O BRASIL E O REGIME INTERNACIONAL DE SEGURANÇA CIBERNÉTICA: DO CASO SNOWDEN À APROVAÇÃO DA RESOLUÇÃO A/RES/69/166 DA ONU

Alessandra Cristina Mendonça de Morais Matos[1]
Creomar Lima Carvalho de Souza[2]

RESUMO

Este artigo apresenta a versão reduzida da Monografia "O Brasil e o Regime Internacional de Segurança Cibernética: do Caso Snowden à Aprovação da Resolução A/Res/69/166 da ONU". O trabalho aborda a importância da *cyber security* ao analisar iniciativas de arranjo mundial na área digital e discorrer sobre a segurança cibernética brasileira, assim como o seu posicionamento diante dos episódios de ciberespionagem norte-americana contra o país em 2013, divulgada pelo ex-funcionário da NSA, Edward Snowden. O método científico do trabalho é explicativo-descritivo com levantamento bibliográfico, relato da problemática e estudo de caso. Como principais resultados, o Brasil tem priorizado premissas realistas e do conceito tradicional de segurança internacional, podendo ser refletido no Livro Branco de Defesa Nacional (LBDN) de 2012, no qual o setor militar é o que possui maior orçamento (R$ 20,9 bilhões), enquanto o projeto de Defesa Cibernética recebe R$ 3.839,9 milhões. O crescimento dos *cyberattacks* ao Brasil, de .107 incidentes em 1999 para 1.047.031 em 2014 (CERT.br, 2025), expuseram que sua estrutura burocrática ainda não é suficiente para evitar ataques cibernéticos. O caso Snowden evidenciou a ciberespionagem praticada pelos EUA, incluindo o Brasil e até sua empresa estata No âmbito internacional, a defesa cibernética foi securitizada com a Cúpula Mundial sobre a Sociedade da Informação e a Resolução da ONU A/RES/68/167. No Brasil, foi desenvolvido o Expresso V3 como forma de garantir a segurança das comunicações governamentais via *e-mail* e criado o Marco Civil da Internet no Brasil, que estabeleceu direitos e deveres de usuários na Internet.

Palavras-chaves: Segurança cibernética brasileira; Ciberespionagem norte-americana; Soberania nacional; Marco Civil da Internet; Cúpula Mundial Sobre a Sociedade da Informação.

ABSTRACT

This article presents the abridged version of the Monograph "Brazil and the International Cybersecurity Regime: from the Snowden Case to the Approval of UN Resolution A/Res/69/166". The paper addresses the importance of cybersecurity by analyzing global initiatives in the digital area and discussing Brazilian cybersecurity, as well as its position regarding the episodes of US cyberespionage against the country in 2013, disclosed by former NSA employee Edward Snowden. The scientific method of the paper is explanatory-descriptive, with a bibliographical survey, a report on the problem, and a case study. The main results indicate that Brazil has prioritized realistic premises and the traditional concept of international security, which can be reflected in the 2012 National Defense White Paper (LBDN), in which the military sector has the largest budget (R$20.9 billion), while the Cyber Defense

project receives R$839.9 million. The increase in cyberattacks in Brazil, from 3,107 incidents in 1999 to 1,047,031 in 2014 (CERT.br, 2025), has shown that its bureaucratic structure is still not sufficient to prevent cyberattacks. The Snowden case highlighted the cyber espionage practiced by the United States, including Brazil and even its state-owned company. At the international level, cyber defense was securitized with the World Summit on the Information Society and UN Resolution A/RES/68/167. In Brazil, Expresso V3 was developed as a way to guarantee the security of government communications via e-mail and the Brazilian Internet Civil Rights Framework was created, which established the rights and duties of Internet users.

Keywords: Brazilian cybersecurity; US cyberespionage; National sovereignty; Internet Civil Rights Framework; World Summit on the Information Society.

INTRODUÇÃO

A sociedade do conhecimento[3] contribuiu para que a informação se tornasse uma forma de poder difuso[4] para o mundo. Os Estados já não possuem controle pleno sobre tais avanços e informações, e os indivíduos passaram a ter maior participação nesse segmento. Segundo Nye (2011), a política torna-se mais volátil e menos autossuficiente frente a um cenário globalizado, pois a agenda política é ampliada e há o surgimento de novos atores que participam da construção do mundo.

Por ser um poder difuso, a tecnologia contribuiu para o surgimento de problemáticas que acontecem fora do controle dos Estados (Nye, 2011). Com a redução dos custos de comunicação e de disseminação de informações, a política mundial não possui apenas os governos como atores unitários, mas também indivíduos, empresas privadas, terroristas, estão habilitados a desempenhar tais funções.

Consequentemente, os Estados têm menor controle de suas agendas e dividem a governança do sistema internacional com outros atores, os quais executam ações que podem comprometer a segurança dos Estados através de ataques cibernéticos, ou *cyberattacks*[5], aos sistemas de infraestruturas críticas, como elétrico, fornecimento de água, telecomunicações, dentre outros (Nye, 2011).

De acordo com a *International Telecommunication Union (UIT)* (2025)[6], há aproximadamente 67% da população mundial, ou 5,4 bilhões de pessoas, conectadas à Internet. Com a maior oferta de acesso e com o crescente número de usuários, o ciberespaço (*cyberspace* ou *cyberdomain*)[7] se torna uma ameaça aos Estados.

Segundo Barros, Gomes e Freitas (2011), as ações de cunho ofensivo no espaço cibernético podem impactar a segurança nacional. Pelo fato de as informações contidas nesse espaço virtual estarem interligadas, atores podem influenciar ou controlar tais informações e suas infraestruturas. A criação, a modificação e o controle das informações no *cyberspace* constituem o *cyberpower*[8], que vem modificando os domínios de poder e força e pode ser utilizado para obter resultados no ciberespaço ou fora dele por meio do *cyber domain*.

Devido à ausência de controle pleno do espaço cibernético, o Estado precisa se precaver e proteger-se dos *cyberattacks*, pois podem afetar os diversos domínios como, o econômico, político e societal (NYE, 2011).

