

ESTADO, SOBERANIA DIGITAL E TECNOLOGIAS EMERGENTES: INTERAÇÕES ENTRE DIREITO INTERNACIONAL, SEGURANÇA CIBERNÉTICA E INTELIGÊNCIA ARTIFICIAL

*Fabrcio Bertini Pasquot Polido**

Resumo: Este artigo examina a complexa relação entre a soberania do Estado em matéria digital, compreendendo questões de direito internacional, segurança cibernética e inteligência artificial (IA). Ele busca estabelecer os desafios éticos e práticos enfrentados pelos Estados, como a possível utilização da IA em ataques cibernéticos transfronteiriços, e algumas respostas do direito internacional a essas questões. Igualmente, ele analisa as dificuldades encontradas pelos Estados na tarefa de proteção de seus espaços soberanos no domínio digital, os desafios normativos relacionados à manipulação de dados, à concentração de poder por conglomerados transnacionais de tecnologia e as tensões enfrentadas pelas jurisdições estatais na interface com novas tecnologias, em especial quanto às manifestações do (neo)colonialismo de dados. São destacadas estratégias para fortalecimento da soberania digital, incluindo reformas nos sistemas jurídicos domésticos rumo a quadros normativos sólidos orientados pelo uso ético, responsável e transparente de IA e promoção das bases normativas para segurança cibernética.

Palavras-chave: Soberania digital; Inteligência Artificial; Colonialismo de dados; Cooperação internacional; Ordem transnacional digital.

STATE, DIGITAL SOVEREIGNTY AND EMERGING TECHNOLOGIES: INTERACTIONS BETWEEN INTERNATIONAL LAW, CYBERSECURITY, AND ARTIFICIAL INTELLIGENCE

Abstract: This article examines the complex relationship between state sovereignty and the digital matters, encompassing issues of international law, cybersecurity, and artificial intelligence (AI). It elucidates the ethical and practical challenges faced by states, such as the potential use of AI in cross-border cyber-attacks, and the responses of international law to these issues. "Similarly, it analyses the difficulties encountered by States in the task of protecting their sovereign spaces in the digital realm, the normative challenges related to data manipulation and the concentration of power by transnational technology corporations, and the tensions faced by state jurisdictions at the interface with new technologies, particularly regarding the manifestations of data (neo)colonialism. One could highlight the strategies to strengthen digital sovereignty, including reforms in domestic legal systems towards sound normative frameworks

* Professor Associado de Direito Internacional, Direito Comparado e Novas Tecnologias da Faculdade de Direito da Universidade Federal de Minas Gerais – UFMG, Brasil. Professor do corpo permanente do Programa de Pós-Graduação em Direito e do Programa de Pós-Graduação em Inovação Tecnológica e Propriedade Intelectual da UFMG. Doutor em Direito Internacional (‘summa cum laude’) pela Universidade de São Paulo-USP e Mestre em Direito pela Università degli Studi di Torino/Itália. É Coordenador do Centro de Estudos Jurídicos Transnacionais e Comparados e Grupo de Estudos Internacionais em Propriedade Intelectual, Internet e Inovação – GNet da UFMG. Foi pesquisador visitante – nível Pós-Doutorado – junto ao Instituto Max-Planck de Direito Internacional Privado e Comparado, Hamburgo e Senior Fellow do Instituto Weizenbaum para Sociedade Conectada. Foi Professor Visitante na Kent Law School, Universidade de Buenos Aires e Humbolt-Universität zu Berlin. Atualmente é também Professor Visitante na Universidade de Barcelona -UB, Bolsista de Produtividade do Conselho Nacional de Desenvolvimento Científico e Tecnológico - CNPQ – Nível 2 e e co-fundador da Cátedra PhiloTech – Filosofia da Tecnologia e Direito Digital da UFMG. ORCID: <https://orcid.org/0000-0001-5631-8438>. Contato: fpolido@ufmg.br.

guided by ethical, responsible, and transparent use of AI and the promotion of policies and legal grounds for cybersecurity.

Keywords: Digital sovereignty; Artificial Intelligence; Data colonialism; International cooperation; Digital transnational order.

ESTADO, SOBERANÍA DIGITAL Y TECNOLOGÍAS EMERGENTES: INTERACCIONES ENTRE DERECHO INTERNACIONAL, CIBERSEGURIDAD E INTELIGENCIA ARTIFICIAL

Resumen: Este artículo examina la compleja relación entre la soberanía del Estado en el ámbito digital, abarcando cuestiones de derecho internacional, ciberseguridad e inteligencia artificial (IA). Busca establecer los desafíos éticos y prácticos que enfrentan los Estados, como el posible uso de la IA en ataques cibernéticos transfronterizos, y algunas respuestas del derecho internacional a estas cuestiones. Asimismo, analiza las dificultades que encuentran los Estados en la tarea de proteger sus espacios soberanos en el ámbito digital, los desafíos normativos relacionados con la manipulación de datos y la concentración de poder por parte de conglomerados transnacionales de tecnología, y las tensiones que enfrentan las jurisdicciones estatales en la interfaz con las nuevas tecnologías, especialmente en lo que respecta a las manifestaciones del (neo)colonialismo de datos. Se destacan las estrategias para fortalecer la soberanía digital, incluidas las reformas en los sistemas jurídicos nacionales hacia marcos normativos sólidos orientados al uso ético, responsable y transparente de la IA y la promoción de las bases normativas para la seguridad cibernética.

