CASO SNOWDEN: MARCO NORMATIVO DA SOBERANIA DIGITAL

VICTÓRIA DE AQUINO[1]; CHARLES PENNAFORTE[2]

[1] *Universidade Federal do Rio Grande – vwyc.aquinno@gmail.com*
[2]*Universidade Federal de Pelotas – charlespennaforte@ufpel.edu.br*

1. INTRODUÇÃO

Este trabalho integra as atividades do Grupo de Pesquisa CNPq Geopolítica e Mercosul (GeoMercosul) e do Laboratório de Geopolítica, Relações Internacionais e Movimentos Antissistêmicos (LabGRIMA).O presente trabalho propõe uma análise do caso Edward Snowden sob a ênfase nos efeitos geopolíticos e normativos provocados pelo vazamento massivo de informações sigilosas da Agência Nacional de Segurança dos Estados Unidos (NSA). O episódio — que, embora deflagrado em território norte-americano, teve seus desdobramentos mediados por potências como China e Rússia e repercussões diretas sobre Estados-membros da União Europeia e organismos internacionais — exemplifica o declínio e a disfunção na ordem interestatal contemporânea, na qual o próprio Estado hegemônico não consegue controlar ou conter a ação de seus agentes internos.

Do ponto de vista teórico, este estudo se orienta pela Análise do Sistema-Mundo (ASM), em especial, na perspectiva proposta por Immanuel Wallerstein (declínio da hegemonia estadunidense), Arrighi (fim do atual Ciclo Sistêmico de Acumulação de Acumulação liderado pelos EUA) e Pennaforte (surgimento de países de atuação antissistêmica frente ao declínio econômico e geopolítico dos EUA no cenário internacional). A análise é complementada pela Teoria Crítica das Relações Internacionais (1987), ao enfatizar que a crise da hegemonia projeta-se nos espectros normativo, institucional e tecnológico, concomitantemente às dimensões militar e econômica. À luz deste panorama, o ciberespaço passa a integrar o domínio estratégico do conflito sistêmico, abarcando tanto Estados quanto infraestruturas digitais corporativas, cuja operação e proteção encontram-se reguladas por marcos normativos nacionais e internacionais, em especial no âmbito da segurança da informação, soberania digital e responsabilidade civil e penal por danos a ativos críticos.

Observa-se que a transição sistêmica em curso (WALLERSTEIN, 2004) fragiliza a capacidade do centro hegemônico de impor sua racionalidade sobre o sistema internacional. O vazamento realizado por Snowden, ao mesmo tempo em que expõe a hipertrofia da vigilância estatal, transcorrer a incapacidade de o Estado norte-americano controlar os fluxos informacionais que ele próprio gera — um colapso do controle vertical de soberania, deslocado agora para vetores horizontais e transnacionais de poder. A problemática que se impõe é: **como pode um Estado que se pretende hegemônico perder o controle sobre o próprio aparato de inteligência? E, mais ainda, quais as consequências jurídicas quando o crime (vazamento de informações sigilosas) é cometido**

por um nacional, a partir de dados obtidos em solo americano, mas cujos impactos ocorrem em países que não detêm soberania digital plena e que são afetados por decisões de potências terceiras? A partir dessas questões, objetiva-se compreender o caso Snowden como uma marco normativo crítico diante de um sistema-mundo em reorganização digital.

2. METODOLOGIA

Adotou-se metodologia qualitativa baseada em análise crítica documental e bibliográfica, com recorte temporal entre 2013 — ano do vazamento de Edward Snowden — e 2025. Serão examinados fontes primárias constituídas por legislações nacionais e internacionais — notadamente o **Espionage Act de 1917** (EUA), o **Capítulo 28 do Código Penal da Federação Russa** (arts. 272, 273 e 274.1) e a **Lei de Cibersegurança da República Popular da China (2017)**, incluindo sua revisão de 2024 e a **Data Security Law (2021)** —, tratados multilaterais, resoluções do **Conselho de Segurança da Organização das Nações Unidas**, discursos oficiais e relatórios de órgãos governamentais russos e chineses; assim como **fontes secundárias**, compreendendo publicações acadêmicas e relatórios de organizações internacionais especializados em cibersegurança e direito internacional. .

O estudo focaliza especialmente as normativas internacionais surgidas nesse período, como a intensificação dos debates para a criação de normas para o uso de tecnologias cibernéticas em conflitos armados, exemplificados pelo *Tallinn Manual 2.0* (2017), a revisão e ampliação da Convenção de Budapeste sobre Cibercrime, e resoluções do Conselho de Segurança da ONU sobre segurança cibernética.A pesquisa integra abordagens contemporâneas da geopolítica digital e do direito internacional, permitindo desconstruir narrativas oficiais e evidenciar as contradições entre o discurso de segurança nacional e os limites efetivos do controle estatal sobre o ciberespaço. Tal recorte temporal possibilita avaliar o impacto do vazamento Snowden como um catalisador das transformações normativas e da governança global da informação.

3. RESULTADOS E DISCUSSÃO

A pesquisa encontra-se em sua fase inicial. Constata-se que o caso Edward Snowden inaugura uma nova categoria de conflito jurídico-geopolítico, caracterizada pela transnacionalidade dos delitos digitais. A hegemonia dos Estados Unidos é contestada por sua incapacidade estrutural de conter vazamentos internos e controlar o domínio e a soberania informacional que projeta globalmente. O direito internacional clássico, fundamentado na territorialidade e soberania estatal, apresenta-se inadequado para regular infrações cibernéticas cuja autoria, meios e efeitos se dispersam por múltiplas jurisdições. O episódio impulsionou a criação de marcos regulatórios, como o Regulamento Geral de Proteção de Dados (GDPR) da União Europeia, e reacendeu o debate sobre a aplicabilidade da jurisdição universal no ciberespaço.

