Научная статья
УДК 342.72
doi:10.21685/2307-9525-2021-9-3-7

ДЕЛО «ЛАРРИ КЛЕЙМАН ПРОТИВ ОБАМЫ»: ЗАЩИТА ПРАВА НА НЕПРИКОСНОВЕННОСТЬ ЧАСТНОЙ ЖИЗНИ В УСЛОВИЯХ БОРЬБЫ С ТЕРРОРИЗМОМ

Георгий Борисович Романовский

Пензенский государственный университет, Пенза, Россия
up406@mail.ru

Аннотация. *Актуальность и цели.* Меры противодействия терроризму носят универсальный характер, что предопределяет актуальность исследований зарубежного законодательства и судебной практики в заявленной сфере. Рассматриваются особенности ограничений права на неприкосновенность частной жизни в условиях противодействия терроризму в Соединенных Штатах Америки. Основная цель – анализ порядка выдачи судебного ордера на осуществление электронного наблюдения, определяемого Законом 1978 г. о наблюдении за деятельностью иностранных разведывательных служб в США. Подробно изучены также изменения в указанный закон, установленные Актом Патриота в 2001 г. после атаки террористов-смертников на башни Всемирного торгового центра. *Материалы и методы.* Эмпирическую базу исследования составили судебные материалы по иску Ларри Клеймана против Обамы (судебное дело рассматривалось в федеральных судах США). В качестве основного был использован сравнительно-правовой метод исследования. *Результаты.* В ходе судебного разбирательства в различных федеральных инстанциях по жалобе Ларри Клеймана (адвоката и правозащитника) были выявлены значимые пробелы в деятельности американских спецслужб. Информационное значение данного дела обусловливалось перечнем ответчиков, в числе которых были высшие должностные лица американской администрации, включая Президента США Барака Обаму. *Выводы.* Выявленные в ходе судебного разбирательства недостатки легли в основу принятия Акта о свободе в 2015 г. Таким образом, первоначальное решение, запрещающее массовый сбор метаданных об американских пользователях, было отменено апелляционной инстанцией. Это позволило сохранить общие принципы массового сбора данных о гражданах в целях противодействия терроризму.

Ключевые слова: права человека, право на неприкосновенность частной жизни, США, противодействие, терроризм, программа слежения

Финансирование: исследование выполнено при финансовой поддержке РФФИ в рамках научного проекта № 20-011-00096.

Для цитирования: Романовский Г. Б. Дело «Ларри Клейман против Обамы»: защита права на неприкосновенность частной жизни в условиях борьбы с терроризмом // Электронный научный журнал «Наука. Общество. Государство». 2021. Т. 9, № 3. С. 68–77. doi:10.21685/2307-9525-2021-9-3-7

Original article

KLAYMAN v. OBAMA CASE: PROTECTING PRIVACY WHILE FIGHTING TERRORISM

Georgy B. Romanovsky

Penza State University, Penza, Russia
up406@mail.ru

Abstract. *Background.* Counterterrorism measures are universal in nature, which predetermines the relevance of studying foreign legislation and judicial practice in the stated area. The article examines the features of restrictions on the right to privacy in the context of countering terrorism in the United States of America. The main objective is to analyze the procedure for issuing a judicial order for electronic surveillance, as defined by the United States Foreign Intelligence Surveillance Act of 1978. The amendments to this law established by the Patriot Act in 2001 after the terrorist attacks on the towers of the World Trade Center are also detailed. *Materials and methods.* The empirical basis of the research is made up of court materials on the suit of Larry Klayman versus Obama (the case was considered in the federal courts in the US). The comparative legal research method is used as the main one. *Results.* In the course of legal proceedings at various level of jurisdiction on the complaint of Larry Klayman (an attorney and human rights activist), the significant gaps in the activity of the American intelligence services were identified. The informational value of this case stemmed from the list of defendants, including senior officials of the American administration, including US President Barack Obama. *Conclusions.* The gaps identified during the proceedings formed the basis for adopting the Freedom Act in 2015. Thus, the original decision prohibiting the massive collection of metadata on American users was overturned by the appellate court. This made it possible to preserve the general principles of mass collection of data on citizens in order to counter terrorism.

Keywords: human rights, privacy, US, countermeasures, terrorism, surveillance program

Acknowledgments: the research was carried out with the financial support of the Russian Foundation for Basic Research within the research project no. 20-011-00096.

