ПОЛИЦИЯ И ЗАЩИТА ПРАВ ЧЕЛОВЕКА

Патрикеев П.А., Остроушко А.В.

О НЕОБХОДИМОСТИ ОГРАНИЧЕНИЯ ДЕЙСТВИЙ СПЕЦСЛУЖБ ПО СБОРУ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ О ГРАЖДАНАХ НОРМАМИ МЕЖДУНАРОДНОГО ПРАВА

Аннотация: *Проблема защиты любой личностной информации приобретает в свете недавних событий, связанных с раскрытием фактов массовой слежки государственных спецслужб за пользователями сети Интернет. В настоящей работе на примере деятельности американских спецслужб по работе с конфиденциальной информацией, как об американских гражданах, так и гражданах других стран, будет сделана попытка выявить угрозы информационной безопасности личности, основные проблемы в области соблюдения прав человека на неприкосновенность частной жизни в ходе деятельности компетентных органов государства и возможные пути их решения. Для подготовки статьи авторами были использованы следующие методологические основы: совокупность общенаучных и специальных методов познания социально-правовой действительности. Из числа общенаучных методов исследования использовались методы анализа, синтеза, сравнения, измерения. В качестве частнонаучного метода применялся сравнительно-правовой метод. Для повышения информационной безопасности личности нужно выработать комплекс правовых мер, позволяющих эффективно защитить данные и метаданные о личности. Основным выводом данного исследования является то, что особенности современной трансграничной передачи данных и организации сетей телекоммуникации, делают национальное законодательство неэффективным в процессе защиты информации о своих гражданах.В сложившейся ситуации эти проблем требуют урегулирования международным правом в самое ближайшее время.*

Ключевые слова: *Частная жизнь, конфиденциальная информация, сеть Интернет, спецслужбы, метаданные, сбор информации, ограничения, международное право, национальная безопасность, Эдвард Сноуден.*

Review: *The problem of personal data protection has become particularly urgent in the light of the recent disclosure of facts of mass spying on the Internet users by special services. The authors of the article study the work of*

DOI: 10.7256/2222-1964.2015.4.16213

the NSA with confidential information of the Americans and the citizens of other countries in order to reveal personal information security threats, the main problems of the right to privacy observance in the activities of government services and the ways to solve them. The authors apply the set of general scientific and special methods of socio-legal reality cognition. Among the general scientific methods the authors use the methods of analysis, synthesis, comparison and measurement. The comparative-legal approach is used as a special scientific method. The purpose of personal information security improvement requires a range of measures aimed at the effective protection of personal data and metadata. The authors conclude that the peculiarities of the modern transboundary data transmission and telecommunication networks organization reduce the efficiency of national legislation in the sphere of citizens' personal data protection. In this situation these issues should be urgently regulated by the international law.

Keywords: *International law, restrictions, collection of information, metadata, special services, Internet, confidential information, privacy, national security, Edward Snowden.*

Бурное развитие средств и способов межличностного общения, появление новых информационных технологий, формирование единой базы персональных данных со всей неумолимостью ставит перед современным обществом проблему создания действенного механизма, обеспечивающего неприкосновенность сферы частной жизни каждого человека, а, в частности, конфиденциальности его корреспонденции и личных данных[1]. Особенно резкое звучание данная проблема приобретает в свете недавних событий, связанных с раскрытием Эдвардом Сноуденом фактов массовой слежки государственных спецслужб за пользователями сети Интернет[2].

Неприкосновенность частной жизни – одно из основополагающих прав человека во все времена. Данное право находит свое закрепление в широчайшем пласте международных источников как-то: Всеобщая декларация прав человека от 10 декабря 1948 г., Европейская Конвенция о защите прав человека и основных свобод, Международный пакт о гражданских и политических правах и многие другие; Право на тайну сообщений включают в состав права на неприкосновенность личной жизни как более крупного института, но связь в данном случае несет обратный характер: без реализации одного из них полноценное функционирование другого невозможно. Европейский Суд по правам человека своими решениями по применению Европейской Конвенции о защите прав человека и основных свобод признал, что скрытое наблюдение за почтой и связью, является, ввиду исключительных условий, необходимым в демократическом обществе, но при этом должны существовать необходимые и эффективные гаран-

