственность органов власти.

В определенной степени сторонником законопроекта можно назвать профессора Джозефа Итона, выступающего с середины 1980-х годов в поддержку введения в США универсального удостоверения личности[28]. В 2003 г. вышла обновленная редакция его книги «Privacy Card», в которой он привел множество аргументов в пользу того, что такая мера может оказать положительный эффект в борьбе против терроризма [Eaton, 2003].

Сложно сказать, насколько риторика сторонников закона «Патриот» соответствовала реальности, но благодаря ей американская общественность была убеждена в том, что для предотвращения террористической угрозы необходимо собрать и проанализировать максимально исчерпывающую информацию о каждом человеке, и только это позволит сделать вывод о возможной подготовке очередной атаки. Попытки предотвратить принятие закона потерпели полный провал. Впрочем, ряд правозащитных организаций и политиков продолжали его критиковать: по состоянию на март 2005 г. администрации 371 города и 4 легислатуры штатов приняли резолюции с требованиями сократить полномочия государства, предусмотренные в законе «Патриот» (в январе 2004 г. подобных резолюций было 236, а в 2002 г. — 22) [Keenan, 2005: 99].

* * *

В 2013 г. мощнейшая волна критики антитеррористического законодательства возобновилась в связи с публикациями бывшего сотрудника АНБ Эдварда Сноудена[29]. Его разоблачения касались технической стороны вопроса. Учитывая, что данный аспект оставался за рамками законодательства, представить себе масштабы деятельности в этой сфере было невозможно.

Благодаря сведениям, обнародованным Э. Сноуденом, стало известно, что программа PRISM позволяла американским специальным службам получать данные провайдеров интернет-связи и различных интернет-сервисов, включая самые популярные совре-

---

[28] Как известно, в США не существует универсального удостоверения личности. Наиболее популярными документами для идентификации человека являются водительское удостоверение и заграничный паспорт, получаемые не всеми гражданами. Идея введения универсального удостоверения личности всегда встречает сопротивление среди американских правозащитников.

[29] NSA slides explain the PRISM data-collection program // The Washington Post. 06.06.2013; updated 10.07.2013. Available at: http://www.washingtonpost.com/wp-srv/special/politics/prism-collection-documents/ (accessed: 12.11.2016).

менные ИТ-компании[30]. Первой к программе PRISM присоединилась Microsoft — в 2007 г., затем Yahoo, Google, Facebook, PalTalk, YouTube, Skype, America Online и в 2012 г. — Apple. Стоит отметить, что их клиентами являются далеко не только американские граждане. Деятельность большинства этих компаний носит глобальный характер, поэтому неудивительно, что среди жертв оказались и иностранцы, включая даже некоторых мировых лидеров. В частности, выяснилось, что американские спецслужбы имели доступ к конфиденциальной информации канцлера ФРГ Ангелы Меркель[31].

После разоблачений Э. Сноудена установленные законодательством полномочия АНБ и других американских спецслужб в сфере доступа к персональным данным были суммированы в специальном докладе Белого дома[32].

Сам директор АНБ и по совместительству руководитель американского стратегического киберкомандования Кейт Александер был вынужден «оправдываться» перед законодательной властью. Так, 18 июля 2013 г. прошли открытые слушания в Комитете по разведке Палаты представителей, на которых генерал К. Александер заявил, что если бы такая программа, как PRISM, существовала ранее, можно было бы предотвратить террористические акты 11 сентября 2001 г.[33]

После скандальных разоблачений бывшего сотрудника АНБ телекоммуникационные компании, попавшие в «список Сноудена», заняли достаточно жесткую позицию, отвергнув все обвинения.

Microsoft опубликовала опровержение обнародованных данных через газету «The Guardian» — ту самую, к которой обратился и Э. Сноуден в начале скандала. В заявлении Microsoft говорится,

---

[30] Наиболее противоречивой и скандальной из всех программ, о которых рассказал Эдвард Сноуден, оказалась PRISM (не аббревиатура, а название, но при этом во всех источниках пишется заглавными буквами). Помимо нее, однако, бывший сотрудник АНБ рассказал и о других проектах американских специальных служб. Подробнее о них — в обзоре российского эксперта ПИР-Центра Олега Демидова: Демидов О. Десять разоблачений Сноудена, которые потрясли мир: как ответит Россия и ее партнеры // ПИР Центр. Доступ: http://www.pircenter.org/media/content/files/11/13814320770.pdf (дата обращения: 12.11.2016).

[31] Watt N., Mason R. Angela Merkel phone-bugging claims are result of Snowden leaks, MP claims // The Guardian. 24.10.2013. Available at: https://www.theguardian.com/world/2013/oct/24/angela-merkel-bugging-snowden-leaks-mp (accessed: 10.11.2016).

[32] Obama administration white paper on NSA surveillance oversight // The Washington Post. Available at: http://apps.washingtonpost.com/g/page/politics/white-house-surveillance-reform-plan/388/ (accessed: 10.10.2016).