Segundo o *U.S. Department of Homeland Security*[9] (2013), empresas, governos, militares, instituições financeiras, hospitais e demais entidades, utilizam o espaço cibernético. Essas entidades fazem uso desse espaço com a finalidade de coletar, processar e armazenar informações confidenciais em computadores para transmitir através de redes os dados para outros computadores.

Frente a essa problemática, as ameaças advindas do espaço cibernético aumentam a cada dia dada a grande quantidade de pessoas que possuem acesso às informações. Por esse motivo, observa-se a necessidade da formulação de uma segurança do espaço digital, denominada segurança cibernética (ou

cybersecurity), pois, de acordo com o *U.S. Department of Homeland Security* (2013), os ataques cibernéticos e espionagem digital são a principal ameaça à segurança nacional.

Logo, a *cybersecurity* tornou-se um assunto recorrente nas relações internacionais e de interesse dos Estados por englobar as tecnologias digitais e abordar uma das novas ameaças que surgiram na segurança internacional, os ataques cibernéticos.

Como a grande maioria dos Estados do sistema internacional, o Brasil também deve investir em *cybersecurity*. Levando em consideração a sua vulnerabilidade no espaço cibernético, o Brasil foi alvo de espionagem digital por parte da Agência de Segurança Nacional (*National Security Agency – NSA*, em inglês) dos Estados Unidos da América (EUA), em 2013, fato divulgado pelo ex-funcionário da NSA, Edward Snowden. Por esse motivo, o país passa a ser um objeto de análise relevante para esse trabalho (Greenwald; Kaz; Casado, 2013; Harding, 2014).

Este artigo apresenta a versão reduzida da Monografia "O Brasil e o Regime Internacional de Segurança Cibernética: do Caso Snowden a Aprovação da Resolução A/Res/69/166 da ONU" e tem como objetivo compreender como as ameaças no ciberespaço podem comprometer a soberania de um Estado, a partir da revisão do conceito de segurança cibernética e suas implicações em termos de segurança internacional; revisão dos movimentos de securitização quanto os atos perlocucionários de defesa cibernética; e análise do posicionamento brasileiro acerca do tema a partir de um caso concreto.

O método científico do trabalho é de cunho explicativo-descritivo com levantamento bibliográfico, relato da problemática e estudo de caso. Em relação ao método de abordagem, foi utilizado o hipotético-dedutivo através de pesquisa bibliográfica, como livros e artigos referentes aos conceitos de segurança internacional e cibernética, ciberespionagem e teorias das escolas clássicas de Relações Internacionais. O segundo procedimento técnico de pesquisa utilizado foi a análise prática do assunto, a espionagem digital no Brasil por parte da Agência de Segurança Nacional (NSA) em 2013, divulgado pelo seu ex-funcionário, Edward Snowden. Para subsidiar a análise do caso foram utilizados documentos do governo brasileiro como o Livro Branco de Defesa Nacional e documentos da Secretaria de Assuntos Estratégicos (SAE) e artigos publicados sobre o assunto.

A CIBERESPIONAGEM E A TENTATIVA DE UM REGIME INTERNACIONAL

A ciberespionagem tornou-se uma questão recorrente no sistema internacional e pode ser definida como o uso de ações e operações para obter informações confidenciais, que residem ou transitam por redes ou sistemas computacionais do adversário (Lin, 2010).

O acesso às informações restritas de origem governamental pode ser utilizado como vantagem e apresenta uma ameaça para a soberania estatal, pois diminui o controle do Estado dentro de sua jurisdição territorial, além de comprometer infraestruturas críticas do país.

Ciberataques a infraestruturas críticas de um país são uma séria ameaça que pode ter impactos significativos na sociedade, como a interrupção de serviços essenciais e a instabilidade econômica. Países como os Estados Unidos, Brasil e outros enfrentam um aumento de ciberataques a infraestruturas críticas, incluindo energia, água, telecomunicações e transportes. Na economia, os ciberataques podem causar danos econômicos, como o aumento do custo de produção, a interrupção do comércio e a perda de confiança nos sistemas financeiros. Quanto à segurança nacional, ciberataques podem ser usados para obter informações estratégicas, comprometer sistemas de defesa e causar instabilidade política (Tidy, 2022).

Podemos citar alguns seguintes ciberataques a infraestruturas crítica, como: a) ataque à Colonial Pipeline em 2021, quando a empresa de oleodutos foi vítima de um

ciberataque que interrompeu o fornecimento de combustível para grande parte do país, causando pânico e filas de gasolina nos EUA; b) ataque à estação de tratamento de água em Olds, Flórida, em 2021, no qual hackers comprometeram a estação de tratamento de água de uma pequena cidade na Flórida, aumentando o nível de hidróxido de sódio no tratamento da água, o que poderia ter causado sérios problemas de saúde; e c) ataque WannaCry, em 2017, quando o vírus WannaCry causou grandes transtornos em 150 países, interrompendo serviços de saúde e afetando sistemas de computadores em diversas empresas (Tidy, 2022).

Embora a espionagem não viole nenhuma lei internacional, ela aumenta a insegurança no ciberespaço e faz os países procurarem meios tecnológicos para estender a sua soberania frente ao surgimento crescente de ameaças que compromete a segurança nacional e internacional (Nye, 2011).

Uma forma de reduzir tais ameaças é a construção de regimes internacionais no *cyberspace*. No entanto, essa iniciativa é vista como morosa, dado que os Estados agem de acordo com seus interesses (Jatobá, 2013).

Os regimes internacionais podem ser entendidos como princípios, normas, regras e procedimentos decisórios de tomada de decisões, através do qual as expectativas dos atores em uma determinada área temática são convergentes (Krasner, 2012; Herz; Hoffmann, 2004).

Apesar do crescimento da interdependência e cooperação entre os Estados, interesses particulares podem se sobrepor ao interesse geral, o que torna necessária a construção de normas que delimitam o comportamento dos países. A função mais importante dos arranjos internacionais é estabelecer expectativas recíprocas de comportamentos dos atores envolvidos (Keohane, 1982).

