OBSERVARE 2nd International Conference

2 - 3 July, 2014

II Congresso Internacional do OBSERVARE

2 - 3 Julho, 2014

Actas

Universidade Autónoma de Lisboa | Fundação Calouste Gulbenkian

http://observare.ual.pt/conference

UAL UNIVERSIDADE AUTÓNOMA DE LISBOA

OBSERVARE Observatório de Relações Exteriores UNIVERSIDADE AUTÓNOMA DE LISBOA

Segurança Humana e os Cidadãos Europeus:

O Impacto do PATRIOT Act e do Foreign Intelligence Amendments Act

Ana Vanessa Silva

Mestranda em Relações Internacionais / Universidade do Minho

Portugal

E-mail: vanessa_silva8@hotmail.com

Abstract

A proliferação dos poderes de vigilância combinados com a priorização da segurança nacional numa conjuntura contraterrorista contribuiu para a edificação de programas de vigilância em massa. A proteção da privacidade tem-se constituído, sem dúvida, como um dos direitos fundamentais mais impugnados. A reconfiguração da vigilância no pós-11 de Setembro, que permite um acesso massificado a dados de comunicações (Internet e serviços de telecomunicações), estendeu-se sobretudo com a aplicação de dois documentos legislativos: *PATRIOT Act*, 2001 e o *Foreign Intelligence Surveillance Amendments Act*, 2008).

Estes documentos introduziram os dois instrumentos legais utilizados pelo governo norte-americano para a recolha de dados de cidadãos estrangeiros: a seção 215 do *PATRIOT Act*, e a seção 702 do *Foreign Intelligence Surveillance Amendments Act*.

Consciente deste facto, o objetivo desta comunicação incide na análise do impacto exercido sob as liberdades civis, em particular o direito à privacidade, dos cidadãos europeus, através da aplicação de programas de vigilância em massa derivados da aplicação extraterritorial de legislação norte-americana.

"It is even not the question of espionage activities between different governments. It is the question of the nature, the scale, and the depth of surveillance that can be tolerated in and between democracies" (Bigo, 2013:9)

1-Introdução

O contexto pós-11 de Setembro demarcou-se pela enfatização das preocupações securitárias e, consequentemente, pela revitalização da segurança nacional, não unicamente, mas com particular enfoque, nos Estados Unidos da América. A ameaça desterritorializada e indeterminada imposta pelo terrorismo marcou o despoletar de um contexto de medo, urgência e excecionalidade que resultou numa tendencial priorização da segurança nacional face às liberdades civis, e nomeadamente à segurança humana.

O aumento das capacidades de vigilância e uma maior troca de informações entre autoridades judiciais e as agências de segurança nacional despontou, deste modo, como uma das soluções mais adequadas para fazer face a um mundo de "unknown unknowns" (Rumsfeld, 2002).

A extensão destes poderes de vigilância dos indivíduos acentuou-se sobretudo no período pós-11 de Setembro. De facto, seis semanas após os ataques terroristas que detonaram as torres gémeas era aprovado um documento legislativo que estendia longamente a capacidade governamental de vigilância, primordialmente através de emendas a estatutos precedentes[1]: o *USA PATRIOT Act*[2]. Este documento legislativo, composto por dez títulos, emerge da necessidade e vontade das autoridades americanas de facilitar as investigações de terrorismo, melhorar as trocas de informação entre as diversas agências de segurança (por exemplo, maior troca de informação entre o *Federal Bureau of Investigation* e a *Central Agency of Intelligence*), alterar a própria definição de terrorismo, tornando-a mais abrangente, entre outros propósitos.

O *PATRIOT Act* abriu um precedente ao aumento, gradualmente significativo, da vigilância como instrumento essencial à manutenção da segurança nacional. De facto, este introduz emendas expressivas a um estatuto precedente – o *Foreign Intelligence Surveillance Act* de 1978[3]. Um dos principais impactos desta emenda legislativa é a extensão da

[1] FISA 1978; ECPA; Privacy Act
[2] Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act (adiante designado como *PATRIOT Act*).
[3] O Foreign Intelligence Surveillance Act (FISA) emerge em 1978 com o propósito de diferenciar a vigilância direcionada para cidadãos americanos e a vigilância de cidadãos estrangeiros, focando-se exclusivamente no segundo grupo. Este despoleta sobretudo numa tentativa de controlar os abusos governamentais de vigilância doméstica da segunda metade do século XX. Deste modo, este documento

possibilidade de obtenção de dados que estão na posse de empresas dos EUA, por parte do governo norte-americano (Hoboken, Arnbak e Eijk, 2013:5), através de provisões como a seção 215 (*PATRIOT Act*), entre outras. As emendas significativas ao *FISA* promulgadas inicialmente pela aplicação do *PATRIOT Act* culminariam mais tarde com a edificação de uma legislação que visava estender ainda mais o escopo e âmbito de aplicação de instrumentos de vigilância – o *Foreign Intelligence Surveillance Amendments Act* (FAA).