[33] Congressional Hearings. June 18, 2013. House Select Intelligence Committee Holds Hearing on Disclosure of National Security Agency Surveillance Programs // Congressman Lynn Westmoreland official website. Available at: https://westmoreland.house.gov/images/user_images/gt/6-19-13%20Intel%20Hearing%20Transcript%20NSA%20Leaks.pdf (accessed: 20.11.2016).

что компания «сотрудничала с американским правительством как в целях правоохранительной деятельности, так и в интересах национальной безопасности. Передача данных о клиентах осуществлялась в соответствии с принятыми законодательными процедурами» («we provide customer data only in response to legal processes»). Кроме того, в заявлении отмечено, что в ряде случаев органам государственной безопасности было отказано в доступе к данным клиентов, если разглашение конфиденциальной информации подразумевало нарушение действующего законодательства[34].

Ларри Пейдж, разработчик и основатель Google, заявил, что его компания «никогда не предоставляла прямого доступа американскому или иному правительству к своим серверам, и о программе PRISM не имели представления до вчерашнего дня. Юридическая служба Google внимательно изучает все запросы о разглашении конфиденциальных данных, поступающие от американских органов государственной безопасности, и предоставление доступа происходит исключительно в соответствии с действующим законодательством»[35]. В подтверждение своих слов Л. Пейдж заявил, что Google добивается изменения норм о транспарентности и прозрачности взаимодействия телекоммуникационного сектора экономики с правительством. Он также представил ссылку на доклад, в котором содержится информация о количестве удовлетворенных и неудовлетворенных запросов американского правительства в Google относительно предоставления конфиденциальных сведений клиентов[36].

Apple также опубликовала похожее заявление, в котором разъяснила, что сотрудники компании ничего не слышали о программе PRISM и предоставляют доступ к данным своих пользователей только при условии предъявления судебного ордера. Последовав примеру коллег из Google, Apple раскрыла некоторые цифры, отражающие количество правительственных запросов на клиентскую информацию[37].

Практически такое же заявление сделал и Марк Цукерберг. О программе PRISM он не слышал, все запросы тщательно обрабатывала юридическая служба и удовлетворяла их в соответствии

---

[34] How Microsoft handed the NSA access to encrypted messages // The Guardian. 12.07.2013. Available at: https://www.theguardian.com/world/2013/jul/11/microsoft-nsa-collaboration-user-data (accessed: 20.11.2016).

[35] Page L., Drummond D. What the...? // Google Blog. 07.06.2013. Available at: http://googleblog.blogspot.ru/2013/06/what.html (accessed: 20.11.2016).

[36] Google Transparency report. Available at: http://www.google.com/transparencyreport/userdatarequests/US/ (accessed: 10.10.2016).

[37] Apple's commitment to customer privacy. 16.06.2013. Available at: http://www.apple.com/apples-commitment-to-customer-privacy/ (accessed: 20.11.2016).

с законодательством[38]. Facebook также опубликовала данные о запросах американской разведки[39].

Таким образом, все ключевые участники «сноуденгейта» — телекоммуникационные компании, предоставляющие ключевые интернет-сервисы, — подтвердили, что органы госбезопасности США обращаются с просьбами о доступе к конфиденциальной информации о клиентах. Более того, все они заявили, что удовлетворяют подобные запросы в соответствии с принятым американским законодательством. Вместе с тем, как утверждают ряд экспертов[40], прямой доступ к серверам компаний мог быть обеспечен незаметно, т.е. они могли даже не знать о том, что такая деятельность ведется. Важно отметить, что судебный ордер требовался только для того, чтобы собрать информацию об американском гражданине, получение же сведений об иностранцах проходило без какой-либо юридической санкции.

Помимо обнародования запросов спецслужб на раскрытие конфиденциальных данных лидеры компаний совместно подписали письмо в адрес президента США с требованием провести организационно-правовую реформу доступа органов государственной безопасности к частной информации граждан[41]. Решение проблемы авторы письма видели в повышении ответственности, отчетности перед законодательными и судебными ветвями власти, прозрачности и транспарентности деятельности специальных служб.

Публикации Э. Сноудена спровоцировали моментальную реакцию американских законодателей. Член Палаты представителей Джеймс Сенсенбреннер, автор и инициатор закона «Патриот», заявил, что спецслужбы превысили свои полномочия и настало время «остановить практику массового сбора информации»[42]. Примечательно, что автором текста нового законопроекта о компетенции органов госбезопасности вновь выступил он же.

---

[38] Zuckerberg M. I want to respond personally to the outrageous press reports about PRISM // Facebook.com. Available at: https://www.facebook.com/zuck/posts/10100828955847631 (accessed: 15.11.2016).

[39] Facebook Global Government Requests Report. Available at: https://www.facebook.com/about/government_requests (accessed: 15.11.2016).

[40] Gellman B., Poitras L. Documents: U.S. mining data from 9 leading Internet firms; companies deny knowledge // The Washington Post. 07.06.2013. Available at: https://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story.html (accessed: 12.11.2016).