Em sua maioria, a operacionalização resulta na criação de organizações internacionais (OI) com o intuito de implementar os princípios, normas e regras que foram acordadas, além de ser responsável por gerenciar as questões administrativas e financeiras (Levy; Young; Zurn, 1995).

Os Estados não são os únicos atores dos regimes internacionais, os indivíduos e os atores não-estatais também compõem o escopo. Os atores não-estatais colaboram para que novos temas sejam incluídos na agenda internacional. Eles desempenham a função de fazer com que os Estados se atentem para questões específicas, induzindo-os a desenvolver mecanismos institucionais a fim de lidar com elas (Levy; Young; Zurn, 1995). Por esse motivo, os atores não-estatais também participam das delegações nacionais responsáveis pelos regimes internacionais.

A Cúpula Mundial sobre a Sociedade da Informação (CMSI), que ocorreu em 2003 e em 2005, na Suíça e na Tunísia, respectivamente, foi uma tentativa sem sucesso de implementação de medidas de segurança cibernética, em decorrência das divergências entre os Estados quanto às responsabilidades e os compromissos necessários para sua efetiva implementação (Serpro, 2014).

Apesar dos acontecimentos no *cyberspace* impactarem as estruturas de um Estado conforme citado acima, grande parte dos países não têm a percepção de que o espaço cibernético deve ser assegurado. Por esse motivo, a governança desse ambiente é dificultada.

No caso do Brasil, a segurança cibernética era pouco debatida. Somente após o caso de espionagem digital no Brasil, em 2013, divulgado pelo ex-funcionário da NSA, Edward Snowden, que o país passou a olhar para a temática.

O CASO DE ESPIONAGEM DIGITAL DOS ESTADOS UNIDOS DA AMÉRICA (EUA) CONTRA O BRASIL

No dia 06 de julho de 2013, o jornal brasileiro “O Globo”, divulgou o artigo produzido pelo jornalista americano Glenn Greenwald, do jornal inglês *The Guardian*, sobre a ciberespionagem norte-americana. Greenwald

foi procurado por Edward Joseph Snowden[10] por ser um dos jornalistas políticos mais críticos ao governo americano (Greenwald; Kaz; Casado, 2013; Harding, 2014).

Snowden compartilhou arquivos que demonstravam que a Casa Branca "não espionava apenas seus inimigos (criminosos, Al-Qaeda, terroristas, russos) ou mesmo seus supostos aliados (Alemanha, França)" (Harding, 2014, p. 6), mas também as comunicações de milhões de cidadãos norte-americanos e de outros países.

A NSA trabalhava conjuntamente com o *Government Communications Headquarters (GCHQ)*, um serviço de inteligência do Reino Unido. A agência norte-americana financiava atividades de vigilância britânicas e passou a praticar observação eletrônica em massa (Harding, 2014).

Um dos fatos facilitadores de coleta de informações foi o ligamento secreto de interceptadores de dados de fibra ótica submarina feito pela NSA e GCHQ que atravessam o mundo (Harding, 2014). Além disso, os países "convenciam empresas de telecomunicações a entregar seus dados", como *Google*, *Microsoft*, *Facebook* e *a Apple* (Harding, 2014, p. 12).

A espionagem digital norte-americana aumentou devido aos atentados terroristas de 11 de setembro de 2001 às Torres Gêmeas do *World Trade Center*, em Nova York. Mesmo após a divulgação de que os EUA estavam espionando os seus cidadãos em 2005, o Departamento de Justiça e a NSA trabalharam em conjunto para criar uma autorização legal secreta de espionagem nacional (Harding, 2014).

Um elemento jurídico utilizado pelos EUA para obter acesso às informações de seus nacionais e estrangeiros foi a lei *Patriot Act*. É uma lei antiterrorista formulada no governo de George W. Bush após os atentados de 11 de setembro (Exame, 2011). O *Patriot Act* foi instaurado com o intuito de monitorar as pessoas supostamente envolvidas com terrorismo, sem autorização da Justiça (Harding, 2014).

Essa lei legitima a interferência na soberania de outros países, infringindo o Direito Internacional. Cada país possui a sua legislação e as suas normas, dito isso, seria inviável sancionar uma lei interna que também é destinada a outros atores que estão fora do território e competência de um determinado Estado.

Dentre os líderes mundiais estava a então presidente do Brasil, Dilma Rousseff. Apesar dos EUA e o Brasil dispuserem de um bom relacionamento na época, os EUA passaram a investigar mensagens e informações de Dilma e seus assessores (Harding, 2014).

A empresa estatal brasileira de petróleo, a Petrobras, também foi um dos alvos. A empresa é considerada uma das trinta maiores do mundo. Por ser controlada pelo Estado e ter iniciado a exploração de novas áreas de petróleo, a empresa se torna um alvo importante de espionagem externa (Watts, 2013; Harding, 2014).

Em 2012, o Brasil se tornou um dos principais países espionados, ficando somente atrás dos EUA que tiveram, aproximadamente, 2,3 bilhões de telefonemas e mensagens espionadas (Greenwald; Kaz; Casado, 2013).

A Agência de Segurança Nacional dos EUA vem praticando espionagem industrial com fins de obter informações que proporcionem vantagens competitivas comerciais aos EUA. Assim, a coleta de dados ultrapassou o objetivo principal da agência que era a de segurança nacional (Watts, 2013).

Esse fato infringe o Direito Internacional pautado na soberania dos Estados e apresenta uma ameaça para a soberania estatal, causando uma diminuição no controle do Estado dentro de sua jurisdição territorial (Bull, 2002).

OS ATOS PERLOCUCIONÁRIOS NO BRASIL DO SPEECH ACT E OS MOVIMENTOS DE SECURITIZAÇÃO CONTRA A CIBERESPIONAGEM DA NSA: O MARCO CIVIL DA INTERNET E OUTRAS INICIATIVAS

A então presidente do Brasil, Dilma Rousseff, reagiu negativamente à espionagem e considerou o ataque uma violação à soberania do Brasil (Harding, 2014). As relações entre Brasil e EUA sofreram um impacto negativo, resultando no cancelamento da visita oficial da presidente Dilma aos EUA (Monteiro, 2013).

