ISSN 2447-1097

Direito & TI – Porto Alegre / RS www.direitoeti.com.br

A *CIBERESPIONAGEM* E A PRIVACIDADE SOB O CRIVO DOS DIREITOS HUMANOS

Olívia Martins de Quadros Olmos[1]
Rafaela Bolson Dalla Favera[2]

INTRODUÇÃO

No atual cenário em que se vive, a *Internet* tem ocupado uma posição de destaque no dia a dia da grande maioria da população mundial, além de ser um instrumento muito útil para os governos e para as empresas, no desempenho de suas funções. Mas essa tecnologia nem sempre é utilizada da maneira como deveria, de forma justa, sendo, muitas vezes, empregada para a obtenção de vantagens, como dados ou informações não públicas de outros Estados, de pessoas jurídicas ou de pessoas físicas. Essa prática, que no mundo não virtual é conhecida como espionagem, no *ciberespaço* ganha a denominação de *ciberespionagem*.

Diante disso, este artigo objetiva tratar sobre como a *ciberespionagem* afeta os direitos humanos, levando em consideração o caso Edward Snowden, que revelou ao mundo um esquema de vigilância global promovido pelos Estados Unidos. Tal investigação justifica-se, pois, além de ser um tema atual e relevante, por dizer respeito à relação do Direito com as novas tecnologias da informação e da comunicação, servirá, também, para discutir se a *ciberespionagem* fere o direito fundamental à privacidade dos indivíduos.

Para o desenvolvimento do presente estudo foi utilizado o método de abordagem dedutivo, pois a pesquisa partiu de um enfoque geral de conceituação da *ciberespionagem* para, a partir dessa análise mais ampla, verificar especificamente sua relação com os Direitos Humanos e a violação da privacidade dos indivíduos. Já o método de procedimento empregado foi o monográfico, visto ter sido explorado o caso Edward Snowden para, partindo dele, obter uma dimensão real da ocorrência da

[1] Mestre em Letras pela UFSM, Bacharel em Direito pela UNIFRA e integrante do grupo de pesquisa Núcleo de Direito Informacional – NUDI, da UFSM. oliolmos@yahoo.com.br.
[2] Mestranda em Direito pela UFSM, Bacharel em Direito pela UNIFRA e integrante do grupo de pesquisa Núcleo de Direito Informacional – NUDI, da UFSM). rafaeladallafavera@hotmail.com.

espionagem no ambiente virtual, além de buscar possíveis soluções no sentido de evitar ou cessar essa prática.

No referencial teórico do presente trabalho, foram considerados autores como Silva e Veloso, os quais abordam, respectivamente, a *ciberespionagem* no contexto Português e a global relacionada ao Decreto nº 8.135/2013. Nesse estudo, o autor faz uma avaliação da segurança das informações do governo brasileiro. Além disso, a revista "Em Discussão" (2014), do Senado Federal, que explorou diversos aspectos da espionagem cibernética, foi enfatizada nesse trabalho. Tendo em vista a violação da privacidade dos indivíduos, foram evidenciados o artigo 5º da Constituição Federal e o artigo XII da Declaração Universal dos Direitos Humanos de 1948.

1 A *CIBERESPIONAGEM* E OS DIREITOS HUMANOS: VIOLAÇÃO DA PRIVACIDADE DOS INDIVÍDUOS

A espionagem não é algo novo, muito pelo contrário, existem relatos desta prática na Bíblia[i] e, também, no livro "A arte da guerra", escrito pelo chinês Sunzi, ou Sun Tzu, no século VI a.C. Trata-se de uma obra sobre estratégias militares que contêm, em seu último capítulo, noções sobre o "uso de espião"[ii]. A *ciberespionagem*, por sua vez, surgiu com o advento das novas tecnologias da informação e da comunicação, em especial a *Internet*. Para Silva[iii] "[...] ciberespionagem consiste na apropriação ilícita de informação sensível e secreta por meio informático e dele derivado.".

Desde o surgimento da *Internet*, que se deu no ano de 1969, por intermédio da ARPANET, uma rede de computadores estabelecida pela ARPA, nos Estados Unidos, é que a *ciberespionagem* existe[iv]. Mas foi somente no ano de 2013, com as revelações de Edward Snowden, ex-técnico da *National Security Agency (NSA)*, dos Estados Unidos, que essa prática ganhou repercussão internacional. *Snowden* contou ao mundo que o seu país espiona governos, empresas e pessoas de todos os continentes, inclusive os seus próprios cidadãos, mediante a rede mundial de computadores e interceptações telefônicas[v]. Essa confissão do ex-técnico da *NSA* foi recebida por todos com muita repulsa, inclusive pela presidência do Brasil, que também foi alvo da *ciberespionagem* norte-americana. A Constituição Federal Brasileira assegura a privacidade dos seus indivíduos (art. 5º, inc. X), e também a inviolabilidade e o sigilo das correspondências, das comunicações telegráficas, dos dados e das comunicações telefônicas (art. 5º, inc. XII) em seu rol de direitos e deveres individuais e coletivos. Ademais, consta no artigo XII, da Declaração Universal dos Direitos Humanos de 1948, que "Ninguém será sujeito à interferência em sua vida privada, em sua família, em seu lar ou em sua correspondência, nem a ataque em sua honra e reputação. Todo ser humano tem direito à proteção da lei contra tais interferências ou ataques.".