[41] Open letter to the Senate on the USA Freedom Act // Global Government Surveillance Reform. Available at: www.reformgovernmentsurveillance.com/ (accessed: 11.11.2016).

[42] Roberts D. Patriot Act author prepares bill to put NSA bulk collection ‘out of business’ // The Guardian. 10.10.2013. Available at: https://www.theguardian.com/world/2013/oct/10/nsa-surveillance-patriot-act-author-bill (accessed: 20.11.2016).

В ходе широкого обсуждения американское правительство признало необходимость пересмотра антитеррористического законодательства и сокращения возможностей специальных служб по сбору персональных данных. Во время слушаний в Конгрессе по вопросам реформы правового обеспечения АНБ в первую очередь рассматривался законопроект «О свободе» (USA FREEDOM Act)[43], который поддержали представители как Демократической, так и Республиканской партий[44].

В отличие от условий 2001 г., новый закон разрабатывался в более спокойной обстановке. Американские законодатели осознали, что технологические возможности не соответствуют действовавшей на тот момент юридической практике. К тому же закон «Патриот» и ряд директив, составлявших основу юридических полномочий специальных служб в области доступа к конфиденциальной информации, позволяли неоднозначно трактовать существовавшие юридические тексты. При этом эффективность деятельности АНБ и других подобных структур представлялась крайне сомнительной.

В силу указанных обстоятельств принять оперативные меры, устраивавшие все стороны, после публикации скандальных материалов летом 2013 г. не удалось. Обсуждение различных вариантов реформы затянулось на два с половиной года.

В январе 2014 г. авторы закона «Патриот» республиканец Джеймс Сенсенбреннер и демократ Патрик Лихи опубликовали статью, в которой утверждали, что американское разведывательное сообщество не справилось с поставленной задачей, превысило полномочия, в связи с чем назрела необходимость изменения законодательства[45]. Весной 2015 г., когда рассмотрение законопроекта «О свободе» вступило в финальную стадию, проблема компетенции спецслужб стала предметом обсуждения во время предвыборной президентской кампании.

---

[43] USA FREEDOM Act является аббревиатурой: ‘Uniting and Strengthening America by Fulfilling Rights and Ensuring Effective Discipline Over Monitoring Act’, что дословно переводится как «Законопроект об укреплении и усилении Америки посредством реализации прав человека и гарантии строгой дисциплины при осуществлении мониторинга». В данной работе на русском языке используется обозначение «закон “О свободе”».

[44] В Конгрессе 113-го созыва законопроект рассматривался в Палате представителей под номером H.R.3361 (Available at: https://www.congress.gov/bill/113th-congress/house-bill/3361, accessed: 20.11.2016). Инициативу республиканца Джеймса Сенсебреннера поддержали 80 демократических и 72 республиканских членов Палаты. В 2014 г. он не был принят, однако его обсуждение продолжилось после очередных выборов.

[45] Leahy P., Sensenbrenner J. The case for NSA reform // Politico. 28.10.2013. Available at: http://www.politico.com/story/2013/10/leahy-sensenbrenner-nsa-reform-098953 (accessed: 23.11.2016).

Шестеро из участников президентских праймериз были действующими конгрессменами, представляли как демократов, так и республиканцев и голосовали по закону «О свободе». Мнения кандидатов разделились: в обеих партиях нашлись сторонники и противники принимаемого документа. Так, независимый конгрессмен Берни Сандерс голосовал против законопроекта[46], мотивируя свое решение тем, что он «не предусматривает достаточных мер для того, чтобы обезопасить американское общество от сбора конфиденциальной информации»[47]. В 2001 г. Берни Сандерс, член Палаты представителей от штата Вермонт, голосовал также против закона «Патриот». Аналогичного мнения придерживался и республиканский кандидат Рэнд Пол, голосуя против закона «О свободе». Весной 2016 г. он представлял штат Кентукки в Сенате США и считается одним из идеологов «Движения чаепития»[48]. Политическая программа последнего предполагает, в частности, минимальное вмешательство государства в жизнь американских граждан, поэтому, разумеется, вопрос доступа АНБ к конфиденциальной информации считается одним из ключевых. Рэнд Пол прославился как «флибустьер»[49] современной американской политики. В ходе обсуждения проблемы полномочий АНБ сенатор использовал механизм «флибустьерства», выступая в течение десяти с половиной часов с требованием прекратить сбор информации об американцах Агентством национальной безопасности.

Среди республиканских кандидатов были и «ястребы», ратовавшие за усиление военной мощи США. В данном контексте они выступили против законопроекта, мотивируя это тем, что он создаст определенную уязвимость в национальной безопасности Соединенных Штатов. Первоначально они были против пересмотра секции 215 закона «Патриот». Подобные идеи высказал сенатор от штата Флорида Марко Рубио[50]. Наиболее милитаристски настроенный

---

[46] U.S. Senate Roll Call Votes 114th Congress — On Passage of the Bill (H.R. 2048) // United States Senate. Available at: http://www.senate.gov/legislative/LIS/roll_call_lists/roll_call_vote_cfm.cfm?congress=114&session=1&vote=00201 (accessed: 24.11.2016).

