A CIBERSEGURANÇA AMERICANA E A ESCOLA DE COPENHAGUE:

DO PARADIGMA DA SECURITIZAÇÃO AO CASO EDWARD SNOWDEN

Julianny Ribeiro Rodrigues[1]

Leonardo Mèrcher[2]

RESUMO

Edward Snowden tornou-se conhecido mundialmente quando revelou programas de coleta de dados em massa realizados pela Agência Nacional de Segurança dos Estados Unidos. A partir disso, a comunidade internacional passou a apresentar questionamentos acerca do direito à privacidade e até onde o espaço cibernético pode ser, de fato, uma ameaça para a sociedade e governos. Com isso, o presente artigo visa demonstrar como o discurso de que uma ameaça está presente na internet pode favorecer a implementação de medidas emergenciais que, pelas vias legais, não poderiam ser feitas. Do ponto de vista teórico, buscaremos uma abordagem que possa assimilar o caso Snowden com a Teoria da Securitização, formulada pela Escola de Copenhague. A importância desta pesquisa deve-se não somente ao fato da grande repercussão que o caso ganhou – uma vez que tal evento não é de todo modo, recorrente, mas também pela sua relevância em termos de políticas de seguranças nacional e internacional e a abrangência ganhada sobre privacidade e vigilância estatal em massa.

PALAVRAS-CHAVE: Caso Snowden; privacidade; vigilância; segurança; Teoria da Securitização.

INTRODUÇÃO

"Pensou no telecrã, nos ouvidos sempre à escuta. Espiavam as pessoas dia e noite [...]" (ORWELL, 2009). O famoso livro "1984", escrito por George Orwell, foi publicado pela primeira vez em 1949, traz com elementos que nos fazem questionar se já não estamos vivendo em um ambiente similar, em especial quando pensamos em privacidade e a forma como os governos nos descrevem as possíveis ameaças à nossa civilização.

[1] Estudante de Relações Internacionais na UNINTER.
[2] Doutor em Ciência Política pela UFPR, professor universitário do curso de Relações Internacionais da UNINTER.

Ao longo do livro, é ressaltado o quanto os cidadãos eram incentivados a acreditar que existia, de fato, um inimigo com o qual o país estava constantemente em guerra, bem como a menção ao “telecrã”, um aparelho que permitia o Estado controlar seus cidadãos dentro das próprias casas. Apesar de ser tão somente uma ficção, há de se pensar se com algumas políticas adotadas nas últimas décadas essa mesma ficção não se tornou um futuro possível.

Nesse sentido, trazemos neste artigo o papel do *whistleblower* Edward Snowden na nossa sociedade, que revelou documentos secretos da Agência Nacional de Segurança dos Estados Unidos, e como o seu caso pode ser aplicado na teoria de securitização da Escola de Copenhague, de modo que possamos analisar se o ciberespaço tornou-se um assunto securitizado.

1 A EVOLUÇÃO DOS ESTUDOS DE SEGURANÇA INTERNACIONAL NO SÉCULO XX

Até o fim da Segunda Guerra Mundial, a corrente realista, conhecida através de autores como Edward Carr e Kenneth Waltz, predominava no meio internacionalista, trazendo como conceitos de estratégia a dissuasão - ou *deterrence*. Com o início do colapso da União Soviética e consequentemente com a queda do Muro de Berlim, o debate precisou ser renovado. Isso porque, uma vez que grande parte da literatura realista era voltada para aspectos militares e estratégicos e sendo essa mesma lógica reproduzida através da política de manutenção da ordem da Guerra Fria. (TANNO, 2003, p. 50), foi possível a consolidação de outras correntes, em especial, a construtivista. Uma das principais diferenças entre as correntes construtivista e realista é que a primeira enfatiza o papel das ideias na política internacional, por considerarem que elas desempenham uma função importante na construção do mundo social enquanto que para a última, as ideias são vistas como objeto marginal de análise (GUEDES, 2009, p.466).

Com isso, além da vertente tradicionalista, na qual o realismo se encaixa, estudando as ameaças à segurança a partir de uma perspectiva objetivista e enfatiza o uso da força (GUEDES, 2009 p.466), também podemos indicar mais duas vertentes: a crítica e a abrangente (BUZAN, 1997).