Palabras clave: Soberanía digital; Inteligencia Artificial; Colonialismo de datos; Cooperación internacional; Orden transnacional digital.

1 Introdução

Os últimos anos testemunharam uma intensa corrida regulatória global em torno de questões normativas envolvendo tecnologias emergentes, em intersecção com estados, organizações internacionais e atores não-estatais relevantes, como ‘lobbies’ e conglomerados da indústria. Operações de plataformas digitais e serviços digitais em escala transfronteiriça, o uso disseminado de Inteligência Artificial (IA), as novas formas de exploração e tokenização de ativos no ambiente digital e os vários acordos de livre comércio de quarta geração - acordos comerciais digitais e ‘deep trade agreements’ - têm forçado o direito internacional a uma revisão de suas políticas, princípios e procedimentos, desde aspectos relacionados ao compartilhamento de soberania dos estados, cooperação internacional e complexidade das fontes normativas até a transformação de mecanismos de solução de controvérsias e neofederalismo de organizações internacionais.

Indiscutivelmente, os eventos, processos e uma ‘ordem transnacional digital’ também sugerem reações clássicas de competição entre atores estatais e suas respostas regulatórias. Elas se manifestam em distintas frentes, como o ‘efeito-Bruxelas’ gerado com a aprovação e entrada em vigor de instrumentos da União Europeia e sua exportação para outros sistemas legais domésticos; a adoção de leis domésticas críticas ou refratárias a tecnologias digitais e modelos de negócios de empresas estrangeiras¹ e até mesmo o recuo a narrativas de soberania adaptadas à grande disputa tecnológica da globalidade. Todos esses eventos revelam a marcha de irreversível controle de legalidade internacional e interna das condutas de atores no ciberespaço – da internet à infosfera que conhecemos – e da expansão de IA em escala industrial para usos civis e comerciais.

O retrato acima descrito parece oferecer a oportunidade de se repensar o papel do Estado na era cibernética, em que as discussões conceituais e normativas de ‘soberania digital’, ‘soberania de dados’, (neo)colonialismo de dados e dimensão transnacional das relações jurídicas baseadas em tecnologias emergentes possam florescer. O debate no direito internacional e nas relações internacionais, por sua vez, não se apresenta como marginal ou ancilar. Ao contrário, ele impõe tracionar o Estado e suas funções regulatórias, adjudicatórias e executivas (ou aplicativas) para dentro da ordem transnacional digital, com potencial de contestar e limitar as formas, expressões e padrões não democráticos e transparentes de formulação normativa e tomada de decisões por agentes não estatais, especialmente como conglomerados de tecnologias e ‘Big Techs’. Por isso, como será examinado adiante, a discussão reflete justamente novas facetas da jurisdição do Estado em matéria digital, suas repercussões sobre o jogo democrático no direito internacional, interdependência dos atores, interoperabilidade entre sistemas ou ordens legais e necessidade de relançamento da cooperação internacional em matéria digital.

¹ A esse respeito, o recente episódio envolvendo Congresso dos Estados Unidos e plataforma Tik Tok exemplifica esse embate. No final de abril de 2024, o presidente Joe Biden promulgou uma lei como parte de um conjunto de medidas para a segurança nacional, determinando que a ByteDance – a empresa que opera a plataforma Tik Tok - fosse obrigada a alienar os ativos relacionados às operações da rede social nos EUA para uma empresa sediada fora da China. Segundo a Lei, caso isso não ocorra dentro de nove meses, a sanção imposta estabelece o banimento do aplicativo das lojas de aplicativos e servidores do país. Em resposta, o TikTok iniciou uma ação judicial contra o governo dos Estados Unidos, questionando a constitucionalidade da lei que impõe a venda compulsória ou o banimento do aplicativo no país. A esse respeito, ver TIKTOK vows legal fight after Biden signs sell-or-ban bill. *Deutsche Welle*, Bonn, 24 de abr. 2024. Disponível: <https://www.dw.com/en/tiktok-vows-legal-fight-after-biden-signs-sell-or-ban-bill/a-68912207>. Acesso em: 14 de mai. 2024. LIMA-STRONG, Cristiano. Biden signs bill that could ban TikTok, a strike years in the making. *The Washington Post*, Washington D.C., 24 de abr. 2024. Disponível em: <https://www.washingtonpost.com/technology/2024/04/23/tiktok-ban-senate-vote-sale-biden/>. Acesso em: 14 mai. 2024. FUNG, Brian. Biden just signed a potential TikTok ban into law. Here’s what happens next. *CNN*, Atlanta, 24 de abr. 2024. Disponível em: <https://edition.cnn.com/2024/04/23/tech/congress-tiktok-ban-what-next/index.html>. Acesso em: 15 de mai. 2024.