[47] Bernie & Couric interview: Bernie is voting against USA FREEDOM Act // Daily Kos. 02.06.2015. Available at: http://www.dailykos.com/story/2015/06/01/1389699/-BERNIE-COURIC-Interview-Bernie-is-voting-against-USA-FREEDOM-ACT# (accessed: 24.11.2016).

[48] «Движение чаепития» — правоконсервативное ядро Республиканской партии США, объединившее американских политиков, не поддерживающих социальную повестку президента Барака Обамы, предложенную в качестве антикризисных мер во время мирового финансового кризиса 2008–2009 гг.

[49] «Флибустьерство», или «филибастер», — процедурная уловка, призванная отложить или вовсе сорвать голосование в Сенате США посредством выступления с невероятно долгими речами на трибуне. Тема «флибустьерства» затрагивается в классическом американском фильме «Мистер Смит едет в Вашингтон» 1939 г.

[50] Leary A. Rubio: USA FREEDOM Act ‘weakens national security’ // Tampa Bay Times. 02.06.2015. Available at: http://www.tampabay.com/blogs/the-buzz-florida-politics/rubio-usa-freedom-act-weakens-national-security/2232064 (accessed: 25.11.2016).

сенатор-кандидат Линдси Грэм не принимал участия в голосовании, но также заявил, что закон «О свободе» не достигнет поставленной цели, поэтому для поддержания национальной безопасности США следовало бы оставить в силе положения закона «Патриот»[51]. Стоит отметить, что Хиллари Клинтон поддержала принятие законопроекта[52].

После промежуточных выборов 2014 г. документ был вновь внесен на обсуждение в Конгресс[53]. В Палате представителей за него было отдано 338 голосов (и всего 88 против). В Сенате закон «О свободе» был одобрен на голосовании 2 июня 67 голосами против 32. Президент Б. Обама подписал его в тот же день, 2 июня 2015 г., и закон «О свободе» официально заменил закон «Патриот» (краткое сопоставление двух документов представлено в таблице).

**Сохранившиеся и изменившиеся положения закона «Патриот» после принятия закона «О свободе»**[54]

| Изменения, вступившие в силу после принятия закона «О свободе» | Положения закона «Патриот», оставшиеся без изменений |
|---|---|
| Телефонные компании обязаны хранить записи граждан, но АНБ должно получить разрешение суда на доступ к ним | ФБР все еще имеет право следить за гражданами, которые пользуются несколькими телефонами |
| Интернет-провайдеры получили большую свободу публичного раскрытия информации о запросах американских спецслужб | Правило «одинокого волка», разрешающее следить за человеком, несмотря на то что он не был замечен в связях с террористами |
| Проведение дополнительных процедур, связанных с надзором за деятельностью Специального суда по иностранной разведке (FISA Court), обязательное получение ордера на доступ к конфиденциальной информации иностранного гражданина на территории США | – |

[51] Carrol L. Lindsey Graham: FREEDOM Act means less privacy for phone records // Politifact. 04.06.2015. Available at: http://www.politifact.com/truth-o-meter/statements/2015/jun/04/lindsey-graham/lindsey-graham-freedom-act-means-less-privacy-phon/ (accessed: 23.11.2016).

[52] Hattem J. Clinton breaks silence, supports NSA reform bill // The Hill. 05.07.2015. Available at: http://thehill.com/policy/technology/241382-clinton-breaks-silence-supports-nsa-reform-bill (accessed: 23.11.2016).

[53] Nakashima E. Senate fails to advance legislation on NSA reform // The Washington Post. 18.11.2014. Available at: https://www.washingtonpost.com/world/national-security/senate-fails-to-advance-legislation-on-nsa-reform/2014/11/18/a72eb7fc-6f70-11e4-8808-afaa1e3a33ef_story.html (accessed: 20.11.2016).

[54] What makes the USA FREEDOM Act different from the PATRIOT Act? // NBC News. 03.06.2015. Available at: http://www.nbcnews.com/watch/101/what-makes-the-usa-freedom-act-different-from-the-patriot-act-456716355781 (accessed: 20.11.2016).

По опросам общественного мнения, в целом американцы негативно относятся к тому, что правительство США получает конфиденциальную информацию о гражданах[55]. Как заявляют ведущие американские правозащитные организации, принятие закона «О свободе» стало значительным шагом в реформировании полномочий органов государственной безопасности в области доступа к персональным данным. Закон заметно сокращает компетенции АНБ, хотя и сохраняется необходимость разработки дополнительных законодательных мер по обеспечению транспарентности и проведению процедур раскрытия информации[56]. Вместе с тем, несмотря на то что этот документ восстанавливает многие институты ответственности специальных служб перед Конгрессом и судебными инстанциями, продолжается его серьезная критика. Так, американский исследователь Серджио Суарез утверждает, что с принятием закона «О свободе» страна стала менее защищенной [Suarez, 2017]. Представители Центра демократии и технологий, позитивно оценивая принятие закона, обратили внимание на то, что положения о полномочиях американских спецслужб в сфере доступа к конфиденциальной информации иностранных граждан остались в силе[57].