A vertente crítica propõe a emancipação humana, ou seja, quando falamos em estudos de segurança, os objetos em questão são socialmente construídos; a perspectiva abrangente sustenta uma posição em que a pesquisa de segurança não deve se restringir apenas a área militar, considerando também a existência de outras ameaças que não concernentes a essa área.

Com base nessas definições, podemos citar a Escola de Frankfurt como adepta da vertente crítica (TANNO, 2003, p. 50), enquanto a Escola de Copenhague é considerada abrangente. Para esse artigo, daremos enfoque na Escola de Copenhague, que surgiu exatamente com o objetivo de ampliar o debate.

Era necessário um aprofundamento no conceito de segurança (BUZAN, 1991:3-15). Em contraste com os racionalistas, a Escola de Copenhague traz o conceito onde o campo militar o deixa de ser o principal foco nos estudos de

segurança e abre espaço para que outros atores possam fazer parte da agenda de pesquisa. Importante ressaltar, no entanto, que apesar de os autores abrirem as possibilidades de pesquisa, o Estado ainda é visto como principal objeto de referência. Para além dessa ampliação das unidades de análise, a Escola de Copenhague trouxe como contribuição a teoria de securitização.

1.1 A TEORIA DE SECURITIZAÇÃO

De acordo com Buzan et al. (1998) qualquer assunto pode ir de um espectro não politizado, ou seja, que dado Estado não lida com tal tema e não é algo inserido na esfera pública, para um espetro politizado – onde determinado assunto faz parte do debate público, demandando uma ação estatal, e finalmente para o espectro securitizado, fazendo com que o mesmo assunto seja visto como uma ameaça a soberania a tal ponto que seria justificável implantar medidas emergenciais.

A securitização, portanto, seria vista como uma versão extrema da politização (BUZAN et al., 1998, p.23; GUEDES, 2009, p.479). Para Waever (1995) essa medida permite a agentes estatais que os mesmos criem poderes adicionais, tornando determinados assuntos confidenciais à população e desempenhando atividades que em situações, dadas como normais, seriam ilegais (GUEDES,2009, p.480)

Dentro da teoria de securitização é possível destacar alguns conceitos que nos ajudam a compreendê-la. Ela parte do pressuposto de que a segurança está diretamente relacionada com o ato da fala (também denominado como *speech-act*). O agente securitizador, ou seja, aquele que pretende securitizar algum tema, precisa que esse seja socialmente reconhecido como uma ameaça.

A partir disso, há o objeto referente que é a unidade que o agente securitizado declara como ameaçada, consequentemente, necessitando de proteção. (GUEDES, 2009, p.482). Para Buzan (1991), áreas como a econômica, social, política e ambiental também devem ser discutidas. Hansen and Nissenbaum (2009), trouxeram a internet como tema para dentro da teoria de securitização. Se em seu início era visto por um ponto meramente técnico, a partir dos anos 1990, se tornou um alvo para políticos e corporações, com

declarações como "*bits and bytes can be as threatening as bullets and bombs*[3]" (LYNN, 2011).

A seguir, veremos como se deu o início da internet e como o ciberespaço se tornou um ambiente que estimula esse tipo de discurso [LOBATO E KENKEL, 2015, p. 23].

1.2 A SEGURANÇA PARA ALÉM DAS FRONTEIRAS: A INTERNET

A internet surgiu como um projeto, a ARPANET, com o intuito de interligar bases militares dos Estados Unidos durante a Guerra Fria. O projeto veio a partir do trabalho conjunto entre pesquisadores universitários e militares que criaram uma agência que pudesse destacar a tecnologia americana dos demais, em especial, da então União Soviética, a ARPA (Advanced Research Projects Agency), de modo que eles tivessem uma comunicação de ponta para a época e o momento que viviam.

Apesar de o interesse militar pela ARPANET, surgiu uma razoável estabilidade na Guerra Fria na década de 80, de forma que a rede passou a ter mais abertura para ser utilizada no meio acadêmico e ser aprimorada, surgindo o Protocolo de Controle de Transmissão/Protocolo de Internet (Transmission Control Protocol/Internet Protocol) (OLIVEIRA, 2014, p.15).

Em 1987, portanto, seu uso comercial foi liberado nos Estados Unidos. Como podemos ver nos dias de hoje, uma rede mundial que se construiu ao longo dos anos que também podemos chamar de espaço cibernético, ou ciberespaço (LOPES, 2013).