Partindo de uma análise teórico-investigativa e legal-comparativa, este artigo propõe examinar como a ‘soberania digital’ do Estado, em sua jurisdição prescritiva, relaciona-se com a proposta de regular e intervir no campo de tecnologias emergentes. São observadas, nesse sentido, as interações entre direito internacional, governança de dados, segurança cibernética e as recentes discussões em inteligência artificial a partir da dimensão regulatória transnacional. O trabalho, desse modo, é estruturado em quatro partes. A primeira discute a complexidade do conceito de soberania digital do Estado e suas possíveis variações à luz da delimitação da jurisdição do Estado em matéria digital. Na segunda parte, são examinadas algumas questões conceituais e normativas de soberania de dados, como a derivação da soberania digital do Estado e do exercício de jurisdição em matéria digital, destacando-se alguns contornos relacionados à desinformação, à segurança cibernética, à manipulação de dados e à concentração de poder por grandes empresas de tecnologia. A terceira parte aborda os desafios enfrentados pelas jurisdições dos Estados no ambiente digital, incluindo questões de soberania, cibersegurança, colonialismo de dados e cooperação internacional diante da emergência e consolidação da inteligência artificial. Igualmente, observa-se a centralidade da soberania de dados e do domínio de infraestruturas de dados para reforçar estruturas e instituições de segurança cibernética e promover o uso responsável, ético e transparente da inteligência artificial. Por fim, a quarta parte discute estratégias para reforçar a soberania digital dos Estados no contexto da cibersegurança e da inteligência artificial, destacando a necessidade de reformas no direito internacional para enfrentar o neocolonialismo de dados e exemplos de reações estatais.

2 Soberania do estado em matéria digital e ordem transnacional digital

Não existe uma definição teoricamente pactuada sobre soberania digital do Estado. Para as vertentes clássicas do direito internacional, a soberania do Estado traduz um poder, uma autoridade sobre sua população, território definido, um governo independente, autônomo que não esteja sob comando de outro estado e a capacidade de interagir, de se relacionar com outros estados². O artigo 1º da Convenção de Montevideu sobre Direitos e Deveres dos Estados de 1933, por sua vez, estabelece a formulação mais amplamente aceita dos critérios de delimitação para a situação jurídica de Estado como pessoa no direito internacional, a saber, reunir os requisitos de: i) população permanente; ii) território determinado; iii) governo; e iv) “capacidade de entrar em relações com os demais Estados”³.

² A esse respeito, cf, SHAW, Malcolm N. *International law*. Cambridge: Cambridge Univ. Press, 2003, p. 178.

³ Incorporada ao direito brasileiro pelo Decreto nº 3.670, de 31 de janeiro de 1939.

A soberania digital do Estado é um atributo somente reconhecido mais recentemente, que passa a descrever aspectos da autoridade, do direito e da capacidade de um ator estatal controlar seus dados, informações e conteúdos digitais. Isso abrange um controle sobre o ambiente digital em que a população ou vida social estão inseridas, incluindo dados pessoais e não pessoais, infraestruturas para funcionamento de redes e plataformas digitais, programas e outros ativos intangíveis, como direitos de propriedade intelectual, tokens digitais etc.

A soberania digital também traduz a autoridade de um Estado e de sua sociedade em controlar aspectos da ‘criatividade e inventividade e de seus dados’⁴. Quando tecnicamente dados pessoais e não pessoais, outrora disponíveis em determinado território, são submetidos a uma operação transfronteiriça de transferência ou compartilhamento de dados para empresas sediadas em um outro Estado, a soberania ‘de origem’ é completamente perdida⁵. Esses dados passam a estar submetidos à jurisdição de outro Estado, no qual a parte receptora esteja sediada, e subordinados a uma nova ordem de poder e de controle, podendo ser compartilhados entre atores estatais e não estatais (e.g. conglomerados de tecnologias).

Dessa forma, se dados são transferidos de titulares de dados pessoais residentes ou de empresas sediadas no Brasil para empresas de tecnologias e/ou autoridades governamentais nos Estados Unidos ou na China, esse conjunto passa a estar submetido a uma nova jurisdição. As leis e regulamentos domésticos de proteção de dados, em geral, preveem essa situação estabelecendo obrigações para controladores e operadores de dados de prestar garantias e salvaguardas de proteção nas operações de transferência de dados. Mas dificilmente essas mesmas leis teriam como obrigar diretamente Estados, pois em respectivamente a suas soberanias ‘digitais’ teriam por exercer poderes distintos nas tarefas de regulamentação (prescrição de comportamentos), adjudicação de litígios e execução/aplicação de decisões envolvendo esses dados. Também na inexistência de tratados e convenções – instrumentos normativos vinculantes do direito internacional – dificilmente esses mesmos Estados estariam obrigados a se comportar ou se abster de determinada conduta relativamente a esses dados.

Um exemplo recente e problemático diz respeito à categoria dos contratos com o Estado, como os acordos celebrados entre a empresa Microsoft e o Tribunal de Justiça do Estado de São Paulo em março de 2019 para o desenvolvimento de Plataforma Digital Eletrônica,

⁴ PELLEGRINI, Jerônimo *et al.* Inteligência local, soberania digital e soberania de dados. In: PENTEADO, Cláudio; PELLEGRINI, Jerônimo; SILVEIRA, Sérgio Amadeu da (org.). *Plataformização, inteligência artificial e soberania de dados: tecnologia no Brasil 2020-2030*. São Paulo: Ação Educativa, 2023. Disponível em: <https://portolivre.fiocruz.br/plataformizacao-inteligencia-artificial-e-soberania-de-dados-tecnologia-no-brasil-2020-2030>. Acesso em: 12 de abr. 2024 (esp. intervenção de Sérgio Amadeu da Silveira, p. 71).