В целом, признавая определенные успехи в области регулирования деятельности разведывательного сообщества в отношении массового сбора персональных данных, правозащитные организации все-таки скептически относились к закону «О свободе». Эксперты «Human Rights Watch» выразили сомнения в том, что его нормы позволят радикально изменить ситуацию с неправомерным доступом к конфиденциальной информации[58]. Не менее настороженно отнеслись к закону и в правозащитной организации «Electronic Frontier Foundation»[59].

---

[55] Rainie L., Madden M. Americans' privacy strategies post-Snowden // Pew Research Center. 16.03.2015. Available at: http://www.pewinternet.org/2015/03/16/Americans-Privacy-Strategies-Post-Snowden/ (accessed: 23.11.2016); Newport F. Americans disapprove of government surveillance programs // Gallup. 12.06.2013. Available at: http://www.gallup.com/poll/163043/americans-disapprove-government-surveillance-programs.aspx?utm_source=snowden&utm_medium=search&utm_campaign=tiles (accessed: 23.11.2016).

[56] Senate passes USA FREEDOM Act // ACLU. 02.06.2015. Available at: https://www.aclu.org/news/senate-passes-usa-freedom-act (accessed: 23.11.2016).

[57] O'Connor N., Geiger H. CDT supports improved version of USA FREEDOM Act // Center for Democracy & Technology. 29.07.2014. Available at: https://cdt.org/blog/cdt-supports-improved-version-of-usa-freedom-act/ (accessed: 20.11.2016).

[58] US: Pass USA FREEDOM Act. Congress should take first step toward reform // Human Rights Watch. 30.04.2015. Available at: https://www.hrw.org/news/2015/04/30/us-pass-usa-freedom-act (accessed: 26.11.2016).

[59] Cohn C., Reitman R. USA FREEDOM Act passes: What we celebrate, what we mourn, and where we go from here // Electronic Frontier Foundation. 02.06.2015. Available at: https://www.eff.org/ru/deeplinks/2015/05/usa-freedom-act-passes-what-we-celebrate-what-we-mourn-and-where-we-go-here (accessed: 24.11.2016).

Основная критика деятельности американских спецслужб в рассматриваемой сфере была связана с тем, что они занимались массовым сбором данных (*bulk records*). Иными словами, они хранили все записи, при этом в своей работе использовали лишь отдельные элементы, которые находили среди прочей информации.

Согласно новому законодательству «массовый сбор» запрещался, а также усложнялась процедура получения органами госбезопасности конфиденциальной информации[60]. Этот запрет правозащитные организации считают своей победой[61]. В остальном, однако, спецслужбы сохранили полномочия в сфере доступа к персональным данным американских и иностранных граждан. Гарантировать исключительно правомерное использование этих полномочий, разумеется, невозможно. Тем не менее принятие закона «О свободе» по крайней мере означает поворот американской политики в области конфиденциальной информации в сторону повышения контроля за деятельностью специальных служб: усложняются процедурные требования, усиливается их ответственность, а работа становится более прозрачной.

Закон, разумеется, не расставил все точки над «i» в вопросе полномочий АНБ и подобных структур в области конфиденциальной информации. Так, в ходе расследований террористических атак в Сан-Бернардино зимой 2015 г. агенты Федерального бюро расследований не смогли получить данные, содержавшиеся в айфоне погибшего террориста. Более того, они обратились в Apple с запросом открыть сотрудникам агентства доступ не только к конкретному аппарату, найденному на месте преступления, но и ко всем выпускаемым устройствам. Компания оказала полное содействие государству при расследовании террористической атаки, однако вторая просьба вызвала очередную волну общественной дискуссии. Глава Apple Тим Кук опубликовал письмо, в котором детально описал политику компании в отношении передачи конфиденциальной информации американским спецслужбам, и заверил читателей в том, что ее приоритетом является защита персональных

[60] В определенном смысле закон «О свободе» содержит схожие положения с принятым недавно в Российской Федерации законом о хранении персональных данных. Ключевая разница заключается в том, что телекоммуникационные компании являются субъектами американского права и не обязаны хранить персональные данные на физических носителях на территории Соединенных Штатов, но при этом должны предоставлять информацию американским специальным службам по их требованию при соблюдении определенной юридической процедуры.

[61] Hattem J. Obama signs NSA bill, renewing PATRIOT Act powers // The Hill. 02.06.2015. Available at: http://thehill.com/policy/nation-security/243850-obama-signs-nsa-bill-renewing-patriot-act-powers (accessed: 27.11.2016).