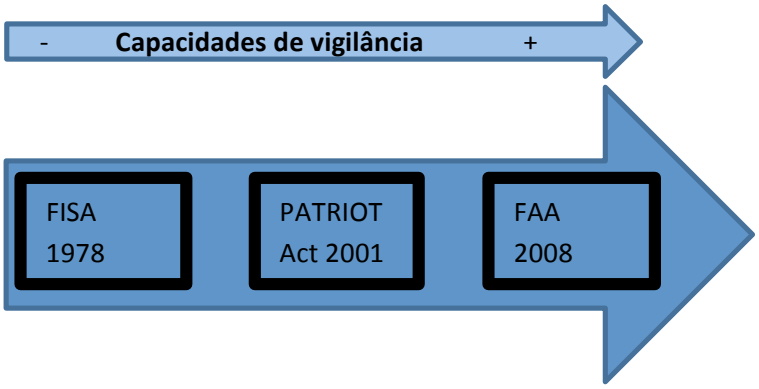

Figura 1 – Evolução Sucessiva Documentos Legislativos

É exatamente nesta evolução que surge a justificação legal para a aplicação de programas de vigilância da Agência de Segurança Nacional, como os revelados por Edward Snowden em Junho de 2013. O propósito desta comunicação assenta assim na análise de dois instrumentos legais – seção 215 do *PATRIOT Act* e seção 702 do FAA – que permitem a aplicação de dois programas de vigilância que têm um impacto direto nas liberdades civis do cidadãos europeus[4] - o programa de recolha em massa de metadados telefónicos e o programa PRISM [5]. Ademais, pretende-se demonstrar que, através da sua aplicação, as liberdades civis, garantidas por estatutos de proteção de dados e privacidade, tais como a Diretiva de Proteção de Dados da União Europeia, são desrespeitadas, subsequentemente restringindo a segurança humana dos cidadãos europeus.

Conceptualização

legislativo permitia a recolha de dados de estrangeiros através de vigilância eletrónica. No entanto, apesar de estar: "initially focused on electronic surveillance, FISA expanded over time to incorporate physical searches, pen registers and trap and trace, and searches of business records and tangible goods" (Donohue, 2014:764).

[4] O foco desta comunicação assenta nos cidadãos europeus, no entanto o impacto da aplicação extraterritorial dos programas de vigilância da Agência de Segurança Nacional (NSA) poderá atingir as liberdades civis de qualquer cidadão estrangeiro.

[5] Estes são apenas dois dos programas revelados por Edward Snowden. De facto, outros programas foram revelados pelo ex-funcionário da CIA, tais como: Upstream, Xkeyscore ou Bullrun.

Primeiramente, torna-se relevante expor, muito brevemente, as bases teóricas desta comunicação. A segurança humana emerge como paradigma no período pós-Guerra Fria, imerso na busca académica de um conceito de segurança mais aprofundado – expansão vertical da segurança para a inclusão de outros objetos de referência, para além do Estado – e alargado – extensão horizontal da segurança na tentativa de incluir outras ameaças para além da militar – de forma a dissolver a insatisfação crescente que envolvia as tradicionais abordagens estato-cêntricas da segurança.

A conceptualização da segurança humana está envolta em debate, sendo que inúmeras expressões foram utilizadas para a caracterizar: "a holistic paradigm" (Acharya, 2004), "a malleable concept" (Christie, 2010), "a paradigm shift and bridging concept" (Glasius, 2008), "a dog that didn't bark" (Chandler, 2008), or even "a reductionist, idealist notion that adds no analytical value" (Buzan, 2004). Com efeito, a compreensão deste paradigma assenta na consciencialização da sua dicotomia conceptual[6].

Deste modo, esta comunicação opta por analisar a segurança humana sob o prisma de uma abordagem restrita. Ademais, é ainda utilizada uma definição contextual de segurança humana, uma vez que esta:

> offers a solution to the concept's deficiencies deriving from its holism, that is to say, its weak descriptive and causal power. They [contextual definitions] also permit the focus of the research to be redirected towards the development of issue-specific micro theories and, thus, they additionally provide a solution to the problem of constructing a comprehensive human security theory with concurrent utility for all relevant disciplines (Tzifakis, 2011:363).

Para os efeitos desta comunicação, entende-se por segurança humana, a ausência de violência material – ameaças físicas à vida e segurança - e de violência imaterial – desrespeito dos direitos civis e políticos dos indivíduos. Com efeito, o conceito de liberdades civis é também entendido como o conjunto de direitos e liberdades fundamentais, tais como a liberdade de expressão, o direito à privacidade, a liberdade de expressão, e outros. Por outras palavras, este é considerado como um sinónimo dos direitos civis e políticos, que constituem a primeira geração de direitos humanos, institucionalizada e legalizada através da Declaração Universal dos Direitos Humanos (1948) e o Pacto Internacional de Direitos Civis e Políticos (1961). Deste modo intenta-se demonstrar o impacto de medidas contraterroristas domésticas (dos EUA) na segurança humana, através do desrespeito das liberdades civis.