Hoje, para além do uso doméstico, as infraestruturas de um Estado dependem do ciberespaço, de modo que, como ataques na internet possam ser feitos sob forma de anonimato, é garantido a essas instituições o discurso de que é necessária uma proteção quase militar para deter possíveis ataques. A próxima seção busca focar o objeto de análise e para tanto foi escolhido os Estados Unidos, não apenas pela sua relevância a nível global, como também pelas notícias, relacionadas ao tema, que envolvem a potência como principal ator.

---

[3] "Bits e bytes podem ser tão ameaçadores quanto balas e bombas" (Tradução nossa).

2. OS ESTADOS UNIDOS E O CIBERESPAÇO

Antes mesmo de haver um ambiente tão amplo como o ciberespaço, os Estados Unidos já demonstravam interesse em não só proteger suas informações governamentais - como coletar dados de outras potências. Após o caso de Watergate, que envolveu o então presidente Richard Nixon, foi-se instalada uma comissão para investigar operações federais de inteligência. Em 1978, portanto, o Congresso americano aprovou a Lei de Vigilância Estrangeira ou FISA (do inglês Foreign Intelligence Surveillance Act). O FISA estabelece procedimentos para a vigilância dentro e fora do país, seja por meios físicos ou eletrônicos. O intuito era impedir que cidadãos americanos tivessem seus dados recolhidos pelo governo ou suas agências sem um mandato judicial, enquanto autorizava a coleta de conteúdo de comunicação de qualquer outra pessoa que não seja americana [WIKIPEDIA, online].

Em 1991, a Academia Nacional de Ciências dos Estados Unidos (em inglês, US National Academy of Sciences) publicou um relatório sobre a segurança no computador, alegando que “Tomorrow’s terrorist may be able to do more damage with a keyboard than with a bomb.[4]” [CYBER TELECOM, online] Esse seria apenas um dos vários avisos sobre o uso de computadores e, consequentemente, da internet, feitos pelo governo e por suas agências ao longo da década. Importante notar, no entanto, que até então não havia nenhuma ameaça ou ator concretos que justificassem tais avisos, ou melhor, que houvesse de fato algum inimigo. Esse é um dos aspectos mais perceptíveis no ciberespaço, dado que uma ameaça pode ser feita por qualquer pessoa – seja terroristas, outros países ou alguém que tenha conhecimento na área. Isso foi amplamente debatido na Comissão Sobre Proteção de Infraestruturas Críticas (em inglês, Comission on Critical Infraestructure Protection), relatório realizado sob o mandato do presidente Bill Clinton, em 1997. No relatório há um consenso de que possíveis inimigos são desconhecidos, enquanto os recursos para ataques são extensos (WASHINGTON, DC, 1997).

[4] “O terrorista de amanhã pode causar mais danos com um teclado do que com uma bomba” (tradução nossa)

2.2 A ERA BUSH: O CIBERESPAÇO COMO ALVO

Após os ataques terroristas de 11 de Setembro, o então presidente George W. Bush assinou uma ordem secreta autorizando a Agência de Segurança Nacional (em inglês, National Security Agency / NSA) a espionar cidadãos americanos, apesar das proibições legais – como o FISA [TIMES, 2005]. O objetivo era monitorar atividades através de telefones, internet e outros meios de comunicação, de modo que pudessem obter alguma informação acerca dos atentados e possíveis ligações com a Al Qaeda.

Além disso, em fevereiro de 2003, o novo departamento no governo americano: o Departamento de Segurança Interna (em inglês, Department of Homeland Security / DHS), surgindo para responder a emergências domésticas, como terrorismo, publicou uma carta chamada “A Estratégia Nacional para Garantir a Segurança no Ciberespaço” (em inglês, *The National Strategy to Secure Cyberspace*), demonstrando, a partir disso, um maior direcionamento do governo para o âmbito da internet.

Apesar de focar em especial na proteção de dados do governo, e articulando diversas prioridades de caráter nacional, a fim de garantir a segurança no ciberespaço, a carta cita como objetivo a expansão dos esforços da população na prevenção de ataques cibernéticos, ou seja, havia um interesse para que a sociedade americana aceitasse esse discurso de que qualquer esforço do governo seria pela proteção do país.