DOI: 10.7256/2222-1964.2015.4.16213

тии против злоупотреблений. Вмешательство не противоречит требованиям Конвенции, если:

a) Это предусмотрено законом и необходимо в демократическом обществе в интересах государственной безопасности, общественного порядка или экономического благосостояния страны, для поддержания порядка и предотвращения преступлений, в целях охраны здоровья и защиты нравственности, а также защиты прав и свобод других лиц;

b) Осуществляется в соответствии с законом, а этот закон и принятые на его основе подзаконные акты известны общественности и легко доступны;

c) В этих нормативных актах фиксируются пределы компетенции государственных органов, уполномоченных принимать решения о подслушивании и осуществлять его, и ограничения на способы реализации этих правомочий;

d) Оно осуществляется в целях предотвращения и пресечения не каких-то мелких, а вполне определенных и наиболее опасных преступлений;

e) Круг лиц, против которых предпринимаются означенные действия, строго ограничен;

f) Подслушивание носит выборочный, а не общепоисковой характер;

g) В случае прекращения преследования или оправдания по требованию соответствующего лица записи либо возвращаются ему, либо уничтожаются.

В России п. 3 ст. 56 Конституции РФ не включает право на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений в список статей, содержащих права и свободы не подлежащие ограничению. Между тем, ограничение данного права, как указано в п. 2 ст. 23, допускается только на основании судебного решения. Режим тайны связи (переписки и иных сообщений) установлен ст. 63 Федерального закона от 07.07.2003 N 126-ФЗ «О связи», согласно которому сообщения граждан, передаваемые по сетям электросвязи, составляют личную тайну, защищаемую Конституцией Российской Федерации. Ограничение права на тайну сообщений, передаваемых по сетям электросвязи, допускается только в случаях, предусмотренных федеральными законами. Ознакомление с информацией и документальной корреспонденцией, передаваемыми по сетям электросвязи и сетям почтовой связи, осуществляются только на основании решения суда, за исключением случаев, установленных федеральными законами. Государство, в лице органов, проводящих оперативно-розыскную деятельность, может осуществлять контроль почтовых отправлений, телеграфных и иных сообщений, прослушивание телефонных переговоров, снятие информации с технических каналов связи только на основании решения суда. Проведение оперативно-розыскных мероприятий, ограничивающих указанные конституционные права граждан, может иметь место лишь при наличии у органов, осуществляющих оперативно-розыскную деятельность, информации о признаках подготавливаемого, совер-

DOI: 10.7256/2222-1964.2015.4.16213

шаемого или совершенного противоправного деяния, по которому производство предварительного следствия обязательно; о лицах, подготавливающих, совершающих или совершивших противоправное деяние, по которому производство предварительного следствия обязательно; о событиях или действиях, создающих угрозу государственной, военной, экономической или экологической безопасности Российской Федерации.

В США массовой сбор и анализ информации о гражданах, так и информации, передаваемой гражданами в почтовых и телеграфных сообщениях, в целях обеспечения национальной безопасности, начался задолго до публикаций материалов ранее упомянутого Эдварда Сноудена. Эта деятельность ведется с начала XX в. (создание MI-8 или Бюро шифров). Расцвет анализа конфиденциальных сообщений приходится на период Второй мировой войны, по окончанию которой был создан Project SHAMROCK – проект, позволявший АБВС (Агентство Безопасности Вооруженных Сил – предтеча АНБ), а позже АНБ (Агентство Национальной Безопасности, созданное 4 ноября 1952 г.) собирать информацию о телеграфных сообщениях. Последующая Холодная война способствовала активизации деятельности спецслужб по сбору личной информации и организации «точечных» слежек, а события 11 сентября привели к новому всплеску активности, приведшее к созданию программы Stellar Wind – программы, с помощью которой велось наблюдение за электронными коммуникациями включая контроль сообщений электронной почты, телефонных разговоров, финансовых операций и интернет-активности.

Несмотря на то, что деятельность по ведению разведывательной деятельности осуществляют множество служб, входящих, согласно правительственному распоряжению № 12333 от 4 декабря 1998 г. в РС США (Разведывательное сообщество США), именно АНБ является органом, отвечающего за все виды электронной разведки с крайне широкими полномочиями.