O Brasil anunciou medidas concretas em resposta ao ocorrido, como o plano de construir um cabo submarino[11], ligando a América do Sul à Europa, o que, teoricamente, dificultaria a interceptação de informações brasileiras por terceiros (Harding, 2014). O Brasil possui seis sistemas de cabos de fibra óptica e dentre os seis sistemas, quatro deles fazem conexão com os EUA, facilitando a interceptação de informações (Tozetto, 2013).

Outra proposta do Brasil foi a iniciativa de armazenar dados de usuários brasileiros de empresas de comunicação norte-americanas em servidores locais, ou seja, implementar servidores no Brasil para que não seja mais necessária a passagem de dados por servidores estrangeiros (Tozetto, 2013).

De imediato, o Brasil criou um sistema de e-mail com maior segurança contra interceptação, o Expresso V3, implantado em dezembro de 2013. Utilizado por cerca de quatorze órgãos do governo brasileiro[12], ele visa garantir a inviolabilidade das mensagens oficiais (Brasil, 2014). O Expresso V3 possui recursos de criptografia e ambientes para tráfego e armazenamento próprios do Serpro[13] (Brasil, 2014). Teoricamente, o sistema proporciona segurança no acesso ao e-mail, autenticidade do emissor, integridade e confidencialidade do conteúdo (Brasil, 2014).

Outra medida brasileira foi o projeto de lei do Marco Civil da Internet. O Marco Civil da Internet visa estabelecer direitos e deveres de usuários e empresas na Internet. O projeto trata questões de privacidade, proteção de dados, liberdade de expressão e neutralidade de rede. Foi o primeiro projeto de lei a ser colocado em consulta pública *online* pelo Governo Federal em outubro de 2009 e contou com a contribuição de, aproximadamente, 2.000 contribuições na plataforma (FGV, 2014).

Em 2011, o projeto de lei foi apresentado pelo Brasil na 66ª Assembleia Geral da ONU (Cultura Digital, 2011). O discurso foi proferido no painel "*Internet Access for All*?" e teve como prerrogativa compartilhar com os demais Estados a iniciativa brasileira para a regulamentação da Internet (Cultura Digital, 2011).

Durante o Encontro Global Multissetorial sobre o Futuro da Governança da Internet – NETMundial, realizado em 23 de abril de 2014, a presidente Dilma Rousseff sancionou um Projeto de Lei, que se transformou em uma norma jurídica, a Lei 12.965/2014. A adoção da lei repercutiu positivamente para os demais países do mundo (Araújo, 2014). O projeto foi apresentado no seminário "Liberdade de expressão e o Poder Judiciário", organizado pela Organização das Nações Unidas para a Educação, a Ciência e a Cultura (UNESCO), nos dias 7 e 8 de abril de 2014 (ONU, 2014).

O Marco Civil da Internet preenche a lacuna existente na legislação brasileira quanto à obrigatoriedade e aos prazos de preservação de dados de usuários da Internet registrados pelos provedores, com o propósito de identificar responsáveis pela divulgação de material ofensivo e outras práticas ilícitas na rede (Giacchetta; Freitas; Meneguetti, 2014). A Lei 12.965/2014, estabelece princípios para a regulação da internet no Brasil, sendo os três principais: a neutralidade, a privacidade e a liberdade de expressão (Lourenço, 2014).

Outro aspecto contido na lei é referente ao direito do usuário. Ele terá todos os seus dados pessoais fornecidos ao provedor de aplicações de Internet excluídos ao término da relação entre as partes. O provedor somente poderá fornecer os dados pessoais do usuário a terceiros com seu livre consentimento ou por ordem judicial, e qualquer operação que ocorra em território brasileiro deverá, obrigatoriamente, respeitar a legislação do Brasil (Giacchetta; Freitas; Meneguetti, 2014).

O Marco Civil da Internet no Brasil também apresenta as penalidades caso haja o seu descumprimento, como a aplicabilidade de advertência, suspensão temporária ou a proibição de atividades relacionadas à interceptação de informações de usuários (Giacchetta; Freitas; Meneguetti, 2014).

Tais iniciativas foram importantes para fortalecer a segurança cibernética brasileira. Isso porque o Brasil vinha priorizando premissas realistas e do conceito tradicional de segurança internacional, podendo ser refletidas no LBDN de 2012, no qual o setor militar é o que possui maior orçamento (R$ 20,9 bilhões), enquanto o projeto de Defesa Cibernética recebe somente R$ 839,9 milhões. Importante ressaltar que não foi possível verificar se houve uma priorização ou não dos recursos em defesa cibernética ao longo do tempo, pois não há mais dados disponíveis no Livro Branco de 2020 com esse detalhamento (Brasil, 2012).

Apesar de dispor de uma estrutura burocrática responsável pela sua segurança cibernética, o crescimento dos *cyberattacks* destinados ao Brasil aumentaram de 3.107 incidentes em 1999 para 1.047.031 em 2014, expõe a vulnerabilidade da segurança cibernética brasileira (CERT.br, 2025)[14].

A estrutura de segurança cibernética brasileira é composta pelos seguintes órgãos: Conselho de Defesa Nacional (CDN), órgão de consulta da Presidência da República sobre assuntos de defesa e soberania nacional; Câmara de Relações Exteriores e Defesa Nacional (CREDEN) da Presidência da República; Comitê Gestor de Segurança da Informação (CGSI), que assessora o CDN; Gabinete de Segurança Institucional da Presidência da República (GSIPR), que coordena assuntos estratégicos da segurança, seja de cunho informativo, cibernético ou das infraestruturas críticas do Estado e da sociedade (Barros; Gomes; Freitas, 2011) e o Grupo Técnico de Segurança Cibernética (GT SEG CIBER), que busca propor diretrizes e estratégias de segurança cibernética (Mandarino; Canongia, 2010).