---

[6] Por dicotomia conceptual pretende-se abordar as duas conceções dominantes: uma conceção alargada (*freedom from fear* e *freedom from want*) e um conceito mais restrito de segurança humana (*freedom from fear* e ausência de violência). Para mais informações, consultar: Shahrbanou Tadjbakhsh e Anuradha M. Chenoy. 2007. *Human Security: Concepts and Implications*. New York: Routledge.

2- Modelos de Regulação da Privacidade: UE vs. EUA

O conceito de privacidade, à semelhança de inúmeros conceitos que envolvem a disciplina das Relações Internacionais, é debatido e não-consensual. Deste modo, os modelos de regulação da privacidade apresentam também diferenças (Bygrave, 2013: 7). Existem dois modelos predominantes na esfera internacional: o modelo de regulação americano e o modelo de regulação europeu, cujas características apesar de serem similares em princípios, distinguem-se nas formas de aplicação[7].

De facto, as divergências emergem nos estatutos legais de proteção de dados e privacidade. Enquanto os EUA optam por documentos legislativos menos rigorosos e abrangentes, preferindo legislação especializada em determinada área no âmbito da privacidade (leis separadas que regem os dados da saúde, da comunicação, entre outras), os Estados-membros da União Europeia optaram pela edificação de um documento legislativo mais abrangente e reforçado: a Diretiva Europeia de Proteção de Dados de 1995 (Bygrave, 2013; Stratford, 1998; Rubinstein, Nojeim and Lee, 2014). Segundo Lee Bygrave as distinções dos modelos de regulação assentam inicialmente no próprio entendimento do conceito de privacidade. Se por um lado, os EUA tendem a percecionar a privacidade como a liberdade da intrusão governamental, no contexto europeu a privacidade está também extremamente correlacionada com a dignidade e honra individual, sendo não só um valor fundamental para o indivíduo, mas também para a sociedade contribuindo para a manutenção da democracia e pluralismo (Whitman, 2004; Bygrave, 2013).

Apesar de existência de certas divergências na estruturação dos modelos de regulação de proteção de dados e privacidade, pretende-se evitar comparações normativas. Não obstante, o facto da União Europeia regular estes direitos através de uma legislação abrangente e mais compreensiva, tal não implica que em outras questões de direitos fundamentais a cultura política norte-americana seja mais sensível, tal como em assuntos relacionados com a liberdade de expressão (Hoboken, Arnbak and Eijk, 2013:3).

A desarmonia, com maior impacto para o tema tratado nesta comunicação é, sem dúvida a proibição, instaurada pela Directiva de Protecção de Dados da EU, de transferência de dados pessoais para países não-europeus cujos níveis de proteção de dados não sejam 'adequados'[8].

---

[7] Para mais informações acerca do desenvolvimento do conceito de privacidade, bem como as similitudes e diferenças entre os modelos de regulação americano e europeu, consultar. Lee Bygrave. 2013. Transatlantic Tensions on Data Privacy. *Transworld*, Working Paper 19:1-21.

[8] Artº 25 Directiva 95/46/EC: "Os Estados-membros estabelecerão que a transferência para um país terceiro de dados pessoais objeto de tratamento, ou que se destinem a ser objeto de tratamento após a sua transferência, só pode realizar-se se, sob reserva da observância das disposições nacionais adotadas nos

Apesar, da UE ter reconhecido a não-adequabilidade[9] da proteção de dados nos EUA, esforços de harmonização foram encetados, com o estabelecimento de medidas *ad hoc* no sentido de estabelecer transferências de dados que satisfizessem ambas as partes (Schwartz, 2013). Entre estas medidas podem destacar-se: o *Safe Harbour Agrement*, algumas *Model Contractual Clauses* e *Binding Corporate Rules* (Schwartz, 2013:1967):

3- Privacidade e Proteção de Dados no Contexto Pós-11/9

Uma das características principais da vigilância no pós-11 de Setembro é a tendência progressiva para a 'tecnologização da segurança'[10]. De facto, gera-se um entendimento generalizado e redimensionado da necessidade de utilização das novas tecnologias como instrumentos de segurança ao serviço do Estado (Ceyhan, 2008:103).

Além disso, a crescente consciencialização da globalização, o desenvolvimento tecnológico na extração de dados, a utilização crescente de serviços de 'cloud computing'[11] por parte dos indivíduos, e a maior facilidade de análise de dados recolhidos contribuíram para uma crescente expansão da vigilância para além das fronteiras – vigilância transnacional (Cate, Dempsey and Rubinstein, 2012:195; Sinha, 2014; Hoboken and Rubinstein, 2014). Sem embargo, a espionagem internacional não é um fator de surpresa no seio da comunidade internacional, no entanto a escala em que é realizada atualmente surpreende pela capacidade de intrusão e desrespeito dos direitos fundamentais (Bowden, 2013;).