For citation: Romanovsky G.B. Klayman v. Obama Case: Protecting Privacy while Fighting Terrorism. *Elektronnyy nauchnyy zhurnal "Nauka. Obshchestvo. Gosudarstvo" = Electronic scientific journal "Science. Society. State*". 2021;9(3):68–77. (In Russ.). doi:10.21685/2307-9525-2021-9-3-7

11 сентября 2001 г. стало поворотным событием в мировой истории. Уже на момент первого осмысления масштабного теракта – нападения на башни-близнецы Всемирного торгового центра в Нью-Йорке – была высказана значимая идея: мир никогда уже не будет жить так, как жил до 11 сентября. Для справедливости следует отметить, что такие поворотные моменты в нашу эпоху происходили неоднократно. Самым масштабным событием, по-видимому, следует назвать пандемию коронавирусной инфекции. Так, знаменитый политик Генри Киссинджер опубликовал знаковую статью в известном мировом издании – «Пандемия коронавируса навсегда изменит мировой порядок»[1].

Прямым следствием 11 сентября 2001 г. стало объявление войны против террора, вылившейся в целостную концепцию, призванную систематизировать обновленный перечень ограничений основных прав человека, определившую иное место безопасности в конституционной аксиологии. Юридическим оформлением концепции стало принятие Акта Патриота (причем весьма быстрое для многостраничного документа, что породило дополнительные конспирологические теории об участии самого государства в атаках против собственных граждан).

В течение последующих двадцати лет антитеррористическое законодательство еще больше расширило возможности спецслужб по осуществлению контроля за гражданами страны. Данная тенденция характерна не только для США, но и практически для всех развитых стран, так или иначе участвующих в противодействии мировой угрозе. Каждое государство понимало свою незащищенность без принятия дополнительных мер, даже если на каком-то этапе в этой сфере господствовала нейтральная политика, продиктованная нежеланием включаться в решение серьезных мировых проблем. Терроризм принял черты глобального движения, утратив свои национальные признаки и локальные особенности [1]. Точно так же можно указывать и на новое видение законодательства в сфере борьбы

[1] Kissinger H. A. The Coronavirus Pandemic Will Forever Alter the World Order // The Wall Street Journal. 2020. April 3. URL: https://www.wsj.com/articles/the-coronavirus-pandemic-will-forever-alter-the-world-order-11585953005 (дата обращения: 20.06.2021).

с данным видом преступлений. В 2001 г. страны Западной Европы, проявляя солидарность с США, поспешно принимали изменения в свое законодательство, усиливая полномочия правоохранительных органов, расширяя понятие терроризма, допуская различные исключения в принятых правилах вторжения в частную жизнь, упрощая нормы о мониторинге различных видов коммуникаций. В течение нескольких месяцев были приняты следующие законы:

– в Германии – Закон о борьбе с международным терроризмом – Gesetz zur Bekämpfung des internationalen Terrorismus (TerrorBekämpfG)[1];

– в Италии – Закон от 15 декабря 2001 г. № 438 «О неотложных мерах в целях борьбы с международным терроризмом»[2];

– в Великобритании – Акт о борьбе с терроризмом, преступности и безопасности[3].

Российская Федерация активно сотрудничает с американскими спецслужбами в вопросах предотвращения террористических атак, хотя и в этой сфере можно наблюдать некоторые отголоски политической конфронтации [2]. Иные страны воспроизводили многие положения представленного антитеррористического законодательства, как только им напрямую приходилось сталкиваться с реальностью новых угроз [3]. В числе основных положений новых законов можно найти пункт о расширении полномочий правоохранительных органов по упрощенному допуску к личным данным граждан [4]. При этом на организации, собирающие информацию в силу технических особенностей оказания каких-то услуг, возлагалась обязанность по их обязательному хранению в течение определенного времени (от полугода до трех лет). Такой подход впервые был апробирован в Соединенных Штатах Америки (как раз благодаря Акту Патриота [5]), но активно внедряется и в иных странах. Основная критика новелл выстраивается в последовательном изменении оснований ограничений права на неприкосновенность частной жизни.

Рассмотрим на примере Соединенных Штатов Америки. Право на неприкосновенность частной жизни базируется на IV Поправке к Конституции, хотя текстуально оно там отсутствует. Для понимания проблематики приведем текст поправки: «Не должно нарушаться право народа относительно неприкосновенности личности, бумаг и имущества при неосновательных обысках и арестах; приказы для обысков и арестов могут быть выдаваемы не иначе, как по основательным причинам, подкрепленным присягой или аффирмацией, с точным описанием места обыска и лиц, подлежащих аресту». Нетрудно увидеть, что IV Поправка касается иного права – на неприкосновенность личности. Если вдаваться в историю признания неприкосновенности частной жизни в США, то следует упомянуть работу американских юристов С. Уоррена и Л. Брандайса «Право на неприкосновенность частной жизни», изданную в 1890 г. [6]. Однако понимание новой категории выделялось из права на жизнь, его индивидуализации. Уже во второй половине XX в. право на неприкосновенность частной жизни было определено как следствие провозглашения права на личную неприкосновенность (было представлено расширительное толкование [7–9]). При рассмотрении процедур, ограничивающих право на частную жизнь лица при проведении оперативно-разыскных мероприятий, Верховный Суд США уже отталкивался от текста IV Поправки, требуя при выдаче ордера четких обоснований места проведения, обстоятельств и предполагаемых полученных результатов. Акт Патриота исходил из того, что предотвращение терактов возможно при проведении расширенного мониторинга электронных сетей, когда сложно выделить как место контроля, так и обстоятельства, обусловливающие обоснованность деятельности спецслужб. В практике США

[1] TerrorBekämpfG. URL: http://www.bmi.bund.de/SharedDocs/Gesetzestexte/DE/Terrorismusbekaempfungsgesetz.-pdf?__blob=publicationFile (дата обращения: 20.06.2021).