Como a securitização depende de um discurso bem-sucedido, ou seja, da Teoria do *Speech Act* (ato da fala), no qual o discurso é realizado por um ator que se encontra em uma posição de destaque, o tema pode ser securitizado caso o público-alvo ratifique o entendimento de que algo está sendo ameaçado (Buzan; Hansen, 2009). Dessa forma, a securitização é um processo construído socialmente (*securitization move*) e através do *speech act*, que depende da aceitação da população para que um tema seja objeto de segurança (Duque, 2009).

Diante disso, observa-se que o *speech act* do Brasil foi eficiente ao conseguir securitizar o tema e construir medidas emergenciais, como o Expresso V3, o Marco Civil da Internet e a Resolução da ONU A/RES/68/167, com discursos internacionais na ONU e pronunciamentos na mídia brasileira. Por outro lado, a Lei do Marco Civil da Internet somente teve a sua aprovação impulsionada com a divulgação do caso Snowden. Isso porque a discussão da regulação da Internet foi iniciada em 2009, no entanto, o governo brasileiro demorou dois anos para transformar o protejo em lei.

Além de proferir discursos e notas de desaprovação através da mídia internacional e nacional contra a espionagem digital norte-americana, o Brasil também apresentou propostas nos fóruns internacionais, principalmente na Organização das Nações Unidas (ONU), apresentando uma proposta de resolução sobre o tema.

OS MOVIMENTOS DE SECURITIZAÇÃO DO BRASIL NO ÂMBITO INTERNACIONAL: A PROPOSTA BRASILEIRA CONTRA A CIBERESPIONAGEM APROVADA NA ONU

A divulgação de informações que relataram a espionagem digital norte-americana contra diversos países, inclusive o Brasil, gerou indignação por parte de seus governantes (Harding, 2014; Greenwald; Kaz; Casado, 2013).

Na procura por apoio internacional, Dilma informou que acionaria a ONU visando propor

uma nova governança da Internet contra a invasão de privacidade (Frazão, 2013).

No dia 24 de setembro de 2013, a presidente Dilma Rousseff proferiu um discurso de abertura da 68ª Assembleia-Geral das Nações Unidas. Durante a sua fala, Dilma criticou as ações de espionagem dos EUA no Brasil, pois elas feriam o Direito Internacional e os princípios que regem a relação entre os países, além de violar os direitos humanos, as liberdades civis e desrespeitar a soberania nacional (G1, 2013).

O *speech act* da presidente Dilma também destacou o cunho pacífico e democrático do Brasil, descartando qualquer envolvimento com o terrorismo. Por esse motivo, não via razões para espionagens que se fundamentam nessa assertiva (G1, 2013).

Buscando apoio internacional, o Brasil procurou os demais países vítimas e solicitou apoio à ONU na liderança da formulação de regulações para a utilização do espaço cibernético. Em 2 de dezembro de 2013, o país apresentou uma proposta de resolução para proteger a privacidade dos indivíduos no *cyberspace* (CPI da Espionagem, 2013).

A inovadora proposta de resolução objetivava diminuir práticas semelhantes e contou com o apoio da Alemanha, que sofreu com o grampeamento do telefone celular da presidente da Alemanha, Angela Merkel (CPI da Espionagem, 2013). O apoio alemão foi fundamental para que a proposta brasileira avançasse no âmbito da ONU e fosse aprovada em 26 de novembro de 2013.

Em 18 de dezembro de 2013, com a aprovação do projeto, foi publicada a resolução da ONU A/RES/68/167, aprovada por 193 Estados Partes da Organização. A concordância de todos os membros reflete o reconhecimento da comunidade internacional da importância da temática (Correa, 2013).

Em 2014, a resolução A/RES/68/167 da ONU foi atualizada por meio da resolução ONU A/RES/69/166, de 18 de dezembro de 2014, que enfatiza a proteção do direito à privacidade no espaço cibernético e discriminação de qualquer forma de vigilância e coleta de dados das comunicações digitais. Também solicita ao Conselho de Direitos Humanos um mandato especial para analisar o assunto e propor princípios e normas de regulamentação do *cyberspace* (Brasil, 2014; Vallone, 2014).

A A/RES/69/166 também incluiu a segurança de metadados[15] de informações pessoais virtuais. As empresas privadas também foram inseridas no texto, destacando a responsabilidade que cada uma tem de tratar dados pessoais, respeitando, sempre, os direitos humanos (Brasil, 2014).

Apesar das medidas e políticas brasileiras tomadas em relação à espionagem digital norte-americana contra o Brasil, há diversos setores que também necessitam de proteção. Nesse sentido, um dos maiores desafios do Brasil são os crimes cibernéticos que ocorrem no setor financeiro (McAfee, 2014). O setor possui medidas de controle e de proteção de dados que também são deficientes.

CONSIDERAÇÕES FINAIS

Os avanços tecnológicos deram à informação o *status* de poder difuso, influenciando a agenda política global com novos atores, incluindo não-estatais como indivíduos e empresas privadas. Esse poder disperso facilitou o surgimento de desafios, como ataques cibernéticos, que ameaçam a segurança nacional num ambiente que abriga dados críticos financeiros, políticos e de infraestrutura.

Conforme os ataques cibernéticos aumentaram, a necessidade de uma segurança cibernética abrangente ficou clara. Essa segurança visa proteger o espaço digital em todos os setores: econômico, político e social. A questão central é como as ameaças cibernéticas afetam a soberania dos Estados, postulando que a conscientização sobre essas ameaças impulsiona a securitização do tema.

O artigo apresentou o estudo de caso sobre a espionagem digital no Brasil por parte da Agência de Segurança Nacional (NSA) em 2013,

divulgado pelo seu ex-funcionário, Edward Snowden. Revisou conceitos importantes de segurança internacional e cibernética, apresentando a Cúpula Mundial sobre a Sociedade da Informação como uma resposta internacional ao desafio cibernético, realçando o envolvimento de múltiplos atores globais.