Para os anos finais de seu último mandato, Bush enfrentou incidentes relacionados a ataques bem sucedidos a sistemas de informação e bancos de dados do governo, o que o levou a propor um aumento de 10% no financiamento da cibersegurança para o ano de 2009, o que significava 7,3 bilhões de dólares. [ABCNEWS, online]

O subsecretário de proteção do DHS à época, Robert Jamison, afirmou: “estamos preocupados que as ameaças sejam reais e crescentes [...] Estamos mais vulneráveis como nação”. No mesmo ano, o Senado americano aprovou um novo projeto de lei que possibilitava a expansão dos poderes de vigilância dentro do país, além de garantir a imunidade legal para as empresas que cooperavam no programa de escuta telefônica realizado pela NSA.

De acordo com Bush, tal projeto era “crítico para a segurança nacional” e que era necessário se “unir e aprovar leis importantes” como aquela [THE NEW YORK TIMES, online]. Entre a secreta ordem presidencial que mencionamos anteriormente até esse projeto de lei, houve um espaço de seis anos, onde cidadãos americanos já podiam ter seus dados recolhidos através dessas mesmas escutas.

2.3 A CHEGADA DE BARACK OBAMA – A SECURITIZAÇÃO DO CIBERESPAÇO

Os discursos sobre um inimigo desconhecido no ciberespaço e sobre necessidade de aumentar o controle na área não cessaram com a chegada do democrata Barack Obama à presidência. O que era visto como medida emergencial tornou-se uma prática comum no governo americano.

Em seu primeiro ano de mandato, Obama teve de lidar com oficiais das agências de inteligência alertando, anonimamente para a imprensa, sobre como a NSA interceptava ligações telefônicas bem como e-mails pessoais e mensagens de cidadãos americanos, de forma “sistemática e significante” [THE NEW YORK TIMES, online]. No ano seguinte, em 2010, um juiz federal determinou que essas interceptações eram uma violação ao FISA [THE NEW YORK TIMES, online], que conforme mencionamos, exige um mandato judicial para o caso de espionagem doméstica. Dois anos depois, o próprio presidente Obama escreveu um artigo para o jornal americano The Wall Street Journal, onde ele afirma que ataques cibernéticos são “um dos desafios econômicos e nacionais mais sérios que enfrentamos” [WALL STREET JOURNAL, online]. No mesmo artigo, ele continua:

> “Temos a oportunidade – e a responsabilidade – de agir agora e estar um passo a frente de nossos adversários. Para o bem da nossa segurança nacional e econômica, peço ao Senado para aprovar a Lei de Segurança Cibernética de 2012 [...].” [WALL STREET JOURNAL, online]

E finaliza com a seguinte asserção: “é hora de fortalecer nossas defesas contra esse perigo crescente”. [WALL STREET JOURNAL, online] Sua declaração demonstra o movimento feito à época para tornar o ciberespaço uma grande ameaça ao país, dando caráter militar na coordenação das atividades de

operação e defesa, conforme um dos comandos dentro do Departamento de Defesa propôs em 2012, expressando como objetivo “conduzir operações ciberespaciais militares de espectro total” (HJALMARSSON).

Ainda no mesmo ano, Leon Panetta, então secretário de Defesa dos Estados Unidos, fez um discurso em um evento sobre segurança nacional para empresários, no qual podemos identificar mais um elemento securitizador na fala de alguém do governo. Ele afirmou: “[...] Nós precisamos do Congresso e nós precisamos de todos vocês para nos ajudar nesse esforço. [...] Isso não é apenas uma responsabilidade, é um dever que temos para com as nossas crianças e as crianças das crianças no futuro”. [US DEPARTMENT OF DEFENSE , online]

3. OS VAZAMENTOS DE DADOS DA NSA: EDWARD SNOWDEN

O até então desconhecido Edward Snowden atuava como administrador de sistemas, prestando serviços para a NSA e CIA. Porém conforme a descrição que o próprio Snowden mais tarde confirmou, o trabalho dele era muito mais amplo. Ele era considerado um especialista em tecnologia e cibersegurança.

Em 2013, Edward Snowden trabalhava para a NSA através da empresa Booz Allen Hamilton, em uma instalação da agência no Hawaii. Descontente com o rumo que as agências governamentais estavam seguindo, reuniu ao longo de meses documentos secretos que só pessoas do mais alto escalão da área poderiam ter acesso.