O impacto é extremamente amplificado devido à crescente utilização de serviços de 'cloud computing' como foi acima referido. De facto, consciente da supremacia americana no fornecimento deste género de serviços, bem como da legislação americana que permite acesso governamental aos dados dos utilizadores destes serviços, para além do território americano, compreende-se as potencialidades da vigilância em massa (Schwartz, 2013, Bowden, 2013)

---

termos das outras disposições da presente diretiva , o país terceiro em questão assegurar um nível de proteção adequado."

[9] Ver: Working Party on the Protection of Individuals with regard to the Processing of Personal Data, Opinião 1/99 concerning the level of data protection in the United States and the ongoing discussions between the European Commission and the United States Government. Disponível em: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/1999/wp15_en.pdf

[10] De acordo com Ceyhan, a 'tecnologização da segurança' consiste em: "making of technology the centerpiece of security systems nd its perception as an absolute security provider" (Ceyhan, 2008:102).

[11] O termo 'cloud computing' refere-se a um "technical arrangement under which users store their data on remote servers under the control of other parties, and rely on software applications stored and perhaps executed elsewhere, rather than on their own computers" (Svantesson e Clarke, 2010:391).

Além disso, verifica-se também uma reforma do paradigma da vigilância, que evoluiu da tradicional vigilância particularizada, para uma vigilância em massa (Harris, 2013:2; Donohue, 2014)

A busca governamental de dados pessoais colecionados por empresas privadas tem sofrido um incremento substancial. Deste modo,"government agencies seek larger and larger volumes of data, claiming that bulk access is necessary to find "the needle in the haystack" (Harris, 2013:2; Donohue, 2014:892). De acordo com o argumento utilizado pelas autoridades de segurança nacional americanas[12] tendo em conta as ameaças não-tradicionais que os EUA enfrentam, em particular e com especial enfoque o terrorismo, torna-se essencial a recolha de dados em massa para a possível utilização no futuro. Esta é uma vigilância não-direcionada e indeterminada. São exatamente estas caraterísticas que aleitam debates acerca da necessidade, proporcionalidade e legitimidade deste tipo de vigilância (Greene e Rodriguez, 2014:4;

4- Emergência de novos Programas de Vigilância: Instrumentos Legais

Nesta conjuntura de securitização do terrorismo (Lobo Fernandes, Entrevista, 2014; Pureza, Entrevista, 2014), redimensionado após os ataques terroristas de Setembro de 2001, aliado a uma progressiva tendência para a vigilância em nome da proteção da segurança nacional, programas de vigilância cada vez mais intrusivos despontaram (Moraes, 2014; Bowden, 2013; Estes programas demarcam-se pelo sigilo massivo em que emergem. (Greene e Rofriguez, 2014:5)

As revelações de Edward Snowden no início do Verão de 2013[13] vieram abalar claramente o equilíbrio e confiança no seio das relações transatlânticas (Moraes, 2014:24)

Since June 2013, the leak of thousands of classified documents regarding highly sensitive U.S. surveillance activities by former National Security Agency (NSA) contractor Edward Snowden has greatly intensified discussions of privacy, trust, and freedom in relation to the use of global computing and communication services (Hoboken e Rubinstein, 2014:488).

De facto, segundo este ex-funcionário da CIA, a Agência Nacional de Segurança desenvolveu inúmeros programas de vigilância com capacidade de recolha em massa de dados

[12] "The mission of the NSA is to make the nation safer by providing policy makers and military commanders with timely foreign intelligence and by protecting national security information networks" (NSA's Civil Liberties and Privacy Office Report, 2014:1).

[13] Para mais informações consultar: http://www.theguardian.com/world/interactive/2013/jun/06/verizon-telephone-data-court-order; http://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order

de cidadãos americanos (através de programas como o de recolha de metadados telefónicos) e, exclusivamente, de estrangeiros (programas como o PRISM).

Esta comunicação visa focar-se unicamente no impacto dos instrumentos legais que permitiram os dois programas supracitados, e consequentemente desprezaram as liberdades civis dos cidadãos europeus, não só por uma questão de restrição analítica, mas também pela escala expressiva de vigilância permitida por ambos os programas.

Primeiramente, é necessário expor os instrumentos legais utilizados para a aplicação dos programas. Enquanto o *PATRIOT Act* contribui para a justificação de programas de vigilância com a seção 215, o FAA insere a seção 702. Ambas as autoridades legais necessitam da autorização e supervisão do Tribunal do FISA (FISC), para a vigilância (EU Report, 2013)

Seção 215 do *PATRIOT Act*:

Esta seção permite ao FBI, através de uma ordem judicial atribuída pelo FISC, aceder a qualquer tipo de registo de empresas, desde que estes sejam considerados necessários para uma investigação que tem por base a recolha de '*foreign intelligence information*'[14]. Esta provisão surge no *PATRIOT Act* como emenda ao precedente *Foreign Intelligence Surveillance Act* (1978). Com o surgimento do FAA esta seção voltou a ser emendada.