O fato é que no atual meio em que se vive, a obtenção de informações é algo extremamente valioso, principalmente para os Estados. Não é de se surpreender que os Estados Unidos estejam à frente de qualquer outro país na aquisição de dados que lhe interessem, pois é lá que se encontram situadas a infraestrutura da rede mundial de computadores, como cabos submarinos, *hardwares*, *softwares* etc., e, também, as maiores empresas do ramo, como *Google*, *Facebook* etc.. Por outro lado, no ano de 2012 foi realizada uma pesquisa pela *Security & Defence Agenda (SDA)*, um centro de estudos de Bruxelas, que constatou que nenhum dos vinte e três países analisados possui uma proteção forte contra a *ciberespionagem* ou os *ciberataques*, nem mesmo os Estados Unidos. O país que possui a proteção mais fraca é o México, seguido do Brasil, da Índia e da Romênia[vi].

Após todos esses acontecimentos, o Brasil passou a adotar algumas providências. A primeira delas foi a publicação do Decreto nº 8.135/2013, também conhecido como "decreto do e-mail seguro", que foi instituído com o objetivo de assegurar a proteção das informações derivadas das comunicações eletrônicas da Administração Pública Federal[vii]. Algum tempo depois, entrou em vigor a Lei nº 12.965/2014, intitulada de "Marco Civil da *Internet*", que estabelece princípios, garantias, direitos e deveres para o uso da *Internet* no país. No entanto, as medidas aplicadas até então não são suficientes para combater a *ciberespionagem*, que exige estratégias de proteção mais elaboradas pelos governos de cada Estado, além de uma colaboração internacional.

Na visão de Silva[viii], é preciso criar uma *"ciberbarreira"* contra quatro espécies de ameaças virtuais, quais sejam: *cibercrime*, *ciberespionagem*, *ciberterrorismo* e *ciberguerra*. Primeiro, os funcionários dos governos e das empresas devem ser treinados para saber lidar com os riscos que envolvem a utilização das Tecnologias de Informação (TI). Além disso, é preciso que eles compreendam como proteger os dados dos seus aparelhos, como computadores, *tablets*, *smartphones* etc.. Políticas claras e simples relacionadas à tecnologia devem ser adotadas, além da necessidade de haver um responsável pela segurança. Mas só isso não basta, aconselha-se aos Estados que implantem Centros Nacionais de *Cibersegurança*, capazes de reagir a essas ameaças[ix], e também que cooperem uns com os outros no combate a essas práticas[x].

A questão é saber se os governos e as empresas possuem verbas suficientes para realizar todas essas operações de segurança e se estão capacitados para tanto. Enquanto isso, parece que as pessoas físicas são as mais vulneráveis à *ciberespionagem*, pois o ser humano está cada dia mais exposto na *Internet*, principalmente diante dos *sites* de redes sociais, onde revelam, muitas vezes, informações pessoais. O *site* de relacionamento *Facebook*, que é o mais utilizado mundo, foi citado por Snowden como uma das empresas que fornece informações de seus usuários para a *NSA*, muito embora isso tenha sido negado pelo seu fundador Mark Zuckerberg[xi]. Se essa afirmação for verídica, representa

uma completa afronta à privacidade dos indivíduos, que deve ser repreendida, mas, acima de tudo, combatida.

Essa pesquisa ainda está em andamento, mas com o que foi possível expor no presente trabalho percebe-se que o tema *"ciberespionagem"* pode ensejar inúmeras discussões, principalmente por ser algo pouco explorado pela academia e por não haver uma solução definitiva em curto prazo. Essa temática envolve não só os governos e as empresas, como também as pessoas físicas, que têm a sua privacidade violada no universo virtual. O que se deve continuar fazendo é buscar formas mais elaboradas e capazes de barrar essa ameaça, que continua assombrando todos aqueles que fazem uso das novas tecnologias.

CONCLUSÃO

Diante de todo o exposto, pode-se perceber que com o avanço das novas tecnologias, em especial a *Internet*, fica cada vez mais acirrada a colisão entre o direito à privacidade e a obtenção e o uso de dados e informações coletadas no *ciberespaço*. Milhares de cidadãos, em todo o mundo, estão expostos ao monitoramento de seus passos por programas que espionam tudo o que se escreve, se fala e se disponibiliza no ambiente virtual, o que foi confirmado por Edward Snowden no ano de 2013.

No presente artigo foi possível observar o controle do trânsito de dados e dos conteúdos que circulam pela rede, trazendo riscos ao sigilo de informações de governos e de empresas, e à privacidade dos cidadãos. O ser humano, como ser vulnerável a esses ataques, não possui uma efetiva proteção contra a *ciberespionagem*, muito embora a Declaração Universal dos Direitos Humanos de 1948, em seu artigo XII, assegure a proteção das pessoas contra interferências na vida privada, na família, no lar e na correspondência. No mesmo sentido, se direciona a Constituição Federal brasileira, em seu artigo 5º, ao primar pelo direito fundamental à privacidade dos seus cidadãos.