[2] Legge 15 dicembre 2001, № 438 «Conversione in legge, con modificazioni, del decretolegge 18 ottobre 2001, n. 374, recante disposizioni urgenti per contrastare il terrorismo internazionale». URL: http://www.camera.it/parlam/leggi/01438l.htm#decreto (дата обращения: 20.06.2021).

[3] Anti-terrorism, Crime and Security Act, 2001. URL: http://www.legislation.gov.uk/ukpga/2001/24 (дата обращения: 20.06.2021).

стал пропагандироваться «метод невода», когда массовый сбор различных данных осуществляется вне каких-то конкретных подозрений. В последующем собранная информация систематизируется и обрабатывается. Технологическим элементом стала специальная программа *Carnivore*, которая осуществляет массовое архивирование всех электронных сообщений вне зависимости от того, кто является автором – добропорядочный гражданин США или преступник. В настоящее время данная программа является далеко не единственной используемой американскими спецслужбами.

Внедрение такого программного обеспечения строится на необходимости разведывательной деятельности в отношении международной угрозы, которую представляют террористические организации [10]. Такая модель всеобщего контроля не урегулирована порядком, тождественным выдаче судебного ордера на прослушивание телефонных переговоров, поскольку в нем сложно указать основания и субъекта слежки [11].

Общественная огласка использования таких «хищнических» программ произошла в 2013 г. в результате разглашения секретных сведений сотрудником Агентства национальной безопасности Э. Сноуденом. В его интервью было выдвинуто обвинение в осуществлении глобальной слежки как за гражданами США, так и за любыми иностранцами, где бы они ни находились. Практически сразу после скандальной истории адвокат Ларри Клейман (основатель правозащитной организации «Freedom Watch») обратился в суд с иском против целого ряда высших должностных лиц государства. В качестве ответчиков фигурировали лично Президент США Б. Х. Обама, Директор Агенства национальной безопасноти (АНБ) К. Б. Александер, Генеральный прокурор США Э. Х. Холдер-младший, а также компании, оказывающие интернет-услуги (Facebook, Yahoo!, Google, Microsoft, Apple, YouTube, крупный американский провайдер Verizon Communications и др.). Л. Клейман выступал как истец и как адвокат других истцов, которые подали совместный иск. Сам Ларри Клейман является ярым противником всех представителей Демократической партии США. Когда Х. Клинтон баллотировалась в Президенты США, на сайте организации размещались различные оскорбительные материалы в ее адрес. Сейчас на этом сайте представлен показательный процесс над Президентом США Д. Байденом[1]. Им издаются книги (можно заказать на сайте с автографом автора), в которых показана утрата величия Соединенных Штатов Америки и сделан призыв к смене власти. Несмотря на всю эпатажность его поведения, сторонников у Л. Клеймана весьма немного. По-видимому, подобный иск был отчасти попыткой привлечь внимание (что можно признать удачным ходом), но имел кратковременный эффект.

Иск подавался также как групповой в защиту прав неопределенного круга лиц – всех пользователей Интернета. В обосновании запрета на проведение системных ограничений, связанных с мониторингом интернет-пространства и хранением метаданных, авторы ссылались на нарушение I, IV и V Поправок к Конституции США. IV Поправка упоминалась ранее. I Поправка посвящена свободе слова, религии, ассоциаций, а V – праву на надлежащее судебное разбирательство. Свобода слова нарушается, по мнению заявителей, тем, что каждый гражданин, зная о контроле за электронным общением, будет скрывать свое истинное мнение, в том числе по политическим вопросам жизни американского общества. Основной акцент был сделан на нарушении конфиденциальности, вторжении в уединение.

Причиной иска стала информация о существовании правительственной программы PRISM (кодовое название), позволяющей осуществлять контроль за всеми электронными сообщениями. Особенность ее использования заключается в том, что большинство интернет-коммуникаций проходит через серверы технологических гигантов, расположенных в США. Исходя из этого внедрение специального продукта в системы ключевых провайдеров позволяет контролировать все электронное общение. Опубликование засекреченных докладов Э. Сноуденом [12]

[1] Freedom Watch. URL: https://www.freedomwatchusa.org/ (дата обращения: 20.06.2021).

