O Cosmopolítico

v. 7 n.2 - dezembro de 2020

Beatriz Tenório de Oliveira

Graduanda em Relações Internacionais pela Universidade Federal Fluminense (UFF) e membro do corpo editorial do Cosmopolítico

(IN)SEGURANÇA DIGITAL: O SISTEMA DE CIBERDEFESA BRASILEIRO

Por Beatriz Tenório de Oliveira

1 INTRODUÇÃO

Em um contexto contemporâneo de inovações tecnológicas no Brasil e no mundo, as relações internacionais estão marcadas pela intensa transformação digital que dominou a sociedade, a economia e a política, sobretudo na última década. Nesse panorama, há a emergência do ciberespaço e de sua proteção como importantes pautas nas agendas políticas internacionais, de forma que os países do sistema devem incluir a proteção de dados digitais em seus programas de defesa, de forma a performar sua soberania em um novo contexto digital. Ao se tratar da ciberdefesa brasileira, apesar da formalização de estruturas governamentais para a defesa digital, ainda são visualizados desafios para a concretização de uma organização de cibersegurança de qualidade.

O fenômeno do ciberespaço surge como um importante campo de atuação nas relações internacionais contemporâneas, sendo ele o palco de intensas transformações socioculturais e políticas através da intensificação do fluxo de comunicações e informações. Por essa perspec-

tiva, entende-se que, composto por redes não físicas de uma grande quantidade de dados e informações, o ciberespaço se configura como uma área que apresenta limites não definidos e ultrapassa os conceitos de território e fronteira. Tendo em vista a ampla dimensão do ciberespaço, introduz-se a problemática da cibersegurança como a necessidade da iniciativa governamental para a proteção de dados dos mais diversos setores, em escala doméstica e internacional (LEITE, 2016, p. 4).

Nesse sentido, há diversas categorias e objetivos na prática do cibercrime, nas quais é possível obter, dentre suas dimensões, a "violação da confidencialidade e dados pessoais; burla informática e de telecomunicações; falsidade informática; dano e sabotagem; acesso ilegítimo; ou de autodeterminação" (LEITE, 2016, p. 6). Desse modo, ao atribuir o impasse da responsabilização e a dificuldade na dimensionalização do ciberespaço como agravantes para os crimes digitais, é possível concluir que o baixo risco de detecção dos crimes e de suas origens incentiva os cibercriminosos a praticar seus procedimentos ilícitos (MENDES, 2018, p. 8).

Além disso, deve-se reforçar a necessidade da temática da segurança em um ambiente de interações tecnológicas, diante da constante possibilidade do surgimento de novas ameaças no contexto digital. Logo, visto sua frequente transformação e aprimoramento, se torna primordial o surgimento de uma nova esfera de análise. Nesse entendimento, é pertinente a definição do ciberespaço e de sua emergência como um importante campo para as agendas de relações internacionais entre os Estados (MILITÃO, 2014, p. 46).

Em relação ao enfoque internacional da cibersegurança, é possível ressaltar sua importância perante o alto valor que as informações digitais apresentam ao interesse nacional. Nesse sentido, a realidade dos cibercrimes exige por parte dos Estados medidas de securitização, responsáveis por arquitetar instrumentos protetivos e defensivos para proteger essas informações. Assim, tais medidas de segurança são visualizadas também como uma via que permite a performance dos Estados e sua soberania através de suas missões de segurança e defesa nacional (LEITE, 2016, p. 5-7).

2 O PANORAMA DO CIBERESPAÇO E CIBERDEFESA BRASILEIROS

Ao abordar o ciberespaço do Brasil, é pertinente a consideração de sua

grande dimensão populacional com acesso digital, que, contemplada por um grande aumento na adesão digital durante a última década e originada pela expansão da classe média nacional, se configura como a maior população tanto *online* quanto *offline* da América Latina. Assim sendo, essa configuração inseriu o Brasil em uma posição de grande vulnerabilidade em relação a ameaças cibernéticas. Nesse contexto, o grande fluxo de dados, transações e interações sociais no país viabiliza um amplo leque de ocorrências de crimes digitais, em que se destacam ataques de risco econômico nos âmbitos civil, corporativo e bancário. Além disso, deve-se ressaltar a posição do setor governamental, que é alvo de práticas como a vigilância cibernética e o hacktivismo (DINIZ; MUGGAH; GLENNY, 2014, p. 3-6).

Nessa lógica, referindo-se ao Brasil, é válido apontar dois momentos-chave relacionados a sua segurança digital, que impulsionaram debates e medidas para o arranjo da ciberdefesa visualizada contemporaneamente. Primeiramente, é mencionado o escândalo da espionagem estadunidense ao governo brasileiro em 2013, que demonstrou, na prática, a fragilidade da proteção de dados governamentais do país. Além disso, é compreendida a realização dos grandes eventos internacionais entre 2012 e 2016 - como a Copa do Mundo e as Olimpíadas - como impulsionadores de uma melhor estruturação de defesa cibernética atual, como por exemplo a criação do Centro de Defesa Cibernética (CDCiber) (HUREL; LOBATO, 2018, p. 3).