⁵ *Idem.*

envolvendo ainda sistemas de TI, serviços de computação em nuvem e inteligência artificial⁶. À exceção da previsão legal (formal) de que entes públicos possam contratar prestação de serviços que não sejam afetos a suas atividades fim⁷, é evidente que uma análise mais acurada levaria à constatação de que os arranjos privados não podem submeter dados pessoais e não-pessoais de partes brasileiras, no curso da prestação jurisdicional, que é um serviço público e de interesse público, ao completo controle de agentes privados sem as contrapartidas e salvaguardas legais aplicáveis segundo o direito brasileiro. Ainda mais na hipótese, dentre esses casos, de acesso, compartilhamento ou transmissão de dados pessoais sensíveis, relativos a titulares jurisdicionados, para uma empresa de tecnologia sediada no estrangeiro, com propósito de aperfeiçoamento de algoritmos de inteligência artificial, que incluem técnicas de aprendizado profundo, aprendizado de máquina e algoritmos de aprendizado automático⁸.

Não se trata de uma visão ‘nacionalista de dados’ – dentro do trocadilho possível-, mas antes da preocupação, como no caso dos Estados Unidos, a respeito do intenso grau de colaboração nada transparente entre agentes privados e órgãos de segurança nacional (e.g. da Agência de Segurança Nacional – NSA). Há décadas, esses órgãos recebem dados pessoais e não-pessoais para o controle, monitoramento e vigilância tanto no ambiente online quanto presencial de cidadãos no território estadunidense e no estrangeiro⁹.

⁶ O Conselho Nacional de Justiça, por sua vez, expressamente proibiu a entrega desses dados sensíveis e relacionados a processos judiciais para Microsoft no bojo do contrato de prestação de serviços com a Microsoft, porque isso representaria violação de direitos fundamentais, como direito à privacidade, e direitos dos titulares de dados pessoais no Brasil. Estimado em R\$ 1,3 bilhão, o Contrato foi suspenso pela decisão do CNJ, com relatoria do Cons. Márcio Schiefler Fontes, que expressamente afirmou que o contrato “colocar(ia) em risco a segurança e os interesses nacionais do Brasil”. Na sessão do CNJ em 12 de março, além de confirmar a suspensão, o plenário abriu processo de diligência para que as áreas técnicas do conselho possam analisar as informações repassadas pelo TJ-SP sobre o caso.

⁷ No Brasil, cf. art. 2º, inciso VII, e art. 114 da Lei de Licitações e Contratos Administrativos (Lei nº 14.133, de 1º de abril de 2021), relativamente às ‘contratações de tecnologia da informação e de comunicação’ e prazo de vigência máximo de 15 (quinze) anos para contratos que prevejam a operação continuada de “sistemas estruturantes de tecnologia da informação”. Seguindo uma abordagem analítica e crítica, seria possível inferir que a legislação administrativa brasileira vigente parte de tratativa meramente formal entre Estado/Administração e terceiros (contratação pública, o contrato com Estado) e agentes privados que desenvolvam e ofertem serviços de TI e comunicação; da mesma forma, a lei estipula duração das relações jurídicas – prazo contratual em no máximo 15 anos – como patamar bastante problemático e que sugere bases propícias para controle tecnológico a ser exercido por esses agentes, quando eles implementem “sistemas estruturantes de tecnologia da informação” no serviço público e em conexão com a atuação dos entes da Administração Pública.

⁸ SOVEREIGNTY in Cyberspace: Theory and Practice (Version 4.0). *World Internet Conference*, Wuzhen, 16 de jan. 2024. Disponível em: https://subsites.chinadaily.com.cn/wic/2024-01/16/c_956165.htm. Acesso em: 15 de abr. 2024.

⁹ A esse respeito, ver SURVEILLANCE Techniques: How Your Data Becomes Our Data. *Domestic Surveillance Directorate*, [s. l.], 2021. Disponível em: <https://nsa.gov1.info/surveillance/>. Acesso em: 19 de jun. 2024; e TAITZ, Sarah. Five Things to Know About NSA Mass Surveillance and the Coming Fight in Congress. *ACLU*, Nova Iorque, 11 de abr. 2023. Disponível em: <https://www.aclu.org/news/national-security/five-things-to-know-about-nsa-mass-surveillance-and-the-coming-fight-in-congress>. Acesso em: 17 de abr. 2024.

Esses aspectos demonstram que o espaço cibernético, mais amplo que o digital, tornou-se domínio de interesse para as instituições da governança global, segundo a qual estados soberanos permanecem atores-chave na manutenção de uma ordem jurídica transnacional para o ciberespaço, de uma ‘ordem transnacional digital’. Por isso, parece ser determinante que a comunidade internacional persiga objetivos de políticas normativas baseadas no respeito à soberania dos Estados, cooperação em áreas relacionadas à matéria digital (e.g. regulação de plataformas, privacidade e proteção de dados, Inteligência Artificial, aplicação das leis eleitorais no ambiente digital) e pratiquem as mesmas bases de ‘soberania digital’ em consonância com os princípios de consulta igualitária e busca de consenso¹⁰.

O respeito às decisões em matéria digital refletidas na soberania do Estado e no exercício da jurisdição também permite construir instituições e mecanismos voltados para o compartilhamento de poderes entre atores estatais e não-estatais para questões da vida social digital¹¹, elemento indispensável na conformação de uma ordem transnacional digital fundada em normas do direito internacional.