указывало, что в тесном сотрудничестве находились все гиганты, которые впоследствии фигурировали в иске Л. Клеймана. После этого Google сделал официальное заявление, что сотрудничество с государственными правоохранительными органами США осуществляется только в рамках закона и только на основании официальных запросов. Представитель Apple заявил, что «никогда не слышал» о PRISM[1]. Джо Салливан, начальник службы безопасности Facebook, также отверг столь тесное сотрудничество по вопросу бесконтрольной передачи персональных данных: «Мы не предоставляем правительственным организациям прямой доступ к серверам Facebook. Когда у Facebook запрашивают данные или информацию о конкретных лицах, мы внимательно изучаем любой такой запрос на соответствие всем применимым законам и предоставляем информацию только в той мере, в какой это требуется по закону»[2]. В заявлении другого технологического гиганта указывалось: «Yahoo! очень серьезно относится к конфиденциальности пользователей. Мы не предоставляем правительству прямой доступ к нашим серверам, системам или сети»[3]. Подобные пресс-релизы показательны, поскольку большинство компаний продвигало свой продукт на рынке под слоганом тотальной защиты личной конфиденциальности.

PRISM позволяет АНБ вне обязательного ордера осуществлять разведывательный мониторинг электронного поля общения. Содействие провайдеров не требовалось, поскольку контроль мог проводиться без какого-то уведомления. Была раскрыта также информация о существовании дополнительной программы – BLARNEY, которая нацелена на сбор метаданных – технической информации о коммуникационном трафике и сетевых устройствах по мере ее прохождения по магистрали Интернета.

Правовая основа указанных программ виделась в толковании следующих законов:

– Закон 1978 г. о наблюдении за деятельностью иностранных разведывательных служб в США (Foreign Intelligence Surveillance Act, используется также сокращенное название – FISA[4]);

– Закон 1994 г. о помощи провайдеров коммуникационных услуг правоохранительным органам (The Communications Assistance for Law Enforcement Act, сокращенное название – CALEA[5]).

Каждый из этих законов вводил специальные правила проведения оперативно-разыскных мероприятий в отношении иностранных граждан и зарубежных организаций. Черта по отношению к собственным гражданам – особенность американской системы. Выдача ордера также осуществляется специальным судом – так называемым судом FISA [13]. Ключевое обвинение, адресованное официальным властям США, строилось на том, что программы позволяли на основании общих ордеров (в действительности выдаваемых судом FISA) осуществлять общий контроль, под который попадали и коммуникации граждан США. Общий ордер заключался не в разрешении контроля за конкретным пользователем или владельцем IP-адреса, а в мониторинге по системным моментам – например, по сообщениям, инициируемым с определенной территории [14]. В данном случае включалась модель «паутины», когда контролю подвергались все адреса, так или иначе связанные с ними, даже находящиеся в косвенной и не

[1] Greenwald G., MacAskill E. NSA Prism program taps in to user data of Apple, Google and others // The Guardian. 2013. 7 Jun. URL: https://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data (дата обращения: 20.06.2021).

[2] Gellman B., Poitras L. U.S., British intelligence mining data from nine U.S. Internet companies in broad secret program // The Washington Post. 2013. 7 June. URL: 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 (дата обращения: 20.06.2021).

[3] Там же.

[4] Foreign Intelligence Surveillance Act of 1978. URL: http://legcounsel.house.gov/Comps/Foreign%20Intelligence%20Surveillance%20Act%20Of%201978.pdf (дата обращения: 20.06.2021).

[5] The Communications Assistance for Law Enforcement Act. URL: https://legcounsel.house.gov/Comps/Communications%20Assistance%20For%20Law%20Enforcement%20Act.pdf (дата обращения: 20.06.2021).

прямой последовательности [15, 16]. Кстати, такой вариант слежения был практически подтвержден официальными представителями АНБ, но с уточнением, что любая информация, не имевшая отношения к расследованию, уничтожалась и не систематизировалась. Представитель администрации Президента США Б. Обамы указывал, что гарантии конституционных прав американских граждан нерушимы, подтверждаются судебными процедурами и обеспечиваются так, чтобы «преследованию подвергались только лица, не являющиеся гражданами США, находящиеся за пределами США; гарантии сводят к минимуму получение, сохранение и распространение случайно полученной информации о гражданах США»[1].

Сам факт существования указанных программ был засекречен. Именно поэтому Э. Сноудену предъявлено официальное обвинение в совершении уголовного преступления. Его наличие исключает его возвращение в Соединенные Штаты Америки. Парламентарии были проинформированы о наличии PRISM, специальный комитет Сената одобрил ее применение. Всем технологическим гигантам (в отношении каждого из них выдавался общий судебный ордер судом FISA) в обмен на сотрудничество с АНБ был предоставлен иммунитет от возможных исков за нарушение конфиденциальности общения. Факт сотрудничества подпадал под режим государственной тайны. Юридическим лицам ФБР направляло «письма национальной безопасности» (national security letter – сокращенно NSL), разглашение которых является уголовным преступлением.