Edward Snowden constitui o primeiro caso documentado de concessão de abrigo político a hackers estrangeiros pela Federação Russa, tendo obtido residência temporária em 2013, renovada em 2014 e 2017, e cidadania russa em 2022, nos termos do **art. 27 da Lei Federal nº 452-FZ/2013** (sobre imigração e concessão de status de refugiado) e em observância ao **princípio de *non-refoulement***, consagrado no **art. 33 da Convenção de 1951 relativa ao Estatuto dos Refugiados**. A medida decorreu do exercício discricionário da soberania estatal, considerando que Snowden não atentou contra os interesses da Rússia ou de Estados aliados, sendo sua proteção justificada por seu valor informacional e geopolítico, o qual também impulsionou a China a consolidar seu aparato de soberania digital por meio da Lei de Cibersegurança de 2017 e da Lei de Segurança de Dados de 2021. Precedentes correlatos, como o caso de **Yevgeniy Nikulin**, o qual a aplicação do **art. 275 do Código Penal da Federação Russa**, que regula crimes cibernéticos e a proteção de cidadãos frente a pedidos de extradição, consolidaram uma política estatal de salvaguarda de agentes cuja atuação possa contribuir para a segurança e inteligência nacional.

4. CONCLUSÕES

Inicialmente o episódio Snowden parece simbolizar a erosão funcional da soberania estatal na era digital. Não obstante, a urgência de reconfigurar o direito internacional, adaptando-o à lógica reticular e pós-territorial das infraestruturas informacionais. Em um sistema-mundo em transição, a ausência de domínio sobre o fluxo e o controle dos dados traduz a vulnerabilidade da capacidade estatal de manutenção da hegemonia.

5. REFERÊNCIAS BIBLIOGRÁFICAS

PENNAFORTE, Charles. *Análise dos Sistemas-Mundo: uma introdução ao pensamento de Immanuel Wallerstein*. 2. ed. Pelotas: Editora da Universidade Federal de Pelotas, 2023.

PENNAFORTE, Charles Pereira. Movimentos antissistêmicos e relações internacionais: uma perspectiva teórica para compreender o sistema-mundo. Pelotas: Editora da Universidade Federal de Pelotas, 2020.

BRASIL. Espionage Act, 18 U.S.C. §§ 641, 793(d), 798(a)(3). 1917.

RUSSIAN FEDERATION. *Criminal Code of the Russian Federation No. 63-FZ of June 13, 1996 (as amended up to Federal Law No. 18-FZ of March 1, 2012)*. Capítulo 28, Arts. 272, 273 e 274.1. 1996 (alterado em 2025). Moscow: State Duma, 2012. Disponível em: https://www.wipo.int/edocs/lexdocs/laws/en/ru/ru080en.pdf.

CHINA. Cybersecurity Law of the People's Republic of China. 1 jun. 2017. Tradução disponível em: https://digichina.stanford.edu/work/translation-cybersecurity-law-of-the-peoples-re

public-of-china-effective-june-1-2017/.

CHINA. China Data Security Law. 2021. Disponível em: https://www.china-briefing.com/news/china-cybersecurity-law-amendments-2025/.

BLAKE, Matthew C. *The Snowden Effect: The Conflict in a Free Society, Who Values Privacy Versus Who Values Security?* Bemidji, 2015. Disponível em: https://www.bemidjistate.edu/academics/departments/political-science/wp-content/uploads/sites/40/2022/03/Matthew-Blake-Senior-Thesis-2015-b.pdf

SCHMITT, Michael N. (Ed.). *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Cambridge: Cambridge University Press, 2017. Disponível em: https://www.cambridge.org/core/books/tallinn-manual-20-on-the-international-law-applicable-to-cyber-operations/E4FFD83EA790D7C4C3C28FC9CA2FB6C9.

CONSELHO DE SEGURANÇA DA ONU. Resoluções sobre segurança cibernética. Disponível em: https://www.un.org/securitycouncil/.

THE ECONOMIST. Edward Snowden's memoir reveals some (but not all). *The Economist*, 13 set. 2019. Disponível em: https://www.economist.com/culture/2019/09/13/edward-snowdens-memoir-reveals-some-but-not-all.

COX, Robert W. *Production, Power, and World Order: Social Forces in the Making of History*. Columbia University Press, 1987.

INTERNATIONAL TELECOMMUNICATION UNION – ITU. *Global Cybersecurity Index 2020*. Disponível em: https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx.

NORTH ATLANTIC TREATY ORGANIZATION – NATO. *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Cambridge University Press, 2017.

REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL (General Data Protection Regulation – GDPR). 27 April 2016. Disponível em: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679.

UNITED NATIONS. *Security Council Resolutions on Cybersecurity*. Disponível em: https://www.un.org/securitycouncil/content/cybersecurity.

WALLERSTEIN, Immanuel. *The Modern World-System IV: Centrist Liberalism Triumphant, 1789-1914*. University of California Press, 2004.

WORLD ECONOMIC FORUM. *Global Risks Report 2024*. Disponível em: https://www.weforum.org/reports/global-risks-report-2024.