As ordens judiciais, atribuídas pelo FISC, relativas a esta seção não podem ser direcionadas a cidadãos americanos, se as atividades que forem afetadas estiverem protegidas pela 1º Emenda da Constituição dos EUA[15].

Um dos programas de vigilância da Agência de Segurança Nacional Americana autorizado por esta seção é o programa de recolha de metadados[16] telefónicos. Deste modo, através da Agência de Segurança Nacional, o governo norte-americano acede aos registos das chamadas nacionais e internacionais realizadas *de* ou *para* determinados provedores de serviços telefónicos (Greene e Rodriguez, 2014:8).

Estes registos são mantidos durante 5 anos, sendo alvo de uma reautorização a cada 90 dias. A área de aplicação deste programa é extremamente extensa, uma vez que "the database is queried by way of 'selectors', such as telephone numbers , for which there is a 'reasonable articulable suspicion' of a link to terrorism. The database is queried to identify every call made

[14] Seção 215 "the Director of the Federal Bureau of Investigation or a designee of the Director (whose rank shall be no lower than Assistant Special Agent in Charge) may make an application for an order requiring the production of any tangible things (including books, records, papers, documents, and other items) for an investigation to obtain foreign intelligence information not concerning a United States person or to protect against international terrorism or clandestine intelligence activities".

[15] 1º Emenda "Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the government for a redress of grievances" (Legal Information Institute, 2014).

[16] Nos EUA uma distinção é feita entre dados de conteúdo (conteúdo das chamadas) e os metadados (tudo o que não é conteúdo, tal como a hora, duração, os números telefónicos envolvidos, entre outros dados da chamada).

to and from the selector, and then as a second 'hop', every call made to or from those numbers. Prior to January 2014, the analysis was carried out to a third 'hop' as well" (Greene e Rodriguez, 2014:8). Deste modo, desde a aplicação do programa, é extremamente provável que este tenha tido acesso a milhões de chamadas.

Seção 702 do *Foreign Intelligence Surveillance Amendments Act*:

Com a aprovação do *Foreign Intelligence Surveillance Amendments Act*, em Julho de 2008, estenderam-se as alterações ao *Foreign Intelligence Surveillance Act* de 1978. Uma dessas alterações constitui-se na introdução de uma nova provisão, seção 702. Ao contrário, da seção acima descrita, a seção 702 visava exclusivamente os cidadãos estrangeiros, sendo o seu objetivo a recolha de informações de estrangeiros que se encontrassem fora do escopo territorial dos EUA.

Esta permite ao Procurador-Geral, bem como ao *Director of National Intelligence*, autorizar conjuntamente "the targeting of persons reasonably believed to be located outside the United States to acquire foreign intelligence information" (Section 702, FAA).

Uma das principais alterações introduzidas por esta emenda é o facto da vigilância exercida sob a alçada desta seção não estar restringida por uma causa provável ou uma suspeita individual. Assim, esta permite ao governo americano aceder a informações de qualquer indivíduo estrangeiro que se encontra fora dos EUA, desde que o propósito da investigação seja a aquisição de '*foreign intelligence information'*.

Um dos programas autorizados através desta provisão é o PRISM[17]:

Este programa foi lançado em 2007, surgindo no seguimento de um programa secreto de escutas sem ordens judiciais ('*warrantless wiretapping'*[18]) e *o Protect America Act*, e permite o acesso aos dados de comunicações recolhidos e armazenados por servidores de Internet, tais como o Facebook, Google, Microsoft, Yahoo, entre outros (Bigo, Boulet, Bowden, Carrera, Guild, Hernanz, Hert, Jeandeboz e Scherrer, 2013:2).

Este programa permite assim ao governo norte-americano aceder aos dados eletrónicos privados de utilizadores destes serviços, surgindo numa evolução e extensão dos instrumentos de vigilância, iniciado no contexto pós-11 de Setembro. Ademais, o seu escopo de funcionamento estende-se sobretudo devido à sua correlação com os serviços de 'cloud computing', pois estes permitem aceder a um muito mais alargado número de dados.

Ambos os programas de vigilância envolvem a recolha massiva de dados de comunicações durante um período extenso de tempo e numa base de quase contínua regularidade (Greene and Rodriguez, 2014:15; Bowden, 2013).

---

[18] Programa secreto iniciado no pós-11 de Setembro, e que foi publicamente revelado em 2005.

5- Impacto nos Cidadãos Europeus

Após a abordagem dos instrumentos legais norte-americanos para a vigilância externa, cuja aplicação pode ser verificada não unicamente, mas particularmente nos dois programas acima mencionados, torna-se relevante expor o impacto da sua aplicação nos cidadãos europeus.