Сбор данных осуществляется через каналы оптоволоконной связи, находящихся на территории США, а также из ресурсов дружественных государств и находящихся на их территории организаций и серверов ряда крупных компаний. Вся информация хранится в засекреченных базах данных, как-то: MAINWAY (хранит информацию о телефонных разговорах), TRACFIN (информация, связанная с финансами), PINWALE (текстовая информация) и т.д.

По данным Эдварда Сноудена, программы наблюдения делятся на апстримовые и даунстримовый[3].

1. Апстрим программы (от англ. «upstream» – входящий поток) – комплекс мероприятий АНБ, посредством которых они перехватывают весь входящий в США сетевой траффик, т.е. все сообщения, передаваемые посредством телефонной связи, интернета, иных источников связи иностранными гражданами. Сбор информации, проходящей

DOI: 10.7256/2222-1964.2015.4.16213

через территорию США по оптоволоконным кабелям – наиболее «чистый» способ получения информации. Она изымается не из серверов, а непосредственно из каналов связи.

2. Даунстрим программа (от англ. «downstream» – исходящий поток) PRISM – это комплекс административных мер, позволяющих собирать информацию с серверов Google, Facebook, Apple, Yahoo и некоторых других крупных компаний, находящихся в США. Целью наблюдения могут быть либо иностранные пользователи, либо граждане США, чьи контакты включают иностранцев. В рамках данной программы спецслужбы с разрешения засекреченного суда FISC могут запросить информацию о конкретной личности.

Однако список государственных программ по осуществлению слежки и сбору конфиденциальной информации является закрытым и функции многих из них нам неизвестны, а те немногие данные, которые просачиваются в открытые источники, не позволяют составить полную картину и степень вторжения деятельности спецслужб США в частную жизнь граждан на территории всего мира.

В то же время можно констатировать, что сбор данных осуществляется по двум направлениям:

1. Сбор, собственно, самой информации. Сообщения электронной почты, записи голосовых и видеочатов, фотографии и видео и т.д. Сбор осуществляется на основании FISA Amendments Act Section 702 с серверов крупных компаний, указанных выше.
2. Сбор метаинформации. Информация об информации: IMEI (международный идентификатор мобильного оборудования), время телефонного разговора и его продолжительность, местоположение участников разговора, серийный номер SIM карты и телефона; дата отправления электронной почты, IP адрес отправителя и получателя, длительность сессии и т.д. Такая информация поступает от телефонных компаний и провайдеров сетей телекоммуникации. Если получение непосредственного содержания сообщений представляет определенную сложность, то сбор метаданных происходит в фоновом режиме. На основе данной информации можно установить, где и в какое время находился человек, с кем он общался, какие сайты посещал.

Правовым основанием всех вышеуказанных действий американских спецслужб являются два документа:

1. Параграф 702 Fisa Amendments Act of 2008 (FAA)[4], который был обновлен в 2012. Он позволяет осуществлять сбор информации о сообщениях без получения ордера, когда хотя бы один из сообщающихся является иностранным гражданином.
2. Параграф 15 Patriot Act [5], позволяющий собирать информации о звонках американских граждан. Собственно, он и дает право АНБ получать информацию от таких

DOI: 10.7256/2222-1964.2015.4.16213

гигантов телефонии как Verizon или AT&T.

Помимо этого, на основе анализа американского законодательства мы можем установить, что действия американских спецслужб фактически легализованы в следующих документах:

a) Foreign Intelligence Surveillance Act (Fisa) of 1978 [6].

В своей оригинальной редакции позволял слежку без судебного ордера сроком до одного года, если ни один из сообщающихся не был американским гражданином, а также если информация, изымаемая ими не касается гражданина США. В этом случае Президент посредством определённых действий со стороны Генерального прокурора установить слежку. Причем объектом слежки без ордера могли быть только лица, подпадающие под описание «иностранной силы» данное п. 1, 2 и 3 параграфа 1801 36 главы 50 раздела U.S.C (Кодекс США). В ином случае – в течение 72 часов после начала слежки должен был быть получен судебный ордер. Для этого, чтобы воспользоваться данной возможностью спецслужба должна была доказать FISC, что цель слежки является иностранным агентом или шпионом.

b) Приказ президента Рейгана 12333 от 4 декабря 1981 г. (был дополнен приказами Буша 13355 от 27 августа 2004 г. и 13470 от 30 июля 2008 г.) [7].

Расширял полномочия спецслужб на сбор информации в целях «защиты нации».

c) USA PATRIOT Act of 2001: Sections 214, 216.