Snowden decidiu sair do emprego e entrar em contato por e-mail criptografado para dois jornalistas investigativos Glenn Greenwald e Laura Poitras, para agendar um encontro, que se deu em Hong Kong. Ele mostrou aos jornalistas documentos classificados de dentro da agência americana que comprovavam a vigilância em massa de não só cidadãos americanos, como de vários outros países.

Esses documentos foram divulgados pelo jornal britânico The Guardian. No dia 21 de Junho, o governo dos Estados Unidos solicitou ao governo da China que o extraditasse. Snowden conseguiu ir para a Rússia, apesar de em seguida ter seu passaporte cancelado e, portanto ficou retido no aeroporto por um mês, quando o governo russo concedeu-lhe asilo de um ano, que vem sendo renovado e hoje tem permissão para viver na Rússia até 2020.

O Departamento de Justiça dos Estados Unidos apresentou acusações contra Snowden alegando violação do Ato de Espionagem de 1917 (em inglês, *Espionage Act of 1917*) e roubo de propriedade do governo.

3.2 OS DOCUMENTOS REVELEVADOS E SEU CONTEÚDO

Um dos documentos revelados por Snowden foi o programa PRISM. Esse programa permite que a comunidade de inteligência americana tenha acesso a nove companhias de tecnologia, o que inclui as informações digitais pertencentes a elas, como e-mails e dados armazenados. Algumas dessas empresas são: Microsoft, Skype, Facebook, Youtube, Yahoo e Apple. Por meio do sistema do programa, é possível coletar voz, texto e vídeos bem como a

localização do alvo em questão, em tempo real. De acordo com o próprio documento, só no mês de abril de 2013, o número de pessoas “alvo” foi de 117,675, mas não informa quantos mais possam ter sido espionados em meses anteriores ou quantos deles são cidadãos americanos.

Outro documento considerado preocupante foi uma ordem judicial secreta dada em abril do mesmo ano, que exige que uma das maiores companhias telefônicas dos Estados Unidos, a Verizon, fornecesse “diariamente” informações à NSA sobre todas as chamadas telefônicas nos sistemas da empresa, sendo elas feitas dentro do país ou não.

O que era surpreendente nessas revelações era o fato de que com o FISA, as ordens judiciais eram direcionadas a um alvo específico, como um suspeito de ser agente de grupo terrorista, por exemplo. No entanto, esses registros eram coletados indiscriminadamente e não dependiam de serem suspeitos de qualquer delito, ou seja, qualquer cidadão americano poderia ser espionado pelo próprio governo. (GUARDIAN, 2013).

Diversos outros documentos foram publicados da mesma forma, com mais informações sobre o método das agências de inteligência americana, em especial, a NSA. Informações sobre como os Estados Unidos conduziram operações de interceptação em estatais brasileiras, como a Petrobras, também foram reveladas [THE GUARDIAN, online].

3.3. O IMPACTO DAS REVELAÇÕES DE EDWARD SNOWDEN

Enquanto a Europa, mais especialmente, a Inglaterra tentou impedir o jornal The Guardian de continuar publicando os documentos, também se descobriu que a agência de escuta telefônica britânica GCHQ realizava a coleta de dados através do PRISM. Já para os países da América do Sul, a indignação demonstrou-se mais presente, sendo feita uma reunião de emergência com os presidentes do Uruguai, Paraguai, Argentina, Venezuela, Suriname, Equador e um representante do Brasil. Os presidentes da Venezuela e da Nicarágua ofereceram a Edward Snowden asilo.

À época, o Google afirmou que não fornece acesso ao governo e que eles estavam indignados pelas tentativas do governo americano em interceptar dados privados da empresa. (AL JAZEERA, 2013).

CONCLUSÃO

O espaço cibernético, apesar de ter nos proporcionado um novo meio de comunicação e até mesmo de viver a vida, também nos traz o questionamento do que é realmente privado nos dias de hoje. Com isso, pode-se dizer que relação entre Estado *versus* indivíduo se estremeceu desde as revelações feitas por Edward Snowden. A população ficou mais alerta em relação à internet. Comunidades e grupos se expandiram para debater sobre a segurança no ciberespaço bem como se criaram redes de apoio a Snowden.

Movimentos que antes se restringiam apenas a acadêmicos e especialistas da área se tornaram conhecidos para um público cada vez maior e disposto a entender como é o processo de espionagem e como se proteger disso. Houve uma clara distinção entre o que os cidadãos esperam de um governo, e o que as grandes empresas e o governo realmente fazem em segredo.