Um dos principais efeitos do aumento das capacidades de vigilância constitui-se, sem dúvida, no foco que este coloca nos cidadãos estrangeiros que não se encontram no território norte-americano (cerca de 95% da restante população mundial). Deste modo, a vigilância destes cidadãos realiza-se através da interceção das suas comunicações realizadas *para* ou *via*[19] os EUA.

Verificou-se assim, através da aplicação destas medidas legislativas, a criação de um *duplo standard*: os cidadãos norte americanos, protegidos pelas provisões constitucionais[20], (em particular 1ª e 4ª emendas) e os cidadãos estrangeiros, grupo no qual se encontram os cidadãos europeus, sem qualquer tipo de proteção assegurada pela 4ª emenda da Constituição Americana (Hoboken, Arnabak and Eijk, 2013:8).

Apesar de algumas das liberdades civis dos cidadãos norte-americanos serem desrespeitadas através da aplicação destas duas seções – 215 e 702 -, a verdade é que estes estão protegidos pela proibição constitucional de realização de '*unreasonable searches and seizures'*. Por outro lado, através da seção 702 do FAA, os cidadãos europeus estão isentos de qualquer proteção atribuída aos cidadãos americanos, pois, segundo um representante do governo norte americano, "the fourth amendment is not an international treaty" (Hayden, 2013).

Deste modo:

> The problem from a European perspective is that the Fourth Amendment right to communications privacy does not apply to searches of non-citizens conducted by the U.S. government outside the U.S. Even American citizens, however, do not enjoy the full protection of the Constitution when the U.S. government is conducting searches outside the U.S. Further, the Constitution has been interpreted to not require a judicial warrant for surveillance conducted inside the U.S but targeted at certain non-citizens ("agents of foreign powers") who are physically outside the U.S. (Harris, 2013:4-5).

Outro facto digno de interesse, é a diminuta atenção prestada – pelos Media, legisladores ou, até mesmo, organizações de defesa das liberdades civis – ao desrespeito das liberdades civis dos estrangeiros, imposto por estas medidas,continuando este tema a ser

[19] Comunicações estabelecidas através de serviços fornecidos por empresas sediadas nos EUA, tais como as comunicações realizadas através do Facebook, Google, Microsoft, entre outras.
[20] Através da aplicação de procedimentos de minimização e de 'targeting', consultar: Report on Findings by the EU Co-Chairs of the ad hoc EU-US Working Group on Data Protection. 2013.

relegado para segundo plano (Bigo, Boulet, Bowden, Carrera, Guild, Hernanz, Hert, Jeandeboz e Scherrer, 2013:20; Harris, 2013; Hoboken, Arnbak and Eijk, 2013:22)

Não obstante, torna-se essencial expor o conceito de '*foreign intelligence information'*, que é extremamente vasto, permitindo ao governo dos EUA aceder a qualquer tipo de informação de cidadãos estrangeiros, quase sem restrições. Este torna-se fundamental, por constituir uma dos objetivos da aplicação de ambas as seções (215 PA e 702 FAA).

Foreign Intelligence Information - "Information with respect to a foreign-based political organization or foreign territory that relates to, and if concerning a United States person is necessary to the conduct of the foreign affairs of the United States" (Legal Information Institute, 2014).

O impacto negativo da aplicação extraterritorial destes instrumentos legais norte-americanos pode ser resumido em três pontos:

1 – <u>Perda da soberania por parte dos Estados europeus sobre a informação</u>

Um dos principais impactos gera-se na incapacidade de manutenção dos Estados-membros da soberania sobre os dados e informações que se geram nos seus territórios. Deste modo, através de programas, tais como PRISM, o governo norte-americano acede a dados de cidadãos e residentes europeus armazenados no território de Estados-Membros, sem o conhecimento e consentimento desses governos nacionais. Não obstante, através destas práticas, as autoridades americanas desrespeitam as 'regras do jogo' das Relações internacionais (Bigo, Boulet, Bowden, Carrera, Guild, Hernanz, Hert, Jeandeboz e Scherrer, 2013:3), uma vez que acedem extraterritorialmente aos dados de milhões de cidadãos europeus.

Esta interferência externa num dos direitos fundamentais dos cidadãos europeus contribuiu para a diminuição da confiança dos Estados-membros e instituições europeias face aos EUA. Não obstante a análise deste impacto, estas revelações contribuíram para o reconhecimento público das divergências nacionais, no seio da UE, quanto à regulação da vigilância de comunicações. De facto, as estruturas legais são marcadas por ambiguidade e áreas cinzentas no que respeita à vigilância em massa de comunicações, bem como se denota a incapacidade de atuação e monitorização dos excessos dos serviços de inteligência, por parte dos mecanismos de controlo (tais como as Comissões de Proteção de Dados) (Bigo, Boulet, Bowden, Carrera, Guild, Hernanz, Hert, Jeandeboz e Scherrer, 2013:4).