Дополняет FISA и позволяет спецслужбам осуществлять собор мета информации через каналы связи, которая может относиться к расследованию террористической или шпионской деятельности, а не просто к личности вероятного иностранного шпиона.

d) USA PATRIOT Act of 2001: Section 215.

Дополняет FISA, позволяющий службам получать доступ к так называемым «tangible things» – «осязаемым вещам». Эти «вещи» не обязательно должны принадлежать подозреваемому, но просто должны быть связаны с самим расследованием. В целом Patriot act значительно расширил компетенцию спецслужб по слежке после 11 сентября.

e) Fisa Amendments Act of 2008: Sections 703, 704.

Благодаря внесению данных изменений у NSA появилась возможность также следить и за американскими гражданами, находящимися не на территории США.

f) Письма национальной безопасности.

Письма национальной безопасности – запрос, позволяющий ФБР собирать необходимую метаинформацию в интересах проводимого расследования. Не подлежат судебному контролю, также к подобным письмам прилагается так называемый «gag order» – постановление о неразглашении содержания письма.

g) Ордеры, выдаваемые FISC.

FISC (United States Foreign Intelligence Surveillance Court) – специализированный суд, выдающий раз-

DOI: 10.7256/2222-1964.2015.4.16213

решения на осуществление слежки за гражданином США. Создан и действует на основе раздела 103(а) FISA. Глава Верховного суда США назначает 11 судей, неподконтрольные Конгрессу. В сущности, FISC в закрытом режиме (процедуры закрыты, решения не публикуются) рассматривает дела о правомочности масштабного сбора метаданных в рамках разведывательных мероприятий спецслужб в отношении предполагаемых террористов и иностранных шпионов. Суд действует ex parte – решение принимаются в присутствии лишь представителя правительства и судьи. Основной пик деятельности – период после событий 11 сентября, когда в общей сложности было сделано около 20000 запросов, из которых только в 11 было отказано.

На основании всего изложенного выше мы можем прийти к следующим выводам:

Деятельность спецслужб, в частности АНБ, основываются на актах, которые преимущественно были изданы после событий 11 сентября, который, в сущности, легализуют осуществление слежки американским правительством за иностранными гражданами.

Законодательно установленные нормы расширительно толкуются в закрытом от общества порядке АНБ посредством решений FISC, а также различных внутриведомственных документов (например, решение FISC о Verizon)

Отсутствует адекватный контроль не только со стороны широкой общественности, но даже со стороны американского правительства и законодателя за деятельностью АНБ в области сбора конфиденциальной информации и слежки, как за иностранными, так и за американскими гражданами. Переписка Директора АНБ и главного судьи FISC демонстрирует, что АНБ зачастую при использовании ордеров выходит за пределы установленной компетенции. Суд не осуществляет постоянный мониторинг деятельности АНБ, которое, в свою очередь, не предоставляет развернутую информацию о своей деятельности FISC.

Отсутствует прозрачность в объемах, способах и качестве получаемой специалистами спецслужб информации. Например, при сборе информации об иностранных гражданах АНБ в процессе также получает так же огромные потоки информации, затрагивающих и граждан США.

Существует международное сотрудничество между спецслужбами США и ряда других государств (Британия, Канада и т.д.), в рамках которого они осуществляют совместную деятельность по сбору конфиденциальной информации граждан и слежку за международными организациями и лидерами стран мира.

Остается открытым вопросы о финансировании сотрудничества между крупнейшими интернет-компаниями и правительством, т.е. оплачивают ли спецслужбы услуги по предоставлению доступа к информации сотрудничающим компаниям или же просто осуществляется силовое давление со стороны АНБ?

Существует огромное количество засекреченных программ, баз дан-

DOI: 10.7256/2222-1964.2015.4.16213

ных и операций АНБ, о большинстве из которых общество не имеет ни малейшего представления.

Отсутствуют действенные международные правовые механизмы способные урегулировать сложившуюся ситуацию.

Все вышеперечисленное в равной мере может быть применено к действиям любой спецслужбы, любого государства в мире. Соответственно для повышения информационной безопасности личности нужно выработать комплекс правовых мер, позволяющих эффективно защитить данные и метаданные о личности. Особенности современной трансграничной передачи данных и организации сетей телекоммуникации, обуславливают, что только национальное законодательство не может эффективно защищать тайну частной жизни своих граждан.