Интересный момент. Дж. Сенсебреннер – конгрессмен, автор Акта Патриота – после опубликования данных и пресс-релиза Б. Обамы подверг оправдания жесткой критике, указывая, что Акт Патриота не был принят для осуществления тотальной неконтролируемой слежки: «На своей пресс-конференции в пятницу президент Обама охарактеризовал массовый сбор телефонных и цифровых записей как "две программы, которые изначально были санкционированы Конгрессом, были неоднократно одобрены Конгрессом". Но Конгресс никогда специально не санкционировал эти программы, и Акт Патриота никогда не был предназначен для того, чтобы позволить администрации Обамы ежедневно шпионить за гражданами»[2]. Однако двумя годами позже, когда речь шла о замене Акта Патриота постоянным документом, не нуждающимся в периодическом продлении, Дж. Сенсебреннер выступил автором Акта о свободе. В новом законе были сохранены все ключевые положения, позволяющие спецслужбам осуществлять широкий контроль за всеми электронными сообщениями (вне зависимости от формы их представления) [17]. В 2013 г. многие конгрессмены публично заявляли о возможном судебном оспаривании допустимости программ PRISM и BLARNEY, но в действительности только Л. Клейман оказался истцом. Сенатор-республиканец Рэнд Пол обратился в суд, но движение дела было приостановлено до вынесения итогового решения по иску Л. Клеймана. В последующем (в 2019 г.) разбирательство было прекращено, поскольку истец прекратил свои активные действия в судебной инстанции (политическая ситуация изменилась – Президентом США был республиканец Д. Трамп).

В своем иске Л. Клейман указывал, что использование программ не прекращается. Это позволяет американским спецслужбам без какого-то судебного контроля осуществлять сбор обширных данных, а именно все записи о звонках (о маршрутизации сообщений, исходный и конечный телефонный номер, идентификационный номер оборудования (IMEI), номера телефонных карт и др.), об электронном общении (чат, видео- и аудиосообщения, фото, уведомления об интернет-активности, запросы в поисковых системах в режиме реального времени и т.д.). Сам иск не содержит четкого обоснования незаконности выявленного

[1] Gellman B., Poitras L. Gellman B., Poitras L. U.S., British intelligence mining data from nine U.S. Internet companies in broad secret program // The Washington Post. 2013. 7 June. URL: 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 (дата обращения: 20.06.2021).

[2] Sensenbrenner J. This abuse of the Patriot Act must end // The Guardian. 2013. 9 Jun. URL: https://www.theguardian.com/commentisfree/2013/jun/09/abuse-patriot-act-must-end (дата обращения: 20.06.2021).

мониторинга, в нем больше политических обвинений, подтверждаемых ссылками на высказывания политиков, обвиняющих администрацию Б. Обамы в неконституционных действиях. Основной довод: «По настоящее время Ответчики не представили американскому народу существенных и значимых объяснений, описывающих произошедшее. Напротив, как сообщается, обвиняемые Обама, Холдер, Министерство юстиции и Агентство национальной безопасности возбудили уголовные дела против того, кто сообщил об этом заговоре против американских граждан, прилагая дальнейшие усилия по пресечению, воспрепятствованию правосудию и сохранению незаконных действий подсудимых в секрете»[1].

Истцы настаивали, что введение таких программ ограничивало их возможности участвовать во внешнем общении из-за опасения быть прослушанными, что нарушает I Поправку к Конституции США. Свобода ассоциации нарушалась тем, что истцы ограничили свои контакты, минимизируя любое общение, имея «страх перед возможным злоупотреблением государственной властью»[2]. Ларри Клейман утверждал, что единственной целью такой политики является запугивание американских граждан, отказ от сопротивления «тиранической администрации».

13 июня 2013 г. директор Национальной разведки опубликовал «Факты о сборе разведывательной информации в соответствии с разделом 702 Закона о наблюдении за деятельностью иностранных разведывательных служб», в которых было представлено официальное мнение о ситуации: «PRISM не является скрытой программой сбора или интеллектуального анализа данных. Это внутренняя правительственная компьютерная система, используемая для облегчения законодательно санкционированного правительством сбора информации о деятельности иностранных разведывательных служб, получаемой от поставщиков услуг электронной связи под надзором суда, как это разрешено разделом 702 Закона о наблюдении за деятельностью иностранных разведывательных служб (FISA) (50 U.S.C. § 1881a). Этот продукт был разрешен Конгрессом, широко известен и открыто обсуждается с момента его создания в 2008 году»[3]. В документе подчеркивается, что информация не получается в одностороннем порядке с серверов американских поставщиков услуг электронной связи. Все данные получены с одобрения суда FISA и с ведома провайдера на основании письменного распоряжения генерального прокурора и директора национальной разведки. Раздел 702 способствует целевому получению информации о деятельности иностранных разведывательных служб и об иностранных объектах, расположенных за пределами Соединенных Штатов. Все это происходит под надзором суда. Были отклонены все обвинения, что представленные программы позволяют вести слежку за гражданами США.