2- <u>Desrespeito dos quadros legais europeus que regulam o direito à privacidade: Carta dos Direitos Fundamentais da União Europeia e a Convenção Europeia dos Direitos Humanos</u>

Os sistemas e instrumentos legais de vigilância em massa tem um efeito imediato no direito à privacidade. Assim, o desrespeito do direito à privacidade garantido pelos quadros legais europeus, artº 8 da Carta dos Direitos Fundamentais da União Europeia e artº 8 da Convenção Europeia dos Direitos Humanos, é outro dos efeitos colaterais da aplicação extraterritorial da legislação norte-americana no seio da UE (Moraes, 2014; Bowden, 2013).

A incapacidade das instituições nacionais e europeias, responsáveis pela proteção de dados e privacidade, garantirem um dos direitos fundamentais, mina a confiança dos cidadãos europeus nas mesmas. No entanto, "surveillance, therefore, has also an effect on other fundamental rights such as freedom of expression, of opinion, of religion, of association, data protection, right to fair trial, access to an effective remedy etc" (LIBE Inquiry, 2014:71)[21].

O Tribunal Europeu dos Direitos Humanos tem repetidamente assegurado que as agências de inteligência, bem como as de segurança nacional devem atuar em sintonia com os direitos fundamentais estabelecidos na Convenção Europeia dos Direitos Humanos (LIBE Inquiry, 2014:72). Apesar de apenas os tribunais poderem afirmar o desrespeito e violação destes princípios, várias declarações tem afirmado este mesmo desrespeito.

3- Desrespeito da Diretiva de Proteção de Dados, bem como os acordos estabelecidos para a sua manutenção

Por último, outro dos efeitos da aplicação destes instrumentos legais, que requerem dados de empresas sedeadas nos EUA, constitui-se no desrespeito por parte do sector privado norte-americano de acordos estabelecidos com a UE para a transferência de dados. Após a aplicação da Diretiva de Proteção de Dados em 1995, bem como a consideração europeia da falta de adequabilidade de proteções de dados nos EUA, estabeleceram-se acordos entre os EUA e a UE para a transferência de dados.

Um desses acordos constituiu-se no *Safe Harbor Agreement* de 2000. Este acordo emerge para implementar um processo no qual as empresas norte-americanas possam cumprir os requisitos da Diretiva de Proteção de Dados. Deste modo, se a empresa americana declarar (apesar da necessidade de um contrato escrito) a aderência aos princípios do *Safe Harbor*, o controlador europeu poderá exportar os dados para essa empresa.

Para além deste acordo outros foram sendo estabelecidos para a transferência de dados, como as Binding Corporate Rules[22]. No entanto, a aplicação destas medidas, bem como a sigilo que deve ser mantido pelas empresas acerca do acesso governamental aos dados, impede o

[21] Para mais informações consultar: LIBE Committee Inquiry: Electronic Mass Surveillance of EU Citizens. Protecting Fundamental Rights in a Digital Age: Proceedings, Outcome and Background Documents.

[22] Consultar: Caspar Bowden. 2013. The US National Security Agency (NSA) Surveillance Programmes (PRISM) and Foreign Intelligence Surveillance Act (FISA) Activities and their Impact on EU citizens' Fundamental Rights. European Parliament's Committee on Civil Liberties, Justice and Home Affairs Report.

cumprimento dos princípios estabelecidos nestes acordos. Deste modo, as empresas sob a jurisdição norte-americana estão sujeitas a conflitos jurisdicionais e de Direito Internacional Público, sendo que "which law they choose to obey will be governed by the penalties applicable and exigencies of the situation, and in practice the predominant allegiances of the company management" (Bowden, 2013:23).

6- Conclusão

A extensão dos poderes de vigilância através da aplicação do *PATRIOT Act*, e subsequentemente do *Foreign Intelligence Surveillance Amendments Act*, contribuiu para a edificação de programas de vigilância cada vez mais intrusivos. Deste modo, a combinação do desenvolvimento tecnológico das capacidades de armazenamento de dados e de serviços de 'cloud computing' (sediados nos EUA) com os poderes extensivos de vigilância de indivíduos, sobretudo estrangeiros, culminou na revelação da existência de programas secretos norte-americanos de vigilância em massa.

Após a consciencialização pública europeia do impacto direto que estes programas impõem sob as liberdades civis, e em particular o direto à privacidade, torna-se imperativo que a União Europeia estabeleça limites à aplicação extraterritorial dos instrumentos legais norte-americanos, bem como fomente a proteção e a garantia dos direitos fundamentais dos seus cidadãos. Algumas propostas de solucionamento foram avançadas, no entanto torna-se manifesta a necessidade de combinar vários tipos de solução, sob o risco de se captar apenas um dos reflexos deste dilema transatlântico.

Em suma, a solução não passa apenas pelo reconhecimento na legislação americana da igualdade dos direitos dos cidadãos europeus, mas também pela reforma da estrutura legal da proteção de dados, bem como pela possibilidade de desenvolvimento de uma 'cloud' europeia. Enquanto o futuro se mantém indefinido, o que se afigura como real é que "neither the United States nor the European Union can afford a transatlantic data war" (Kerry, 2014:17).