Além disso, analisou as consequências no sistema internacional, por exemplo, a formulação do Marco Civil da Internet no Brasil e a aprovação da resolução A/RES/69/166 da ONU. Dentre os principais resultados, identificamos que o Brasil tem priorizado premissas realistas e do conceito tradicional de segurança internacional, podendo ser refletido no LBDN de 2012, no qual o setor militar é o que possui maior orçamento (R$ 20,9 bilhões), enquanto o projeto de Defesa Cibernética recebe somente R$ 839,9 milhões. Importante ressaltar que não foi possível verificar se houve uma priorização ou não dos recursos em defesa cibernética, pois não há mais dados disponíveis no Livro Branco de 2020 com esse detalhamento.

O crescimento dos *cyberattacks* destinados ao Brasil, que aumentaram de 3.107 incidentes em 1999 para 1.047.031 em 2014, segundo dados do CERT.br expuseram que a estrutura burocrática da segurança cibernética brasileira, composta por vários órgãos e grupos de trabalhos, ainda não é suficiente para evitar os ataques cibernéticos. O caso do ex-funcionário da NSA, Edward Snowden, evidenciou a ciberespionagem praticada pelos EUA, incluindo o Brasil e até sua empresa estatal. No âmbito internacional, a defesa cibernética foi incluída na agenda global e securitizado internacionalmente com a Cúpula Mundial sobre a Sociedade da Informação e a Resolução da ONU A/RES/68/167 demonstrou a priorização da proteção do direito à privacidade no espaço cibernético e discriminação de qualquer forma de vigilância e coleta de dados das comunicações digitais.

O Brasil desenvolveu o Expresso V3 com recursos de criptografia e ambientes para tráfego e armazenamento próprios do Serpro para que os servidores do Poder Executivo brasileiro utilizem. Outra medida brasileira foi a criação do Marco Civil da Internet no Brasil, que estabeleceu direitos e deveres de usuários na Internet, tratando questões de privacidade, proteção de dados, liberdade de expressão e neutralidade de rede.

NOTAS

[1]Mestranda em Políticas Públicas pela Universidade Católica de Brasília, Especialista em Análise Política e Políticas Públicas pela Universidade de Brasília (2018) e Bacharela em Relações Internacionais pela Universidade Católica de Brasília (2015). E-mail: alessandra_mmorais@hotmail.com.

[2]Mestre em Relações Internacionais pela Universidade de Brasília. É sócio-fundador da *Dharma Political Risk and Strategy*. Foi por duas vezes bolsista do Departamento de Estado do Governo dos EUA, pesquisador visitante na *University of Florida* em 2010 e observador internacional convidado pela Embaixada dos EUA para acompanhar as eleições presidenciais de 2016. Foi membro do Conselho Deliberativo do Irelgov (*Think Tank* brasileiro de Relações Governamentais), e é membro do Conselho Consultivo do ENRICH in Brazil (iniciativa de inovação da União Europeia com instituições brasileiras) e do Conselho Consultivo da Brazil Foundation.

[3]A sociedade do conhecimento também pode ser entendida como o que Joseph Nye (2011, p. 114) chamou de a "Terceira Revolução Industrial", a qual baseia-se em rápidos avanços tecnológicos em computadores, comunicações e software que, por sua vez levaram a reduções dramáticas no custo de criação, processamento e transmissão e em busca de informações

[4]Poder difuso é aquele exercido por atores não-estatais que encontram-se fora do controle do Estado (Nye, 2011).

[5]Ataques cibernéticos (ou *cyberattacks*) podem ser entendidos como um ato hostil praticado através de computadores, redes ou sistemas, destinados a corromper, interromper ou destruir os sistemas críticos cibernéticos, ativos ou funções de um adversário (Sigalow, 2014).

[6]A UIT é a agência especializada das Nações Unidas para as tecnologias de informação e comunicação - TIC. A organização aloca as órbitas de satélites mundiais e rádio, além de desenvolver as normas técnicas que garantem que as redes e tecnologias estejam interligadas ao objetivo de conectar todas as pessoas do mundo. Disponível em: https://www.itu.int/itu-d/reports/statistics/2023/10/10/ff23-internet-use/. Acesso em: 27/04/2025.

[7]Domínio operacional construído pelo uso de eletrônicos para explorar informações através de sistemas interligados e suas infraestruturas associadas" (Nye, 2011, p. 122, tradução nossa).

[8]Entendido como "a capacidade de obter resultados preferidos através do uso dos recursos de informação eletronicamente interligados do *cyber domain*" (Nye, 2011, p.123, tradução nossa).

[9]O *Department of Homeland Security* é um departamento do gabinete do governo federal dos Estados Unidos da América (EUA) que trabalha para melhorar a segurança interna do país. (UNITED STATES. *Department of Homeland Security*. Disponível em: http://www.usa.gov/directory/federal/department-of-homeland-security.shtml. Acesso em: 11/10/2014.

[10]Snowden trabalhou em empresas privadas subcontratadas, como a Booz Allen Hamilton e a Dell Corporation – da Agência de Segurança Nacional dos Estados Unidos (*National Security Agency - NSA*).

[11] O cabo submarino de fibra ótica foi inaugurado em 2021 e liga o Brasil e Portugal. O EllaLink, como é conhecido, é o primeiro de alta capacidade a ligar os dois países e custou 150 milhões de euros (Silva, 2021).

[12] Dentre eles estão: Secretarias de Administração (vinculada à Secretaria-Geral da Presidência); Micro e Pequena Empresa; Aviação Civil; Promoção da Igualdade Racial; Portos; Políticas para as Mulheres; Secretaria-Geral; Gabinete de Segurança Institucional; Secretarias de Relações Institucionais (SRI), Comunicação Social (Secom), e Assuntos Estratégicos (SAE); Conselho Nacional de Segurança Alimentar e Nutricional (Consea); Secretaria do Conselho de Desenvolvimento Econômico e Social (Sedes); e Vice-Presidência da República (Brasil, 2014).