Иск Л. Клеймана был рассмотрен судьей Окружного суда по округу Колумбия Р. Дж. Леоном. Решение было вынесено быстро – 16 декабря 2013 г.[4] Оно цитируется многими правозащитниками, поскольку в нем были удовлетворены основные требования истцов. В многостраничном документе использование программ слежения было объявлено неконституционным. В ходе судебного рассмотрения представители АНБ уклонились от оценки эффективности внедрения программ слежения, представив лишь в общих чертах отчет о предотвращенных террористических атаках. Истцы же требовали детальных характеристик, хотя такие претензии, вероятно, не будут иметь успеха в любой стране мира. Отказ от предоставления подробной информации позволил судье усомниться в конституционности столь широких полномочий. В решении суда есть и поэтическое

[1] Klayman v. Obama et al. URL: https://docs.justia.com/cases/federal/district-courts/district-of-columbia/dcdce/1:2013cv00851/160387/13/2.html (дата обращения: 20.06.2021).

[2] Ibid.

[3] Facts on the Collection of Intelligence Pursuant to Section 702 of the Foreign Intelligence Surveillance Act. URL: http://www.dni.gov/files/documents/Facts on the Collection of Intelligence Pursuant to Section 702.pdf (дата обращения: 20.06.2021).

[4] Federal Judge's Ruling on N.S.A. Lawsuit. URL: https://assets.documentcloud.org/documents/901810/klaymanvobama215.pdf (дата обращения: 20.06.2021).

отступление – сравнение с «оруэлловскими технологиями». При упоминании судебного решения именно эта аллегория приводится для характеристики тотальной слежки. Судья Р. Леон выделил: «Из-за полного отсутствия доказательств того, что террористический акт когда-либо предотвращался, только из-за того, что подобный поиск в базе данных АНБ ускорял процесс, чем другие методы расследования, – у меня есть серьезные сомнения в эффективности программы сбора метаданных… У меня нет сомнений в том, что автор нашей Конституции Джеймс Мэдисон был бы в ужасе, узнав о подобном»[1].

Истцы настаивали на введении немедленного запрета на использование программ слежения, но судья не поддержал их требования. Апелляционное решение было вынесено в августе 2015 г., оно отменяло постановление судьи Р. Леона. Этому же судье дело было направлено на новое рассмотрение. Отмена основывалась на том, что истцы не были пользователями одного из провайдеров, указанных в качестве ответчиков (компания «Verizon Business Services»). Так в деле появился еще один истец – калифорнийский адвокат Дж. Дж. Литтл. Именно в отношении данного истца было вынесено постановление о прекращении сбора данных. К этому времени Акт Патриота прекратил свое существование – 2 июня 2015 г. Президентом Бараком Обамой был подписан Акт о свободе[2]. Это послужило основанием для подачи апелляционной жалобы, которая была удовлетворена судом второй инстанции. Новое рассмотрение и в этот раз должен был осуществлять тот же судья. 21 ноября 2017 г. судья Р. Леон (автор оруэлловской формулы о тотальной слежке) отклонил все заявленные иски к правительственным органам США[3].

В окончательном решении отсутствуют рассуждения о недемократической системе обеспечения безопасности, сухо излагается конституционность оспариваемых законов. Такой поворот не отражен в публицистических источниках. Большинство журналистских материалов заканчивается цитатой об «оруэлловских технологиях» и признанием Э. Сноуденом прогрессивности судебного решения. Поспешные выводы не следует принимать без детального анализа ситуации. Анализ же тех решений, которые вступили в законную силу, показывает, что американские суды не подвергали сомнению легитимность использования специальных программ сбора информации в телекоммуникационных системах, которые применяются американскими спецслужбами [18–20]. PRISM – не единственная программа, аналогичные функции выполняются, например, Carnivore, Fairview, Tempora, X-Keyscore и др.

Несмотря на слабые перспективы судебного разбирательства (которые были озвучены экспертами), гражданская активность привела к уточнению многих полномочий американских спецслужб по осуществлению контроля за частной жизнью американских граждан. В то же время Акт о свободе не отказался от упрощенной модели слежения за иностранными гражданами, введя лишь некоторые дополнения, касающиеся ограждения американцев от возможных злоупотреблений.

Список литературы

1. Федоров А. В., Сергеев Д. Н. Глобальный терроризм: национальные и международные возможности противодействия // Российский следователь. 2017. № 14. С. 49–53.