По нашему мнению в сложившейся ситуации возник ряд проблем, которые требуют урегулирования международным правом в самое ближайшее время. К таковым относятся:

Внести поправки в международное законодательство, которые установят прозрачную и конкретную процедуру получения правительствами информации как об собственных гражданах, так и иностранных гражданах вне зависимости от их нахождения, а так же запрет на тотальное электронное наблюдение в виртуальном пространстве за гражданами.

Модернизировать механизм внутригосударственного мониторинга за деятельностью спецслужб по сбору и анализу информации.

Создать действенные международно-правовые механизмы, устанавливающий ответственность за нарушение данных ограничений.

Библиография:

1. Энтин М.Л. Международные гарантии прав человека: Опыт Совета Европы. М.: Издательство Московского независимого института международного права. 1997. С. 235.
2. The NSA Files // The Guardian [Official Website]. URL: http://www.theguardian.com/world/the-nsa-files
3. NSA slides explain the PRISM data-collection program [Электронный ресурс] // The Washington Post [Official website]. URL: http://www.washingtonpost.com/wp-srv/special/politics/prism-collection-documents
4. H.R. 6304 (110th): FISA Amendments Act of 2008 // Govtrack [Official website]. URL: https://www.govtrack.us/congress/bills/110/hr6304/text
5. USA PATRIOT Act (H.R. 3162) // Electronic Privacy Information Center [Official website]. URL: http://epic.org/privacy/terrorism/hr3162.html
6. 92 STAT. 1783-FOREIGN INTELLIGENCE SURVEILLANCE ACT // U.S. Government Printing Office [Official website]. URL: http://www.gpo.gov/fdsys/granule/STATUTE-92/STATUTE-92-Pg1783/content-detail.html
7. Executive Order 12333 of Dec. 4, 1981 // Federation of American Scientists [Official website]. URL: http://www.fas.org/irp/offdocs/eo/index.html (дата обращения: 08.11.13)
8. Glenn Greenwald. NSA collecting phone records of millions of Verizon customers daily // The Guardian [Official website]. URL: http://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order

DOI: 10.7256/2222-1964.2015.4.16213

9. Ewen Macaskill, Gabriel Dance. NSA Files Decoded: What the revelations means for you // The Guardian [Official website]. URL: http://www.theguardian.com/world/interactive/2013/nov/01/snowden-nsa-files-surveillance-revelations-decoded#section/1
10. Л.В. Филатова Влияние общепризнанных принципов и норм международного права на развитие информационного законодательства в России // Журнал зарубежного законодательства и сравнительного правоведения / Journal of foreighn legislation and comparative law. – 2011. – 6. – С. 79-86.
11. Р. М. Асланов Зарубежный опыт правового регулирования обеспечения информационной безопасности // Политика и Общество. – 2012. – 2. – С. 45-48.

References (transliterated):

1. Entin M.L. Mezhdunarodnye garantii prav cheloveka: Opyt Soveta Evropy. M.: Izdatel'stvo Moskovskogo nezavisimogo instituta mezhdunarodnogo prava. 1997. S. 235.
2. 2. The NSA Files // The Guardian [Official Website]. URL: http://www.theguardian.com/world/the-nsa-files
3. Glenn Greenwald. NSA collecting phone records of millions of Verizon customers daily // The Guardian [Official website]. URL: http://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order
4. Ewen Macaskill, Gabriel Dance. NSA Files Decoded: What the revelations means for you // The Guardian [Official website]. URL: http://www.theguardian.com/world/interactive/2013/nov/01/snowden-nsa-files-surveillance-revelations-decoded#section/1
5. L.V. Filatova Vliyanie obshchepriznannykh printsipov i norm mezhdunarodnogo prava na razvitie informatsionnogo zakonodatel'stva v Rossii // Zhurnal zarubezhnogo zakonodatel'stva i sravnitel'nogo pravovedeniya / Journal of foreighn legislation and comparative law. – 2011. – 6. – C. 79-86.
6. R. M. Aslanov Zarubezhnyi opyt pravovogo regulirovaniya obespecheniya informatsionnoi bezopasnosti // Politika i Obshchestvo. – 2012. – 2. – C. 45-48.

DOI: 10.7256/2222-1964.2015.4.16213