[13] O Serviço Federal de Processamento de Dados (Serpro) é uma empresa pública de prestação de serviços em tecnologia da informação do Brasil. (Disponível em: https://www.serpro.gov.br/sobre/a-empresa. Acesso em: 12 de novembro de 2014).

[14] O Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT.br) é um Grupo de Resposta a Incidentes de Segurança (CSIRT) de Responsabilidade Nacional de último recurso, mantido pelo NIC.br. O NIC.br é uma entidade civil de direito privado e sem fins lucrativos, encarregada da operação do domínio .br, bem como da distribuição de números IP e do registro de Sistemas Autônomos no País. Conduz ações e projetos que trazem benefícios à infraestrutura da Internet no Brasil e implementa as decisões e os projetos do CGI.br, que é responsável por coordenar e integrar as iniciativas e serviços da Internet no país (CERT.br, 2025).

[15] Os metadados podem ser entendidos como dados que descrevem os dados (Brasil, 2014).

REFERÊNCIAS

ARAUJO, Bruno. **Dilma sanciona o Marco Civil da internet na abertura da NETMundial**. G1, 2014. Disponível em: http://g1.globo.com/tecnologia/noticia/2014/04/netmundial-inicia-com-obrigado-snowden-e-defesa-da-internet-livre.html. Acesso em: 12 mai. 2015.

BARROS, Otávio Santana Rêgo; GOMES, Ulisses de Mesquita; FREITAS, Whitney Lacerda de (Org.). **Desafios estratégicos para segurança e defesa cibernética**. 1ª. ed. Brasília: Secretaria de Assuntos Estratégicos da Presidência da República, 2011.

BAYLIS, John; SMITH, Steve (Ed.). **The Globalization of World Politics**. 2ª. ed. Oxford, 2001.

BRASIL. **Implantação do Expresso V3 contempla seis órgãos**. Portal Brasil, 2014. Disponível em: http://www.brasil.gov.br/governo/2014/03/implantacao-do-expresso-v3-contempla-seis-orgaos. Acesso: 02 mai. 2015.

BRASIL. **Livro Branco de Defesa Nacional, 2012**. Disponível em: http://www.defesa.gov.br/arquivos/2012/mes07/lbdn. pdf. Acesso em: 15 set. 2014.

BRASIL. **Livro Branco de Defesa Nacional, 2020**. Disponível em: https://www.gov.br/defesa/pt-br/arquivos/ajuste-01/estado_e_defesa/livro_branco/Versaodolivroemportugues2020.pdf. Acesso em: 02 mai. 2025.

BRASIL. **ONU adota proposta feita por Brasil e Alemanha para garantir privacidade na internet**. Portal Brasil, 2014. Disponível em: http://www.brasil.gov.br/governo/2014/11/onu-adota-proposta-feita-por-brasil-e-alemanha-para-garantir-privacidade-na-internet. Acesso em: 06 mai. 2015.

BULL, Heddley. **A sociedade anárquica**. Trad. Sérgio Bath. Brasília: Editora Universidade de Brasília, Instituto de Pesquisa de Relações Internacionais; São Paulo: Imprensa Oficial do Estado de São Paulo, 2002.

BUZAN, Barry; HANSEN, Lene. **The Evolution of International Security Studies**. New York: Cambridge University Press, 2009.

CERT.Br. **Sobre o CERT.br. 2025**. Disponível em: https://cert.br/sobre/. Acesso em 27 abr. 2025.

CORREA, Alessandra. **ONU aprova resolução contra espionagem apresentada por Brasil e Alemanha**. BBC, 2013. Disponível em: http://www.bbc.co.uk/portuguese/noticias/2013/12/131218_onu_espionagem_ac. Acesso em: 05 mai. 2015.

CPI DA ESPIONAGEM. **CPI da espionagem: relatório final**. Senado Federal do Brasil, 2013. Disponível em: http://www.senado.leg.br/atividade/materia/getPDF.asp?t=148016&tp=1. Acesso em: 05 mai. 2015.

CULTURA DIGITAL. **A experiência do Marco Civil da Internet foi apresentada na ONU**. Cultura Digital, 2011. Disponível em: http://culturadigital.br/marcocivil/2011/10/22/experiencia-do-marco-civil-da-internet-e-apresentada-na-onu/. Acesso em: 04 mai. 2015.

DUQUE, Marina Guedes. O papel de síntese da escola de Copenhague nos estudos de segurança internacional. **Contexto Int.**, Rio de Janeiro, v. 31, n. 3, Dec. 2009. Disponível em: http://www.scielo.br/scielo.php?script=sci_arttext&pid=S0102-85292009000300003&lng=en&nrm=iso. Acesso em: 15 set. 2014.

EXAME. **Congresso dos EUA prorroga lei antiterrorista Patriot Act**. Exame, 2011. Disponível em: http://exame.abril.com.br/economia/noticias/congresso-dos-eua-prorroga-lei-antiterrorista-patriot-act-2. Acesso em: 29 abr. 2015.

FGV. **Elaborado com apoio da FGV DIREITO RIO, Marco Civil da Internet segue para o Senado**. FGV, 2014. Disponível em: http://direitorio.fgv.br/noticia/elaborado-com-apoio-da-fgv-direito-rio-marco-civil-da-internet-segue-para-o-senado. Acesso em: 04 mai. 2015.

FRAZÃO, Felipe. **Dilma diz que Obama explicará espionagem em 5 dias**. Revista Veja, 2013. Disponível em: http://veja.abril.com.br/noticia/brasil/dilma-diz-que-obama-explicara-espionagem-em-5-dias. Acesso em: 29 abr. 2015.

G1. **Dilma diz na ONU que espionagem fere soberania e direito internacional**. Jornal O Globo, 2013. Disponível em: http://g1.globo.com/mundo/noticia/2013/09/dilma-diz-na-onu-que-espionagem-fere-soberania-e-direito-internacional.html. Acesso em: 30 abr. 2015.