2. Кабасакалова М. Г. Российско-американское сотрудничество в сфере борьбы с международным терроризмом // Международное публичное и частное право. 2014. № 3. С. 21–24.

[1] Federal Judge's Ruling on N.S.A. Lawsuit. URL: https://assets.documentcloud.org/documents/901810/klaymanvobama215.pdf (дата обращения: 20.06.2021).

[2] Act on the «To reform the authorities of the Federal Government to require the production of certain business records, conduct electronic surveillance, use pen registers and trap and trace devices, and use other forms of information gathering for foreign intelligence, counterterrorism, and criminal purposes, and for other purposes». URL: https://www.congress.gov/114/bills/hr2048/BILLS-114hr2048enr.pdf (дата обращения: 20.06.2021).

[3] Memorandum Opinion. URL: https://assets.documentcloud.org/documents/4267780/42df8218-70d7-4c17-9b6e-2704fdb37315.pdf (дата обращения: 20.06.2021).

3. Брылева Е. А. Неприкосновенность частной жизни: частные и публичные интересы // Информационное право. 2018. № 4. С. 4–7.

4. Борисов С. В., Вилинский Г. О. Критерии доверия сотруднику органов внутренних дел и военной полиции в аспекте противодействия экстремистской деятельности и ее финансированию // Право в Вооруженных Силах. 2018. № 7. С. 109–113.

5. Кикоть-Глуходедова Т. В. Основы правовой регламентации деятельности вооруженных сил США по разрешению внутрикризисных ситуаций // Административное право и процесс. 2014. № 7. С. 69–71.

6. Warren S. D., Brandeis L. D. The Right to Privacy // Harvard Law Review. 1890. Vol. IV, № 5. P. 193–220. URL: https://louisville.edu/law/library/special-collections/the-louis-d.-brandeis-collection/the-right-to-privacy

7. Преснякова А. В. Право на неприкосновенность частной жизни в системе конституционных прав и свобод человека и гражданина // Конституционное и муниципальное право. 2010. № 8. С. 18–19.

8. Новиков В. Понятие частной жизни и уголовно-правовая охрана ее неприкосновенности // Уголовное право. 2011. № 1. С. 43–49.

9. Кархалев Д. Н. Способы защиты гражданских прав в США // Нотариус. 2016. № 4. С. 37–39.

10. Чернядьева Н. А. Американская региональная (ОАГ) и национальная (США) модели борьбы с международным терроризмом // Международное уголовное право и международная юстиция. 2016. № 1. С. 26–29.

11. Anyanwu Ch. Fear of communicating fear versus fear of terrorism: A human rights violation or a sign of our time? // International Journal of Speech-Language Pathology. 2018. Vol. 20, № 1. P. 26–33. URL: https://www.tandfonline.com/doi/citedby/10.1080/17549507.2018.1419281?scroll=top&needAccess=true

12. Бородин К. В. Правовое регулирование распространения информации в сети Интернет в условиях информационной войны // Право и кибербезопасность. 2014. № 1. С. 27–31.

13. Романовская О. В. Акт о свободе: ограничения прав человека в США в целях противодействия терроризму // Электронный научный журнал «Наука. Общество. Государство». 2017. Т. 5, № 3 (19). С. 65–71.

14. Бельский А. И., Якимова В. И. Кибертерроризм как один из наиболее опасных видов международного терроризма // Российский следователь. 2020. № 5. С. 66–70.

15. Тарасов А. М. Киберугрозы, прогнозы, предложения // Информационное право. 2014. № 3. С. 11–15.

16. Войниканис Е., Савельев А., Головко Л. [и др.]. Privacy vs security: баланс интересов в информационном обществе // Закон. 2016. № 4. С. 19–25.

17. Романовский В. Г. Профилирование террористов и конституционная защита прав человека // Конституционное и муниципальное право. 2020. № 10. С. 46–50.

18. Жилкин В. А. Международная безопасность и роль России в борьбе с международным терроризмом и информационной безопасностью // Международное публичное и частное право. 2017. № 4. С. 24–27.

19. Шестак В. А., Шайнуров В. А. Доктрина конституционализма в уголовном судопроизводстве: опыт России и США // Мировой судья. 2021. № 1. С. 9–14.

20. Романова А. Ю. Правовое регулирование общедоступных данных в законодательстве зарубежных стран // Конституционное и муниципальное право. 2020. № 9. С. 65–70.

References

1. Fedorov A.V., Sergeev D.N. Global Terrorism: National and International Countermeasures. *Rossiyskiy sledovatel = Russian Investigator*. 2017;(14):49–53. (In Russ.)

2. Kabasakalova M.G. Russian-American Cooperation in Fight against International Terrorism. *Mezhdunarodnoe publichnoe i chastnoe pravo = International Public and Private Law*. 2014;(3):21–24. (In Russ.)

3. Bryleva E.A. Privacy: Private and Public Interests. *Informatsionnoe pravo = Information Law*. 2018;(4):4–7. (In Russ.)