3 O APARATO MILITAR DE DEFESA CIBERNÉTICA

O sistema de defesa cibernética no Brasil tem como marco de institucionalização a criação da Estratégia Nacional de Defesa (END) em 2008, em que o setor Cibernético – juntamente com os setores Espacial e Nuclear – foi considerado um ponto estratégico para a Política Nacional de Defesa (PND), permitindo assim uma melhor estruturação da proteção e da defesa digital na agenda nacional. Desse modo, o PND oficializou o gerenciamento de segurança da tecnologia da informação na responsabilidade do Exército Brasileiro. Além disso, deve ser mencionada a Doutrina Militar de Defesa Cibernética divulgada em 2014, que define termos técnicos e operacionais da ciberdefesa e define o nível e o setor das tomadas de decisão nesse âmbito em níveis político, estratégico, operacional e tático (FERREIRA apud BRASIL, 2019, p. 2).

Nesse panorama, é pertinente mencionar a criação e a atuação do co-

mando do Exército no CDCiber, o qual foi inaugurado em 2012 e tem por finalidade a coordenação e o monitoramento estratégico da rede cibernética, além da orientação e da capacitação do Sistema Militar de Defesa Cibernética. Em relação a sua atuação, é possível destacar a importância do CDCiber na proteção virtual em eventos internacionais de grande porte ocorridos no Brasil a partir da cobertura e segurança do Rio+20 em 2012. Devido ao sucesso operacional no evento, o CDCiber aprimorou sua técnica ao longo dos anos, atuando também na Copa do Mundo de 2014 e nas Olimpíadas de 2016, em que é salientada a realização de parcerias com a Polícia Federal e a Agência Brasileira de Inteligência (ABIN) (FILHO et al. 2019, p. 10-11).

Assim sendo, Diniz, Muggah e Glenny (2014, p. 4) apontam que a infraestrutura militarmente securitizada do sistema de defesa cibernética do governo brasileiro representa uma redefinição do papel contemporâneo das Forças Armadas, que, através da performance de sua soberania em um contexto não tradicional, são capazes de desempenhar a governança cibernética nacional na intenção de um destaque geopolítico melhor. Todavia, os autores apresentam uma válida crítica ao excesso da militarização cibernética, ao ressaltar o desalinhamento das medidas de securitização ao direcionar seus esforços contra ameaças cibernéticas de maior porte e negligenciar o combate à cibercrimes mais recorrentes contra a população (DINIZ; MUGGAH; GLENNY, 2014, p. 3).

4 SNOWDEN: O CASO DA ESPIONAGEM ESTADUNIDENSE ÀS REDES GOVERNAMENTAIS BRASILEIRAS

Uma vez apresentada a estrutura da ciberdefesa brasileira, cabe expor o notório caso de vazamento dos documentos comprobatórios da espionagem estadunidense ao governo brasileiro durante o mandato de Dilma Rousseff em 2013. Na ocasião, Edward Snowden, ex-contratado como analista de sistemas pela Agência Nacional de Segurança estadunidense (NSA), revelou a vigilância por parte da NSA nas redes de dados brasileiras, incluindo o monitoramento nos sistemas presidenciais e empresariais estatais, como a Petrobrás (FILHO, 2019, p. 2-12). Assim, o caso é considerado um marco para a percepção da vulnerabilidade da cibersegurança brasileira, sendo responsável por uma mudança da percepção e posicionamento internacional brasileiro em relação ao setor (FILHO, 2019, p. 2-12).

Nesse cenário, o impacto do caso Snowden na projeção internacional bra-

sileira é evidenciado pela reação nacional diante da exposição: em um primeiro momento, percebe-se o enfraquecimento das relações entre Estados Unidos e Brasil, conforme visualizado no adiamento da previamente agendada visita oficial de Dilma Rousseff à Washington (BAUMAN et al., 2015, p. 10). Além disso, cabe destacar o discurso de Rousseff na abertura da 68ª Assembleia Geral das Nações Unidas. Logo, salienta-se a fala da ex-presidente, que direcionou o caso da vigilância como uma violação à soberania brasileira e também aos direitos humanos. Desta forma, constata-se a inserção do direito à privacidade na agenda da Comissão de Direitos Humanos na ONU como consequência do posicionamento defensivo das nações vigiadas digitalmente pelos Estados Unidos, em que se destacam o Brasil e a Alemanha como nações mais monitoradas. (BAUMAN et al., 2015, p. 10).

5 O BRASIL E A CONVENÇÃO DE BUDAPESTE

Ainda ao aludir à busca do governo brasileiro por sua ciberdefesa, é válido abordar a não adesão do país à Convenção do Conselho da Europa sobre Crimes Cibernéticos, a Convenção de Budapeste. Criada em 2001, a Convenção simboliza o primeiro e único tratado jurídico internacional que rege a defesa e proteção contra crimes cibernéticos em nível internacional (DINIZ; MUGGAH; GLENNY, 2014, p. 27). Nesse contexto, é possível apontar a crítica do Brasil ao tratado, pautada na acusação de sua redação em excluir de forma deliberada os não-membros da União Europeia (DINIZ; MUGGAH; GLENNY, 2014, p. 27). Nesse sentido, o Brasil buscou como alternativa uma cooperação regional com Estados da América Latina e Caribe, elaborando juntamente com o Escritório das Nações Unidas sobre Drogas e Crime (UNODC) uma convenção internacional sobre crimes cibernéticos, realizada em 2010 em Salvador, no nordeste brasileiro (DINIZ; MUGGAH; GLENNY, 2014, p. 27).