O reconhecimento de que estados mantêm poderes para regular, decidir conflitos e executar decisões em matéria digital, dentro de seus espaços soberanos, não significa isolar ou fragmentar o ciberespaço, mas sim facilitar a existência de uma ordem internacional equitativa baseada em escolhas de política normativa direcionadas para a vida social digital de suas populações. Da mesma forma, existem imperativos de cooperação internacional que servem para lidar com ameaças e desafios no ciberespaço e respeito à soberania dos Estados, como as recentes ameaças de ataques cibernéticos e estratégias de ‘cyber warfare’¹². Nesse sentido, a cooperação internacional em matéria digital permanece como vetor duplo, de um lado a assegurar a conectividade global da internet, as bases para fortalecimento da economia digital

¹⁰ Cf. SOVEREIGNTY in Cyberspace, *cit.*

¹¹ Cf. POLIDO, Fabrício B. P. *Direito Internacional Privado nas Fronteiras do Trabalho e Tecnologias*. 2ª ed. Rio de Janeiro: Lumen Iuris, 2021, p. 36 e ss (com referência aos temas de cooperação, convergência e compartilhamento de competências regulatórias (ou jurisdição prescritiva) no direito internacional, com etapas que explicam o neofederalismo entre organizações internacionais, como exercido atualmente entre as Nações Unidas; União Internacional das Telecomunicações; Organização Mundial da Propriedade Intelectual; UNESCO - Organização das Nações Unidas para a Educação, a Ciência e a Cultura; UNCITRAL - Comissão das Nações Unidas para Direito do Comércio Internacional; Organização para Cooperação Econômica e Desenvolvimento-OCDE; Organização Mundial do Comércio; União Europeia, Conselho para Europa e Câmara de Comércio Internacional.

¹² Cf. SINGER, Peter W.; FRIEDMAN, Allan. *Cybersecurity and Cyberwar: what everyone needs to know*. Oxford: Oxford University Press, 2014, p. 85 e ss. Cyberwarfare pode ser considerada ofensiva digital, o uso de ataques cibernéticos contra um Estado inimigo, causando danos comparáveis aos de uma guerra real e/ou interrompendo sistemas vitais de computador, com resultados pretendidos variados, desde espionagem, sabotagem, propaganda, manipulação até uma guerra econômica. Ataques cibernéticos, por seu turno, podem causar danos físicos, materiais, psíquicos a pessoas, além de danos materiais a objetos. Países como Estados Unidos, o Reino Unido, a Rússia, a China, Israel, o Irã e a Coreia do Norte, por exemplo, apresentam-se como atores dispostos de recursos cibernéticos ativos para operações ofensivas e defensivas.

e, de outro, a contribuir para a construção de um ciberespaço pacífico, seguro e aberto. O ciberespaço cooperativo, por sua vez, é ordenado por meio da cooperação internacional e pelo próprio respeito à soberania no ciberespaço, um pressuposto admitido pela Carta das Nações Unidas dentro do desenvolvimento progressivo do direito internacional no Pós-Segunda Guerra e transporte para as relações internacionais vigentes dentro do próprio espaço cibernético¹³.

3 Soberania digital entre dados e inteligência artificial

Em linha com uma noção mais ampla de soberania digital encontra-se uma derivação técnica, a saber, a expressão ‘soberania de dados’¹⁴. Ela se refere ao poder dos estados de manter o controle sobre estruturas, infraestruturas e instituições dedicadas à proteção de dados, criptografia, segurança da informação, acessos a dados e proteção de informações confidenciais. Esse aspecto demonstra que uma abordagem tradicional da soberania do Estado, centrada em certo controle irresistível de fatos, situações e relações ocorridas em seu território, aperfeiçoa-se a ponto de absorver esses mesmos fatos, situações e relações para o ambiente digital. Eles compreendem desde a infraestrutura da internet, do tráfego de dados entre plataformas digitais até interações entre usuários, consumidores, titulares de dados pessoais e cidadãos localizados em um dado território estatal, mas ocorridas no ciberespaço.

Por isso, a ideia de controle estatal não desaparece, mesmo diante de uma aparente ‘deslocalização’ e do fluxo de dados em escala transfronteiriça, ou da ocorrência de operações transfronteiriças envolvendo dados e transferência desses dados para entes públicos e privados localizados no estrangeiro¹⁵.

¹³ Nesse sentido, cf. entre propósitos das Nações Unidas estabelecidos no art. 1(3) da Carta: “Conseguir uma cooperação internacional para resolver os problemas internacionais de caráter econômico, social, cultural ou humanitário, e para promover e estimular o respeito aos direitos humanos e às liberdades fundamentais para todos, sem distinção de raça, sexo, língua ou religião”; e art. 55 da Carta relativamente à cooperação em matéria econômica, social e cultural, também objetivada para criar “condições de estabilidade e bem estar, necessárias às relações pacíficas e amistosas entre as Nações” a partir da “a solução dos problemas internacionais econômicos, sociais, sanitários e conexos; a cooperação internacional, de caráter cultural e educacional” e o respeito universal e efetivo dos direitos humanos e das liberdades fundamentais para todos, sem distinção de raça, sexo, língua ou religião”.