GIACCHETTA, André Zonaro; FREITAS, Ciro Torres; MENEGUETTI, Pamela Gabrielle. **O que muda com a aprovação do Marco Civil da Internet**. Pinheiro Neto Advogados, 2014. Disponível em: http://www.pinheironeto.com.br/arquivos/publicacoes/Anexo%20BI%202.301a.PDF. Acesso em: 04 mai. 2015.

GREENWALD, Glenn. **The NSA's mass and indiscriminate spying on Brazilians**. The Guardian, 2013. Disponível em: http://www.theguardian.com/commentisfree/2013/jul/07/nsa-brazilians-globo-spying. Acesso em: 22 abr. 2015.

KAZ, Roberto; CASADO, José. **EUA espionaram milhões de e-mails e ligações de brasileiros**. O Globo, 2013. Disponível em: http://oglobo.globo.com/mundo/eua-espionaram-milhoes-de-mails-ligacoes-de-brasileiros-8940934#ixzz3Y2hcBWsi. Acesso em: 22 abr. 2015.

HARDING, Luke. **Os arquivos Snowden: a história secreta do homem mais procurado do mundo**. Tradução de Alice Klesck e Bruno Correia. Rio de Janeiro: LeYa, 2014.

HERZ, Mônica; HOFFMANN, Andrea Ribeiro. **Organizações Internacionais: história e práticas**. Rio de Janeiro, Elsevier, 2004.

INTERNATIONAL TELECOMUNICATION UNION. **Global offline population steadily declines to 2.6 billion people in 2023**. Disponível em: https://www.itu.int/itu-d/reports/statistics/2023/10/10/ff23-internet-use/. Acesso em: 27 abr. 2025.

JATOBÁ, Daniel. **Teoria das Relações Internacionais**. São Paulo: Saraiva, 2013.

KEOHANE, Robert O. The Demand for International Regimes. **MIT Press**, International Organization, vol. 36, nº 2, International Regimes, 1982.

KRASNER, Stephen D. Causas estruturais e consequências dos regimes internacionais: regimes como variáveis intervenientes. Tradução de Dalton Guimarães, Feliciano Guimarães e Gustavo Biscaia de Lacerda. **Revista de Sociologia e Política**, vol. 20, nº 42: 93-110 (jun), 2012.

LEVY, Marc A.; YOUNG, Oran R.; ZURN, Michael. **The Study of International Regimes**. European Journal of International Relations, September, 1: 267-330, 1995.

LIN, Herbert S. **Offensive Cyber Operations and the Use of Force**. Journal ofNational Security Law & Policy 4, 2010.

LOURENÇO, Luana. **Dilma sanciona Marco Civil da Internet**. EBC, 2014. Disponível em: http://agenciabrasil.ebc.com.br/politica/noticia/2014-04/dilma-sanciona-marco-civil-da-internet. Acesso em: 12 mai. 2015.

MANDARINO, Raphael Jr. **Um estudo sobre a segurança e a defesa do espaço cibernético brasileiro**. Brasília, 2009.
Strategic and International Studies, Intel Company, 2014a. Disponível em: http://www.mcafee.com/uk/resources/reports/rp-economic-impact-cybercrime2.pdf. Acesso em: 27 abr. 2015.

MONTEIRO, Tânia. **Dilma cancela viagem aos EUA**. Estadão, 2013. Disponível em: http://politica.estadao.com.br/noticias/geral,dilma-cancela-viagem-aos-eua,1075730. Acesso em: 12 mai. 2015.

NYE, Joseph. **The Future of Power**. Washington, DC: PublicAffairs, 2011.

SERPRO. **A Empresa**. Disponível em: https://www.serpro.gov.br/sobre/a-empresa. Acesso em: 12 nov. 2014.

SIGALOW, Martin. **Why Even the Definition of "CyberAttack" Matters**. Open Technology Institute, 2014. Disponível em: http://oti.newamerica.net/blogposts/2014/why_even_the_definition_of_cyber_attack_matters-120120. Acesso em: 26 set. 2014.

TIDY, Joe. **Guerra na Ucrânia: os três ciberataques russos que as potências ocidentais mais temem**. BBC News Brasil. 2022. Disponível em: https://www.bbc.com/portuguese/internacional-60843427#:~:text=A%20for%C3%A7a%20do%20NotPetya&text=Hackers%20norte%2Dcoreanos%20tamb%C3%A9m%20foram,ataque%20parecidos%20um%20m%C3%AAs%20antes.&text=O%20%22worm%22%20(um%20tipo,tamb%C3%A9m%20fizeram%20v%C3%ADtimas%20na%20R%C3%BAssia.%22. Acesso em: 28 abr. 2025.

TOZETTO, Claudia. **Após espionagem dos EUA, Brasil tenta acelerar construção de cabos submarinos**. IG São Paulo, 2013. Disponível em: http://tecnologia.ig.com.br/especial/2013-08-09/apos-espionagem-dos-eua-brasil-tenta-acelerar-construcao-de-cabos-submarinos.html. Acesso em: 02 mai. 2015.

ONU. **Projeto brasileiro de Marco Civil da Internet é modelo internacional, diz relator da ONU**. ONU, 2014. Disponível em: http://www.onu.org.br/projeto-brasileiro-de-marco-civil-da-internet-e-modelo-internacional-diz-relator-da-onu/. Acesso em: 05 mai. 2015.

U.S. **DEPARTMENT OF HOMELAND SECURITY**. Cybersecurity Overvie. 2013.Disponível em: http://www.dhs.gov/cybersecurity-overview. Acesso em: 29 set. 2014.

VALLONE, Giuliana. **ONU aprova resolução proposta por Brasil e Alemanha contra espionagem**. Folha de São Paulo, 2014. Disponível em: http://www1.folha.uol.com.br/mundo/2014/11/1553381-onu-aprova-resolucao-proposta-por-brasil-e-alemanha-contra-espionagem.shtml. Acesso em: 06 mai. 2015.

WATTS, Jonathan. **NSA accused of spying on Brazilian oil company Petrobras**. The Guardian, 2013. Disponível em: http://www.theguardian.com/world/2013/ sep/09/nsa-spying-brazil-oil-petrobras. Acesso em: 22 abr. 2015