данных[62]. Просьбу ФБР он охарактеризовал как «беспрецедентную» и «угрожающую безопасности наших пользователей». Примечательно, что эта просьба, на которую столь горячо отреагировал глава компании, фактически заключается в снижении уровня конфиденциальности, мотивируемом интересами национальной безопасности. Судя по всему, данный инцидент еще не исчерпан, однако дальнейшие действия будут предприниматься уже новой администрацией и Конгрессом.

* * *

Американский опыт государственной политики обеспечения защиты персональных данных в контексте информационной безопасности является уникальным. Он представляет большой интерес с многих точек зрения.

США раньше остальных стран были вынуждены реагировать на новые вызовы информационной революции, а вопросы информационной безопасности очень быстро стали государственным приоритетом. За период в четверть века, в течение которого данная проблематика приобретала все большую актуальность, американская политика в рассматриваемой сфере претерпела заметные изменения.

Приход в 1993 г. к власти в США администрации президента У. Клинтона совпал с распадом Советского Союза. Это событие изменило цели и задачи военно-политического руководства Соединенных Штатов, в фокусе внимания которого оказалось экономическое развитие. Именно в этот период благодаря государственной политике интернет стал использоваться как коммерческая, а не военная технология. Менее 10 лет потребовалось на то, чтобы она распространилась по всей стране. Экономическая политика администрации У. Клинтона принесла определенные плоды, при этом вопросам информационной безопасности не придавалось первостепенное значение.

Благополучный период либерализации сферы информации в 1990-е годы резко сменился значительным усилением государственного контроля в начале 2000-х. Под предлогом борьбы с терроризмом после трагедии 11 сентября в рекордные сроки были приняты жесткие меры, в частности всеобъемлющий антитеррористический закон «Патриот», предоставившие специальным службам широкие юридические полномочия и технические возможности для получения самых разнообразных данных об американских и иностранных гражданах. При этом технологическое превосход-

[62] Cook T. A message to our customers. 16.02.2016. Available at: http://www.apple.com/customer-letter/ (accessed: 25.11.2016).

ство АНБ и прочих организаций, обеспечивающих национальную безопасность США, позволяло перехватывать практически любую персональную информацию.

Вместе с расширением компетенции специальных служб большое развитие получили и другие юридические меры, ограничивавшие доступ общественности к информации об антитеррористической деятельности. Так, были упразднены практически все правовые нормы, гарантировавшие судебную защиту. Антитеррористическое делопроизводство было отделено от уголовного, что позволяло правоохранительным органам и специальным службам пренебрегать многими юридическими процедурами. Антитеррористическая деятельность осуществлялась в соответствии с провозглашенным принципом «превентивной обороны». На основе собранной информации органы национальной безопасности осуществляли действия, направленные на уничтожение потенциальной угрозы до того, как она станет явной. Соблюдения юридической процедуры, в частности получения беспристрастного и независимого мнения суда, в таком случае, разумеется, не требовалось.

Возможно, масштабы работы АНБ с персональной информацией граждан остались бы тайной, если бы не разоблачения Эдварда Сноудена, рядового сотрудника Агентства, который опубликовал в 2013 г. множество материалов, раскрывающих технические детали данной деятельности.

Обнародование этих сведений спровоцировало новую волну общественных дискуссий относительно полномочий специальных служб в сфере доступа к конфиденциальной информации. В результате под давлением общества американская политика обеспечения неприкосновенности персональных данных была пересмотрена.

Реформа законодательства, регулирующего работу органов государственной безопасности с конфиденциальной информацией, была направлена на ограничение их полномочий, повышение транспарентности и ответственности.

Повсеместная востребованность интернет-технологий, а значит, и зависимость современного общества от ресурсов Сети заметно возрастают. Появление и распространение многочисленных мобильных средств связи способствует этому процессу. Общее количество интернет-пользователей на сегодняшний день составляет более половины населения всей планеты[63]. Очевидно, что вопросы информационной политики стали приоритетом деятельности правительств практически во всех странах мира.

---

[63] См. подробнее: Internet World Stats. Available at: http://www.internetworldstats.com/stats.htm (accessed: 27.11.2016).

Учитывая масштабы и степень мирового влияния американских информационных ресурсов, можно утверждать, что политические меры, принимаемые американским правительством, носят глобальный характер. На сегодняшний день еще рано давать какие-либо оценки последним американским новациям в сфере информационной политики и обеспечения конфиденциальности информации. Вместе с тем представляется, что ограничения деятельности американских специальных служб, направленные на поддержку открытого и прозрачного интернета, скорее всего, будут иметь более благоприятный эффект в глобальном измерении. В интересах мирового сообщества, чтобы интернет оставался открытым и прозрачным.

СПИСОК ЛИТЕРАТУРЫ

1. Баталов Э.Я. Проблема демократии в американской политической мысли XX века. М.: Прогресс-Традиция, 2010.

2. Белл Д. Грядущее постиндустриальное общество. М.: Academia, 2004.