Outrossim, Souza e Pereira (2009, p. 1) afirmam que a adesão do Brasil na Convenção de Budapeste facilitaria uma cooperação mais ampla no combate nacional ao cibercrime. Nessa continuidade, o contato com nações de legislações diferentes, porém que sofrem com as mesmas práticas cibercriminosas, seria benéfica à evolução da proteção do ciberespaço. Nesse panorama, a possibilidade do ingresso brasileiro na Convenção de Budapeste foi retomada no fim de 2019, quando o Itamaraty anunciou o convite para a adesão do Brasil à Convenção por parte do Comitê de Ministros do Conselho da Europa (ITAMA-

RATY, 2019).

Assim, o andamento da adesão brasileira representa um resultado da manifestação mais recente do interesse brasileiro em aprimorar a cooperação jurídica internacional em relação aos cibercrimes. Além disso, ainda que o Brasil esteja no processo da tomada de providências internas necessárias para o ingresso da convenção, o país já apresenta a possibilidade de participar da Convenção na modalidade de observador (ITAMARATY, 2019).

REFERÊNCIAS BIBLIOGRÁFICAS

FILHO et al. **Defesa Cibernética no Brasil: Análise da Atuação do Ministério da Defesa na Copa do Mundo de 2014 e nas Olimpíadas de 2016.** XVI Congresso Acadêmico sobre Defesa Nacional (CADN). Rio de Janeiro, 2019.

ÁVILA, Rafael Oliveira; SILVA, Rafael Pinto da. **Brasil Informacional: A Segurança Cibernética Como Desafio à Segurança Nacional.** XII Encontro Nacional de Pesquisa em Ciência da Informação. Brasília, 2011.

BAUMAN et al. **Após Snowden: Repensando o Impacto da Vigilância.** Revista Eco Pós. v.18, n.2. Rio de Janeiro, 2015.

DINIZ, Gustavo; MUGGAH, Robert; GLENNY, Misha. **Deconstructing Cyber Security in Brazil: Threats and Responses.** Igarapé Institute. Strategic Paper 1. Rio de Janeiro, 2014.

FILHO et al. **Novas Ameaças e a Cibersegurança: Uma Análise do Sistema Brasileiro de Defesa Cibernética Frente ao Caso da Espionagem Durante o Governo Dilma Rousseff.** XVI Congresso Acadêmico sobre Defesa Nacional (CADN). Rio de Janeiro, 2019.

FERREIRA, Raphael Ignácio. **Mudanças na política de defesa cibernética brasileira após o escândalo de espionagem norteamericano.** III Encontro Regional do Sudeste da Associação Brasileira de Estudos de Defesa. Niterói, 2019.

HUREL, Louise Marie; LOBATO, Luisa Cruz. **A Strategy for Cybersecurity Governance in Brazil.** Igarapé Institute. Strategic Note. 2018.

ITAMARATY. **Processo de adesão à Convenção de Budapeste - Nota Conjunta do Ministério das Relações Exteriores e do Ministério da Justiça e Segurança Pública.** 2019. Disponível em: https://www.gov.br/mre/pt-br/canais_atendimento/imprensa/notas-a-imprensa/2019/processo-de-adesao-a-convencao-de-budapeste-nota-conjunta-do-ministerio-das-relacoes-exteriores-e-do-ministerio-da-justica-e-seguranca-publica. Acesso em: 28 out. 2020.

LEITE, Ana Marta Xavier Ferreira. **A Problemática da Cibersegurança e Os Seus Desafios.** CEDIS Working Papers. n.49. Lisboa, 2016.

MENDES, Alexandre Ferreira da Silva. **Desafios da cibersegurança no Brasil entre os anos 2000 e 2017.** Artigo TCC - 2018. Disponível em: https://repositorio.uninter.com/handle/1/265. Acesso em: 27 out. 2020.

MILITÃO, Octávio Pimenta. **Guerra da Informação: a Cibersegurança, a Ciberdefesa e os Novos Desafios Colocados ao Sistema Internacional.** Orientador: Doutora Teresa Maria Ferreira Rodrigues e Tenente-Coronel (Doutor) Paulo Fernando Viegas Nunes. 2014. Dissertação (mestrado) - Mestrado em Ciência Política e Relações Internacionais, Universidade Nova de Lisboa. Lisboa, 2014.

SOUZA, Gills Lopes Macedo; PEREIRA, Dalliana Vilar. **A Convenção de Budapeste e as leis brasileiras.** In: Seminário Cibercrime e Cooperação Penal Internacional. Seminário Cibercrime e Cooperação Penal Internacional, n. 1, 2009.