¹⁴ Para as possíveis delimitações conceituais, dentre outros, ver estudos de BRATTON, Benjamin H. *The stack: On software and sovereignty*. MIT press, 2016; MUELLER, Milton, *Communications and the Internet*. In: COGAN, Jacob Katz; HURD, Ian; JOHNSTONE, Ian (Ed.). *The Oxford handbook of international organizations*. Oxford: Oxford University Press, 2016, p. 535 e ss; e WOODS, Andrew Keane. *Digital Sovereignty + Artificial Intelligence*. In: CHANDER, Anupam; SUN, Haochen (eds). *Data Sovereignty: From the Digital Silk Road to the Return of the State* New York. Oxford: Oxford University Press, 2023, p. 115 e ss.

¹⁵ Esse discurso é repetido em foros internacionais especializados, como na apresentação de Abílio Branco, Head Data Protection SOLA da Thales, durante o Congresso Security Leaders Nacional (2023). MACHADO, Léia; SOUSA, Juliana. Especial security leaders: Soberania de dados além da Segurança. *Security Leaders*, São Paulo, 23 de jan. 2024. Disponível em: <https://securityleaders.com.br/especial-security-leaders-soberania-de-dados-alem-da-seguranca/>. Acesso em: 12 de abr. 2024.

Destituir atores estatais de sua soberania digital, com possível perda de parcelas de jurisdição, é também lançar um dos componentes do Estado – sua população permanente¹⁶ –, à exposição de riscos ou prejuízos concretos, como a apropriação de informações sensíveis (a exemplo do campo da saúde, orientação sexual, afiliação política e religiosa) até a manipulação de dados para influenciar decisões políticas com desinformação, direcionar ataques de ódio e discursos antidemocráticos. Por isso mesmo, a concentração massiva de dados nas mãos de ‘Big Techs’- desde aspectos do exercício da mediação computacional sobre comportamentos até a destituição de dados de cidadãos – traz questões mais críticas sobre soberania digital e violação de direitos fundamentais online¹⁷.

A partir da concentração de poder informacional (vertido em acúmulo de conhecimento tecnológico) por conglomerados de tecnologia e a manifestação desse poder em forma da exploração de produtos, serviços e soluções digitais nos mercados, é possível levantar uma indagação legítima. Em que medida será possível ao Estado exercer algum controle sobre o que é residual da tutela informacional e de dados nas redes digitais? Se, por um lado, existem preocupações quanto à esfera pública informacional e à proteção dos direitos fundamentais online, como liberdades comunicativas e informativas vis-à-vis ingerência mínima do Estado, por outro, a crescente escalada da desinformação, das notícias falsas e dos discursos de ódio, racistas e xenofóbicos permanece na encruzilhada das políticas normativas em matéria digital. De acordo com o Relatório de Riscos Globais de 2024 do Fórum Econômico Mundial¹⁸, a desinformação é uma das grandes ameaças para os próximos dois anos, e parece ter sido, de modo muito cínico, mantida por estratégias sistemáticas levadas a cabo por atores estatais e não estatais, como governos autoritários e populistas, grupos extremistas e mesmo empresas de tecnologia¹⁹.

¹⁶ Em referência à clássica menção ao artigo 1º da Convenção de Montevidéu sobre Direitos e Deveres dos Estados de 1933 (nota 3 supra).

¹⁷ Nesse sentido, ver ZUBOFF, Shoshana. We make them dance: surveillance capitalism, the rise of instrumentarian power, and the threat to human rights. In: JØRGENSEN, Rikke Frank (ed.) *Human Rights in the Age of Platforms*. Cambridge: MIT Press, 2019, p. 3-51. Disponível em: <https://direct.mit.edu/books/oa-edited-volume/4531/Human-Rights-in-the-Age-of-Platforms>. Acesso: 14 de mai. 2024.

¹⁸ WORLD ECONOMIC FORUM. The Global Risk Report 2024. Cologny/Genebra: World Economic Forum, 2024. Disponível em: https://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2024.pdf. Acesso em: 19 de jun. 2024.

¹⁹ Podem ser mencionados dois episódios marcantes no caso de conglomerados de tecnologias como também vetores de desinformação, sensacionalismo e notícias falsas. O primeiro diz respeito às ofensivas críticas das ‘Big Techs’ ao PL 2630/2020, que instituiu a Lei Brasileira de Liberdade, Responsabilidade e Transparência na Internet. Em maio de 2023, por exemplo, o Google fixou em sua página oficial um link com uma mensagem dizendo que “o PL das Fake News pode aumentar a confusão sobre o que é verdade ou mentira no Brasil”. Ao clicar, o usuário era remetido a um texto de um diretor de relações governamentais e políticas públicas da empresa, com críticas ao projeto. Outro episódio marcante é o embate entre o empresário Elon Musk, controlador da plataforma X (ex-Twitter) e o Ministro Alexandre de Moraes, do Supremo Tribunal Federal, em abril de 2024, sobre o bloqueio de contas ligadas à disseminação de desinformação e ataques à democracia no Brasil na plataforma digital “X”.

Na esteira de novas aplicações de IA e técnicas promovendo comportamentos inautênticos nas redes sociais, a disseminação de conteúdo desinformativo passa a compor o conjunto dos riscos prementes para pleitos eleitorais ao redor do globo. Não sem surpresa, eles afetam a legitimidade do processo eleitoral, desestabilizam novos governos e, invariavelmente, desafiam a soberania dos Estados em matéria digital.