3. Бжезинский З. Стратегический взгляд: Америка и глобальный кризис. М.: Астрель, 2012.

4. Кастельс М. Информационная эпоха. М.: ГУ ВШЭ, 2000.

5. Киссинджер Г. Мировой порядок. М.: АСТ, 2015.

6. Рогов С.М. Государство и общественное благо: мировые тенденции и российский путь. М.: Институт США и Канады РАН, 2005.

7. Ball H. The USA PATRIOT Act of 2001: Balancing civil liberties and national security. A reference book. Santa Barbara: ABC-CLIO, 2004.

8. Breglio N.K. Leaving FISA behind: The need to return to warrantless foreign intelligence surveillance // Yale Law Journal. 2003. Vol. 113. No. 1. P. 179–217.

9. Carter A.B., Perry W.J. Preventive defense: A new security strategy for America. Washington, D.C.: Brookings Institution Press, 1999.

10. Clinton B., Gore Al. Putting people first. How we can all change America. New York: Times Books, 1992.

11. De Rosa M. Privacy in the age of terror // Washington Quarterly. 2003. Vol. 26. No. 3. P. 27–41.

12. Digital privacy. Theory, technologies, and practices / Ed. by A. Acquisti. New York: Auerbach Publications, 2008.

13. Drucker P. Landmarks of tomorrow. London: Transaction Publishers, 1996.

14. Eaton J.W. The privacy card: A low cost strategy to combat terrorism. Lanham: Rowman & Littlefield, 2003.

15. Etzioni A. The limits of privacy. New York: Basic Books, 2000.

16. Gailbraith J.K. The new industrial state. New Jersey: Princeton University Press, 1967.

17. Hughbank R. Intelligence and its role in protecting against terrorism // Journal of Strategic Security. 2010. Vol. 3. No. 1. P. 31–38.

18. Keenan K.M. Invasion of privacy. A reference handbook. Santa Barbara: ABC-CLIO, 2005.

19. Klosek J. The war on privacy. Westport: Praeger Publishers, 2007.

20. Lessons from the identity trail: Anonymity, privacy, and identity in a networked society / Ed. by I. Kerr. Oxford: Oxford University Press, 2009.

21. Rosenzweig P. Civil liberties and the response to terrorism // Duquesne Law Review. 2004. Vol. 42. P. 663–723.

22. Solove D.J. Reconstructing the electronic surveillance law // The George Washington Law Review. 2004. Vol. 72. P. 1701–1747.

23. Sottiaux S. Terrorism and the limitation of rights: The ECHR and the US Constitution. Oxford; Portland: Hart, 2008.

24. Stevens G.M. Privacy: Total information awareness programs and latest developments. New York: Novinka books, 2003.

25. Suarez S. Is America safer? The USA FREEDOM Act of 2015 and what the FBI and NSA have, can, and should be doing // Law School Student Scholarship. 2017. Paper 882. Available at: http://scholarship.shu.edu/student_scholarship/882 (accessed: 24.11.2016).

26. Toffler A. The third wave. New York: Bantam Books, 1984.

27. Wittes B. Databuse: Digital privacy and the mosaic. Brookings Institution, 2011. Available at: https://www.brookings.edu/wp-content/uploads/2016/06/0401_databuse_wittes.pdf (accessed: 20.11.2016).

**P.A. Sharikov**

## CONFIDENTIALITY OF INFORMATION AND NATIONAL SECURITY POLICY: THE AMERICAN DISCOURSE IN THE XXI CENTURY

*Institute for the US and Canadian Studies,*
*Russian Academy of Sciences*
*2/3 Khlebnyi pereulok, Moscow, 123995*

Rapid development of information technologies in the second half of the 20th century, became a genuine ‘information revolution’ by the beginning of 21st century and had a profound impact on all spheres of social life, including international relations. However, as with any revolutionary phenomena, it is extremely hard to assess its effect today. In that regard, one should pay particular attention to studying the developments in the United States which was the first country in the world to enter the ‘digital era’ and accumulated a unique experience in regulating information space. Many American scholars and politicians focused on finding an optimal balance between confidentiality and national security imperatives. The paper addresses the evolution of the William Clinton, George W. Bush and Barack Obama administrations’ policies on this sensitive issue. The examination of two pieces of legislation required special attention: the USA PATRIOT Act of 2001 and the USA FREEDOM Act of 2011. The paper studies the background and the circumstances of the adoption of these acts. The author emphasizes that if the USA PATRIOT Act, which endowed the special services with large legal powers to access personal information of the American and foreign citizens, was passed within the historically shortest time period, in the wake of the 9/11 terrorist attacks, the debates on the USA FREEDOM Act triggered by Edward Snowden’s revelations

lasted for a long time and echoed throughout the 2016 presidential campaign. The author concludes that today, political regulation of information in the United States is aimed at limiting government control and making intelligence services more transparent.