Para este presente artigo, o caso Snowden pode elucidar que apesar de os governos americanos trazerem um discurso securitizador, ou seja, de transformar o ciberespaço como uma ameaça real e de fato, em um primeiro momento o público possa ter aceitado o discurso, na última década, a resistência da população em relação a estes cresceu.

O direito à privacidade ganhou maior importância e a forma de fazer política deve ser repensada a partir disso.

REFERÊNCIAS

ABC NEWS. **Bush calls for tighter cybersecurity.** Disponível em: < https://abcnews.go.com/Technology/story?id=4457451 HYPERLINK "%20https://abcnews.go.com/Technology/story?id=4457451&page=1"& HYPERLINK "%20https://abcnews.go.com/Technology/story?id=4457451&page=1"page=1>. Acesso em: 03 ago. 2018.

AL JAZEERA. **Google 'outraged' over reports NSA acessed data centers.** (2013). Disponível em: <http://america.aljazeera.com/articles/2013/10/31/google-a-outragedaoverreportsthatnsaspiedondatacenters.html>. Acesso em: 10 set. 2018.

BUZAN, Barry. **People, States and Fear**: an Agenda for International Security Studies in the Post-Cold War Era. Boulder. Colorado, Lynne Rienner Publishers, 1991, pp. 3-15.

BUZAN, Barry; WAEVER, Ole. **Security**: a new framework for analysis. London: Lynne Rienner Publisher, 1998.

CYBER TELECOM. **Computer fraud & Abuse Act.** Disponível em: <http://www.cybertelecom.org/security/crime.htm>. Acesso em: 10 set. 2018.

LOPES, Gills. **Reflexos da digitalização da guerra na política internacional do século XXI**: uma análise exploratória da securitização do ciberespaço nos Estados Unidos, Brasil e Canadá / Dissertação para obtenção do grau de mestrado, UFPE, Recife, 2013.

GUEDES DUQUE, Marina. O Papel de Síntese da Escola de Copenhague nos Estudos de Segurança Internacional. In: **Contexto Internacional**, 2009, vol. 31, nº 3, p.466-489.

HJALMARSSON, Ola. **The securitization of cyberspace** – how the web was won. tutor: Christian Fernández, Deparment of Political Science, Lund University, 2013.

OLIVEIRA, Salvattore Bertini Cavalcanti Siqueira Campos de. **A Securitização do Cyber Space e Seus Desdobramentos Para as Relações Internacionais**. Monografia apresentada para obtenção do grau de bacharel. Faculdade ASCES, Caruaru p. 15, 2014

TANNO, Grace (2003) A Contribuição da Escola de Copenhague aos Estudos de Segurança Internacional, vol. 25, nº1, p 50

THE GUARDIAN. **NSA accused of spying on Brazilian oil company Petrobras.** Disponível em: <https://www.theguardian.com/world/2013/sep/09/nsa-spying-brazil-oil-petrobras>. Acesso em: 05 out. 2018.

THE NEW YORK TIMES. **Federal Judge Finds N.S.A. Wiretapes Were Illegal.** 2010.Disponível em: <https://www.nytimes.com/2010/04/01/us/01nsa.html>. Acesso em: 31 ago. 2018.

US DEPARTMENT OF DEFENSE. **News Transcript.** Disponível em: <http://archive.defense.gov/transcripts/transcript.aspx?transcriptid=5136>. Acesso em: 12 set. 2018.

WAEVER, Ole. Securitization and desecuritization. In: LIPSCHUTZ, Ronnie D.(Ed). **On Security**. New York: Columbia University Press, 1995. Disponível em: http://www.ciaonet.org/book/lipschutz13.html. Acesso em 20 de jun. 2018.

WALL STREET JOURNAL. **Taking the Cyberattack Threat Seriously.** Disponível em: <https://www.wsj.com/articles/SB10000872396390444330904577535492693044650>. Acesso em: 08 ago. 2018.

WIKIPEDIA. **Lei de vigilância estrangeira.** Disponível em: < https://pt.wikipedia.org/wiki/Lei_de_Vigil%C3%A2ncia_de_Intelig%C3%AAncia_Estrangeira>. Acesso em: 03 ago. 2018.