A soberania de dados também diz respeito ao poder do Estado de definir os melhores padrões de infraestrutura de dados, sem que eles permaneçam exclusivamente limitados às decisões de atores não estatais, como decisões corporativas de conglomerados de tecnologia, organizações da indústria ou associações privadas. Isso porque toda a infraestrutura de redes, servidores, sistemas de armazenamento e protocolos que facilitam a coleta, processamento, armazenamento e transferência de dados, forma a base para exercer tecnicamente o controle sobre os dados, seu tráfego e sobre o funcionamento de sistemas digitais. Uma infraestrutura de dados robusta e segura passa a ser essencial para objetivos sistêmicos de proteção contra ameaças cibernéticas e garantir a conformidade com as leis de proteção de dados e privacidade, objeto igualmente de atribuições regulatórias e fiscalizatórias de órgãos estatais, como autoridades nacionais de proteção de dados e segurança cibernética²⁰. A capacidade de um Estado de estabelecer suas próprias regulamentações e padrões para o tratamento de dados depende, pois, do domínio técnico e normativo sobre a sua própria infraestrutura de dados, mais um indicativo de como a jurisdição do Estado nesse campo será exercida.

Em alguma medida, o reconhecimento desse poder de regular ou decidir sobre questões de infraestrutura de dados afetará não apenas certos aspectos relativos à segurança e à integridade de bases de dados e sistemas informacionais localizados e operantes em um dado território, mas também a capacidade do próprio Estado de participar como um ator relevante na

Moraes determinou que Musk fosse incluído como investigado e instaurou um inquérito sobre suas condutas. Isso gerou debates sobre liberdade de expressão versus regulação das redes sociais, com implicações para o cenário político e eleitoral brasileiro. A esse respeito: ELON Musk is feuding with Brazil's powerful Supreme Court. *The Economist*, Londres, 14 de abr. 2024. Disponível: <https://www.economist.com/the-americas/2024/04/14/elon-musk-is-feuding-with-brazils-powerful-supreme-court>. Acesso: 14 de mai. 2024.

²⁰ No direito brasileiro, por exemplo, a jurisdição do Estado em matéria de dados, como componente da matéria digital, é exercida em parte pela Autoridade Nacional de Proteção de Dados, a quem compete “zelar, implementar e fiscalizar o cumprimento” da LGPD em todo o território nacional (art. 5º, inciso XIX, LGPD, sobre a própria definição da autoridade). Ao instituir a Política Nacional de Cibersegurança e o Comitê Nacional de Cibersegurança (PNCiber), o recente Decreto nº 11.856, de 26 de dezembro de 2023, considerou a finalidade de orientar a atividade de segurança cibernética no País, “tendo como um de seus princípios a soberania nacional”, mas optou por ressaltar a necessidade de uma abordagem específica e especializada, distinta das funções da ANPD, sem atribuir-lhe uma função direta, o que pode ser observado criticamente. Ao revés, o Decreto cria o Comitê Nacional de Cibersegurança - CNCiber, no âmbito da Câmara de Relações Exteriores e Defesa Nacional do Conselho de Governo, com propósito de acompanhar a implementação e a evolução da PNCiber, deslocando a atuação em segurança cibernética para outra esfera do Executivo e da Administração Pública Federal brasileira, diferentemente da opção de concentrar essas tarefas nas mãos da ANPD.

economia digital global. Essa participação lastreada na afirmação de soberania digital ocorre como uma forma segura e eficaz, de modo a reforçar os vetores de desenvolvimento socioeconômico das instituições daquele Estado e alavancar sua posição no cenário internacional como agente ativo no regime internacional de proteção de dados²¹.

Participar de modo equitativo e soberano nesse regime faz com que um Estado não se submeta a qualquer forma de controle externo, ingerência ostensiva em seus assuntos internos em matéria digital ou a formas expropriatórias e (neo)colonizadoras envolvendo dados²². O neocolonialismo de dados, por sua vez, é observado na medida em que um Estado é, em teoria, independente e apresenta todos os traços exteriores de soberania nas relações internacionais (como propugnado, por exemplo, pelo art. 4º da Constituição brasileira), no entanto, em realidade, seus sistemas econômico, político e social são dirigidos a partir do exterior. Segundo essa abordagem, a atual construção de regimes de cooperação internacional em matéria de dados e fluxos de dados, também a partir de foros internacionais relevantes (e.g. OCDE, UNESCO, OMPI) não afastariam o poder de Estados coloniais e de conglomerados de tecnologias neles sediados de interferir sobre decisões a serem tomadas por países em desenvolvimento (anteriormente colonizados e descolonizados), também forçados a aceitar certas contrapartidas no campo de proteção de dados e, mais recentemente, em inteligência artificial²³.

Por fim, como um desdobramento da jurisdição em matéria digital, discute-se a medida de reconhecimento do poder soberano do Estado de agir e intervir sobre o campo regulatório de inteligência artificial. De fato, regiões distintas do globo apresentarão diferentes níveis de expressão desse poder. Belli chama atenção, por exemplo, para oito elementos fundamentais (também chamados de "KASE" - 'Key AI Sovereignty Enablers'), que devem ser priorizados para a construção de estruturas de governança de IA por parte de Estados representativos do Sul Global²⁴. Esses elementos incluem: (i) governança de dados, (ii) governança algorítmica, (iii) capacidade computacional, (iv) conectividade significativa, (v)

²¹ Cf. Intervenção oral de CAMPAGNUCCI, Fernanda: Devemos apostar em tecnologias livres diante das infraestruturas de IA. In: PENTEADO; PELLEGRINI; SILVEIRA (org.), *Plataformização, inteligência artificial e soberania de dados*, cit., p. 107.