Para que essa vigilância sem limites não continue ocorrendo, e se possa garantir o efetivo direito à privacidade do ser humano e a proteção de informações governamentais e de empresas, é fundamental uma maior conscientização da importância da definição de ações que levem efetivamente ao aumento da segurança e da confidencialidade dos dados e informações transmitidas pela grande rede. Ainda assim, não é possível afirmar que com a adoção dessas medidas a *ciberespionagem* não mais existirá, pois como visto, a espionagem é algo que sempre existiu, mas a invasão se tornará cada vez mais difícil.

REFERÊNCIAS

BRASIL. **Constituição Federal de 1988.** Vade Mecum Saraiva: OAB e concursos. 4. ed. São Paulo: Saraiva, 2014.

_____. **Declaração universal dos direitos humanos de 1948.** UNIC/Rio, Janeiro de 2009. Disponível em: <http://www.dudh.org.br/wp-content/uploads/2014/12/dudh.pdf>. Acesso em: 03 jul. 2015.

_____. **Marco Civil da Internet.** Vade Mecum Saraiva: OAB e concursos. 4. ed. São Paulo: Saraiva, 2014.

CASTELLS, Manuel. **A galáxia internet:** reflexões sobre internet, negócios e sociedade. 2. ed. Lisboa: Fundação Calouste Gulbenkian, 2007.

ESPIONAGEM cibernética: rede vulnerável. **Revista Em Discussão:** os principais debates do Senado Federal. Ano 5, nº 21, julho de 2014. Disponível em: <http://www12.senado.gov.br/emdiscussao/edicoes/espionagem-cibernetica/@@images/arquivo_pdf/>. Acesso em: 18 ago. 2015.

SILVA, Susana Maria Lopes da. **A ciberespionagem no contexto Português.** 2014. 112p. Dissertação (Mestrado em Guerra da Informação), Academia Militar, Lisboa, Portugal, 2014. Disponível em: <http://comum.rcaap.pt/bitstream/123456789/8750/1/Ciberespionagem%20no%20Contexto%20Portugu%C3%AAs%20Jul%202014%20Susana%20Silva.pdf>. Acesso em: 09 ago. 2015.

SUNZI. **A arte da guerra.** Tradução e edição Adam Sun. São Paulo: Conrad Editora do Brasil, 2006.

VELOSO, Marcelo de Alencar. Ciberespionagem global e o Decreto 8.135: uma avaliação da segurança das informações do governo brasileiro. In: VII CONGRESSO CONSAD DE GESTÃO PÚBLICA, Centro de Convenções Ulysses Guimarães, Brasília – DF, 25 a 27 de março de 2014. Disponível em: <http://pt.slideshare.net/mvsecurity/artigo-consad-2014-ciberespionagem-global-e-o-decreto-8135-uma-avaliao-da-segurana-das-informaes-do-governo-brasileiro>. Acesso em: 19 ago. 2015.

---

[i] SILVA, Susana Maria Lopes da. **A ciberespionagem no contexto Português.** Lisboa: Academia Militar, 2014. p. 2.

[ii] SUNZI. **A arte da guerra.** São Paulo: Conrad Editora do Brasil, 2006. p. 111.

[iii] SILVA, Susana Maria Lopes da. **A ciberespionagem no contexto Português.** Lisboa: Academia Militar, 2014. p. 19.

[iv] CASTELLS, Manuel. **A galáxia internet:** reflexões sobre internet, negócios e sociedade. Lisboa: Fundação Calouste Gulbenkian, 2007. p. 26.

[v] ESPIONAGEM cibernética: rede vulnerável. **Revista Em Discussão:** os principais debates do Senado Federal, 2014.

[vi] ESPIONAGEM cibernética: rede vulnerável. **Revista Em Discussão:** os principais debates do Senado Federal, 2014.

[vii] VELOSO, Marcelo de Alencar. Ciberespionagem global e o Decreto 8.135: uma avaliação da segurança das informações do governo brasileiro. In: VII CONGRESSO CONSAD DE GESTÃO PÚBLICA, Centro de Convenções Ulysses Guimarães, Brasília – DF, 25 a 27 de março de 2014.

[viii] SILVA, Susana Maria Lopes da. **A ciberespionagem no contexto Português.** Lisboa: Academia Militar, 2014. p. 38.

[ix] SILVA, Susana Maria Lopes da. **A ciberespionagem no contexto Português.** Lisboa: Academia Militar, 2014. p. 90.

[x] SILVA, Susana Maria Lopes da. **A ciberespionagem no contexto Português.** Lisboa: Academia Militar, 2014. p. 93.

[xi] ESPIONAGEM cibernética: rede vulnerável. **Revista Em Discussão:** os principais debates do Senado Federal, 2014.