7- Bibliografia

Bigo, Didier, et al. 2013. National Programmes for Mass Surveillance of Personal Data in EU Member States and their Compability with EU Law. Report for the European Parliament's Committee on Civil Liberties, Justice and Home Affairs.

Bowden, Caspar. 2013. The US National Security Agency (NSA) Surveillance Programmes (PRISM) and Foreign Intelligence Surveillance Act (FISA) Activities and their Impact on EU

citizens' Fundamental Rights. Report for European Parliament's Committee on Civil Liberties, Justice and Home Affairs.

Bygrave, Lee. 2013. Transatlantic Tensions on Data Privacy. *Transworld*, Working Paper 19:1-21.

Buzan, Barry. 2004. A Reductionist, Idealistic Notion that Adds Little Analytical Value. *Security Dialogue*, 35(3):369-370.

Cate, F.H., Dempsey, J.X., Rubinstein, I.S., 2012. Systematic Government Access to Private Sector Data. *International Data Privacy Law*, 2(4): 195–199.

Ceyhan, Ayse. 2008. Technologization of Security: Management of Uncertainty and Risk in the Age of Biometrics. *Surveillance and Society*, 5(2): 102-123.

Chandler, Jennifer A. 2009. Personal Privacy versus National Security: Clarifying and Reframing the Trade-off. In *On the Identity Trail: Anonymity, Privacy and Identity in a Networked Society*, eds. Kerr, Lucock and Steeves, 121-138. New York: Oxford University Press.

Christie, Ryerson. 2010. Critical Voices and Human Security: To Endure, To Engage or To Critique? *Security Dialogue*, 41(2):169-190.

Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. Disponível em: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en.

Donohue, Laura. 2014. Bulk Metadata Collection: Statutory and Constitutional Considerations. *Harvard Journal of Law & Public Policy*, 37:757-900.

Foreign Intelligence Surveillance Amendments Act of 2008. Disponível em: https://www.govtrack.us/congress/bills/110/hr6304/text

Harris, Leslie. 2013. Testimony Before the European Parliament LIBE Committee Inquiry on Electronic Mass Surveillance of EU Citizens. Disponível em: https://www.cdt.org/files/pdfs/LIBEtestimony24September.pdf

Hoboken, Joris, Axel Arnbak e Nico Eijk. 2013. Obscured by Clouds or How to Address Governmental Access to Cloud Data from Abroad. Disponível em: http://ssrn.com/abstract=2276103

Kerry, Cameron. 2014. Missed Connections. Talking with Europe about Data, Privacy and Surveillance. Center for Technology Innovation at Brookings. Disponível em: http://www.brookings.edu/~/media/research/files/papers/2014/05/20%20europe%20privacy%20surveillance%20kerry/kerry_europefreetradeprivacy.pdf

Glasius, Marlies. 2008. Human Security from Paradigm Shift to Operalization: Job Description for a Human Security Worker. *Security Dialogue*, 39(1):31-54.

Greene, David e Katitza Rodriguez. 2014. NSA Mass Surveillance Programs: Unnecessary and Disproportionate. *Electronic Frontier Foundation*. Disponível em: https://www.eff.org/files/2014/05/29/unnecessary_and_disproportionate.pdf

Rubinstein, Ira e Joris van Hoboken. 2014. Privacy and Security in the Cloud: Some Realism About Technical Solutions to Transnational Surveillance in the Post-Snowden Era. *Maine Law Review*. 66(2):488-533.
Disponível em: http://papers.ssrn.com/sol3/Papers.cfm?abstract_id=2443604

Rubinstein, Ira, Gregory Nojeim e Ronald Lee. 2014. Systematic Government Access to Personal Data: A Comparative Analysis. *International Data Privacy Law*, 4(2):96-119. Disponível em: http://ssrn.com/abstract=2444414

Sinha, Alex. 2014. *NSA Surveillance Since 9/11 and the Human Right to Privacy*. Disponível em: http://ssrn.com/abstract=2327806

Stratford, Jean. 1998. Data Protection and Privacy in the United States and Europe. *IASSIST Conference*, Yale University.

Svantesson, D e Clarke, R. 2010. Privacy and Consumer Risks in Cloud Computing. *Computer Law and Security Review: the International Journal of Technology Law and Practice*, 26(4).

Tzifakis, Nikolaos. 2011. Problematizing Human Security: A General/Contextual Conceptual Approach. *Southeast European and Black Sea Studies*, 11(4):353-368.

USA PATRIOT Act Additional Reauthorizing Amendments Act of 2006. 2006. Disponível em: http://www.gpo.gov/fdsys/pkg/BILLS-109s2271enr/pdf/BILLS-109s2271enr.pdf

Vega, Teresa del Rocío Espinosa. 2012. US Governmental Access to Data in the Clouds through the USA PATRIOT Act. *Law and Technology Master Thesis*. Tilburg University, Netherlands.