***Keywords:*** United States of America, USA, national security, information security, privacy, USA PATRIOT Act, USA FREEDOM Act, FISA, PRISM, bulk data collection, Yarovaya antiterrorist legislation, Edward Snowden.

**About the author:** *Pavel A. Sharikov* — PhD (Political Science), Head of the Center for Applied Research, Institute for the US and Canadian Studies, Russian Academy of Sciences; Associate Professor at the Chair of Regional Issues of World Politics, School of World Politics, Lomonosov Moscow State University (e-mail: pasha.sharikov@gmail.com).

**Acknowledgements:** This work has been accomplished with financial support from the Russian Foundation for Humanities, research project № 15-37-01203.

REFERENCES

1. Batalov E.Ya. 2010. *Problema demokratii v amerikanskoi politicheskoi mysli XX veka* [Democracy in the American political thought of the 20th century]. Moscow, Progress-Traditsiya Publ. (In Russ.)

2. Bell D. 1973. *The coming of post-industrial society*. New York, Basic Books [Russ. ed.: Bell D. 2004. *Gryadushchee postindustrial'noe obshchestvo*. Moscow, Academia Publ.].

3. Brzezinski Z. 2012. *Strategic vision: America and the crisis of global power*. New York, Basic Books [Russ. ed.: Bzhezinskii Z. 2012. *Strategicheskii vzglyad: Amerika i global'nyi krizis*. Moscow, Astrel' Publ.].

4. Castells M. 2000. *The information age*. Cambridge, Blackwell [Russ. ed.: Kastel's M. 2000. *Informatsionnaya epokha*. Moscow, HSE Publ.].

5. Kissinger H. 2014. World order. New York, Penguin Press [Russ. ed.: Kissindzher G. 2015. *Mirovoi poryadok*. Moscow, AST Publ.].

6. Rogov S.M. 2005. *Gosudarstvo i obshchestvennoe blago: mirovye tendentsii i rossiiskii put'* [State and public good: Global trends and the Russian path]. Moscow, Institut SShA i Kanady RAN Publ. (In Russ.)

7. Ball H. 2004. *The USA PATRIOT Act of 2001: Balancing civil liberties and national security. A reference book*. Santa Barbara, ABC-CLIO.

8. Breglio N.K. 2003. Leaving FISA behind: The need to return to warrantless foreign intelligence surveillance. *Yale Law Journal*, vol. 113, no. 1, pp. 179–217.

9. Carter A.B., Perry W.J. 1999. *Preventive defense: A new security strategy for America*. Washington, D.C., Brookings Institution Press.

10. Clinton B., Gore Al. 1992. *Putting people first. How we can all change America*. New York, Times Books.

11. De Rosa M. 2003. Privacy in the age of terror. *Washington Quarterly*, vol. 26, no. 3, pp. 27–41.

12. Acquisti A. (ed.). 2008. *Digital privacy. Theory, technologies, and practices*. New York, Auerbach Publications.

13. Drucker P. 1996. *Landmarks of tomorrow*. London, Transaction Publishers.

14. Eaton J.W. 2003. *The privacy card: A low cost strategy to combat terrorism*. Lanham, Rowman & Littlefield.

15. Etzioni A. 2000. *The limits of privacy*. New York, Basic Books.

16. Gailbraith J.K. 1967. *The new industrial state*. New Jersey, Princeton University Press.

17. Hughbank R. 2010. Intelligence and its role in protecting against terrorism. *Journal of Strategic Security*, vol. 3, no. 1, pp. 31–38.

18. Keenan K.M. 2005. *Invasion of privacy. A reference handbook*. Santa Barbara, ABC-CLIO.

19. Klosek J. 2007. *The war on privacy*. Westport, Praeger Publishers.

20. Kerr I. (ed.). 2009. *Lessons from the identity trail: Anonymity, privacy, and identity in a networked society*. Oxford, Oxford University Press.

21. Rosenzweig P. 2004. Civil liberties and the response to terrorism. *Duquesne Law Review*, vol. 42, pp. 663–723.

22. Solove D.J. 2004. Reconstructing the electronic surveillance law. *The George Washington Law Review*, vol. 72, pp. 1701–1747.

23. Sottiaux S. 2008. *Terrorism and the limitation of rights: The ECHR and the US Constitution*. Oxford; Portland, Hart.

24. Stevens G.M. 2003. *Privacy: Total information awareness programs and latest developments*. New York, Novinka books.

25. Suarez S. 2017. Is America safer? The USA FREEDOM Act of 2015 and what the FBI and NSA have, can, and should be doing. *Law School Student Scholarship*. Paper 882. Available at: http://scholarship.shu.edu/student_scholarship/882 (accessed: 24.11.2016).

26. Toffler A. 1984. *The third wave*. New York, Bantam Books.

27. Wittes B. 2011. *Databuse: Digital privacy and the mosaic*. Brookings Institution. Available at: https://www.brookings.edu/wp-content/uploads/2016/06/0401_databuse_wittes.pdf (accessed: 20.11.2016).