4. Borisov S.V., Vilinskiy G.O. Criteria of Trust in a Law Enforcement and Military Police Officer in Terms of Countering Extremism and Its Financing. *Pravo v Vooruzhennykh Silakh = Law in the Armed Forces*. 2018;(7):109–113. (In Russ.)

5. Kikot-Glukhodedova T.V. Fundamentals of Regulating Activity of the US Armed Forces to Resolve Intra-Crisis Situations. *Administrativnoe pravo i protsess = Administrative Law and Administrative Process*. 2014;(7):69–71. (In Russ.)

6. Warren S.D., Brandeis L.D. The Right to Privacy. *Harvard Law Review*. 1890;IV(5):193–220. Available at: https://louisville.edu/law/library/special-collections/the-louis-d.-brandeis-collection/the-right-to-privacy

7. Presnyakova A.V. Right to Privacy in the System of Constitutional Rights and Freedoms of a Person and a Citizen. *Konstitutsionnoe i munitsipalnoe pravo = Constitutional and Municipal Law*. 2010;(8):18–19. (In Russ.)

8. Novikov V. Concept of Private Life and Criminal Law Protection of Its Inviolability. *Ugolovnoe pravo = Criminal Law*. 2011;(1):43–49. (In Russ.)

9. Karkhalev D.N. Ways to Protect Civil Rights in the United States of America. *Notarius = Notary*. 2016;(4):37–39. (In Russ.)

10. Chernyadieva N.A. American Regional (OAS) and National (USA) Models of Combating International Terrorism. *Mezhdunarodnoe ugolovnoe pravo i mezh-dunarodnaya yustitsiya = International Criminal Law and International Justice*. 2016;(1):26–29. (In Russ.)

11. Anyanwu Ch. Fear of communicating fear versus fear of terrorism: A human rights violation or a sign of our time? *International Journal of Speech-Language Pathology*. 2018;20(1):26–33. Available at: https://www.tandfonline.com/doi/citedby/10.1080/1754-9507.2018.1419281?scroll=top&needAccess=true

12. Borodin K.V. Legal Regulation of Information Dissemination on the Internet in the Context of Information War. *Pravo i kiberbezopasnost = Law and Cybersecurity*. 2014;(1):27–31. (In Russ.)

13. Romanovskaya O.V. Freedom Act: US Human Rights Limitations to Counter Terrorism. *Elektronnyy nauchnyy zhurnal «Nauka. Obshchestvo. Gosudarstvo» = Electronic Scientific Journal "Science. Society. State"*. 2017;5(3):65–71. (In Russ.)

14. Belskiy A.I., Yakimova V.I. Cyberterrorism as One of the Most Dangerous Types of International Terrorism. *Rossiyskiy sledovatel = Russian Investigator*. 2020;(5):66–70. (In Russ.)

15. Tarasov A.M. Cyberthreats, Forecasts, Proposals. *Informatsionnoe pravo = Information Law*. 2014;(3):11–15. (In Russ.)

16. Voynikanis E., Saveliev A., Golovko L. [et al.]. Privacy vs Security: Balance of Interests in the Information Society. *Zakon = Law*. 2016;(4):19–25. (In Russ.)

17. Romanovskiy V.G. Profiling of Terrorists and Constitutional Protection of Human Rights. *Konstitutsionnoe i munitsipalnoe pravo = Constitutional and Municipal Law*. 2020;(10): 46–50. (In Russ.)

18. Zhilkin V.A. International Security and Role of Russia in Fight against International Terrorism and Information Security. *Mezhdunarodnoe publichnoe i chastnoe pravo = International Public and Private Law*. 2017;(4):24–27. (In Russ.)

19. Shestak V.A., Shaynurov V.A. Doctrine of Constitutionalism in Criminal Proceedings: Practices in the Russian Federation and the United States of America. *Mirovoy sudiya = Justice of the Peace*. 2021;(1):9–14. (In Russ.)

20. Romanova A.Yu. Legal Regulation of Publicly Available Data in the Legislation of Foreign States. *Konstitutsionnoe i munitsipalnoe pravo = Constitutional and Municipal Law*. 2020;(9):65–70. (In Russ.)

Информация об авторе / Information about the author

Г. Б. Романовский – доктор юридических наук, профессор, заведующий кафедрой уголовного права, Пензенский государственный университет, 440026, г. Пенза, ул. Красная, 40.

G.B. Romanovsky – Doctor of Law, Professor, Head of the sub-department of Criminal Law, Penza State University, 40 Krasnaya street, Penza, 440026.

Автор заявляет об отсутствии конфликта интересов / The author declares no conflict of interests

Поступила в редакцию / Received 21.06.2021

Поступила после рецензирования и доработки / Revised 29.07.2021

Принята к публикации / Accepted 25.08.2021