²² A esse respeito, ver também GAGLIARDONE, Iginio. A Postcolonial Perspective on Digital Sovereignty. In: FELDSTEIN, Steven (eds.). *New Digital Dilemmas: Resisting Autocrats, Navigating Geopolitics, Confronting Platforms*. Washington, DC: Carnegie Endowment for International Peace, 2023, p. 23-26.

²³ A expressão neocolonialismo de dados é aqui adaptada da leitura crítica feita por Francis Kwame Nkrumah (1909-1972), líder e teórico político ganhês sobre as tessituras do neocolonialismo. Ver Neo-Colonialism and Nkrumah: Recovering a Critical Concept. In: LANGAN, Mark. *Neo-Colonialism and the Poverty of 'Development in Africa*. Cham: Springer/Palgrave, 2018, p. 1-32.

²⁴ BELLI, Luca. To Get Its AI Foothold, Brazil Needs to Apply the Key AI Sovereignty Enablers (KASE). In: FELDSTEIN, *New Digital Dilemmas*, cit., p. 27 ss.

energia elétrica confiável, (vi) alfabetização digital da população, (vii) segurança cibernética robusta e um (viii) arcabouço regulatório apropriado. A junção desses elementos, ainda na visão de Belli, seriam cruciais para garantir não apenas o crescimento econômico e a justiça social, mas também para afirmar a soberania em IA e evitar qualquer forma de dependência excessiva de sistemas de IA estrangeiros que poderiam transformar um Estado em uma colônia digital²⁵.

A situação de países e organizações internacionais que atualmente se voltam para leis e regulamentos de Inteligência Artificial, como Estados Unidos²⁶, China²⁷, Brasil²⁸ e União Europeia²⁹ demonstra diferentes graus de percepção sobre como aproveitar os desdobramentos da jurisdição do Estado em matéria de IA. Aqueles que já avançaram em bases de governança de dados (no caso de estados que recorrem à aplicação de suas leis domésticas de proteção de dados e ao fortalecimento de suas autoridades nacionais) podem ainda passar por desafios em termos de segurança cibernética, implementação e usos de aplicações de IA e capacidade computacional.

Nesse sentido, a União Europeia, mais uma vez para além das possíveis críticas ao “efeito Bruxelas”, talvez seja o único ator a reunir o conjunto de determinantes a fortalecer as bases de soberania compartilhada em IA. Elas, por forças reversas, não são representam qualquer poder de deter (ou dispor de) capital informacional e tecnológico sobre o desenvolvimento de sistemas e aplicações de IA, como seria a disputa real entre China e Estados Unidos. Antes, instituições da UE têm buscado consolidar um poder técnico e conhecimentos legislativos capazes de submeter o uso e implantação de sistemas de IA a padrões robustos de proteção de usuários e cidadãos e referentes às liberdades fundamentais, como ressaltadas nas

²⁵ *Ibidem*, p. 29 e ss (destacando ainda interconexão entre os oito elementos e a proposta da construção de uma “pilha de soberania em IA” para facilitar a cooperação entre diferentes setores e aumentar a autonomia do país).

²⁶ Nos EUA, a regulamentação de IA tem ocorrido por meio de uma abordagem fragmentada entre os estados. Em 2022, 15 estados e localidades propuseram ou aprovaram legislações relativa à IA. Em nível nacional, em 2022, foi promulgado o documento ‘Blueprint for an AI Bill of Rights’, conjunto de diretrizes para o design e uso responsável da inteligência artificial, criado pelo Escritório de Política Científica e Tecnológica da Casa Branca (OSTP) em meio a um esforço global contínuo para estabelecer mais regulamentações para governar a IA. Mais recentemente, em 2023, o presidente americano Joe Biden assinou uma Ordem Executiva que estabelece regulamentações para o uso e desenvolvimento de inteligência artificial no país.

²⁷ Em março de 2022, a China aprovou um regulamento que rege o uso de algoritmos pelas empresas em sistemas de recomendação on-line e, em 2023, o publicou novas regras para inteligência artificial generativa.

²⁸ No Brasil, desde 2019, têm surgido na Câmara dos Deputados diversos projetos de lei buscando regulamentar a IA. Destaca-se o Projeto de Lei nº 21/2020, que estabelece o Marco Legal de Inteligência Artificial. Após aprovação na Câmara, o Senado Federal criou uma Comissão de Juristas para elaborar um projeto substitutivo. O resultado é o atual PL nº 2338/2023, atualmente em tramitação no Senado Federal. Este segue tendências internacionais, como instrumentos da UNESCO e OCDE, e Regulamento de IA da UE, visando um uso responsável da IA, para proteger direitos fundamentais e promover sistemas seguros e confiáveis.

²⁹ O Parlamento Europeu aprovou, em 13 de março de 2024, o Regulamento de Inteligência Artificial (‘AI Act’), que passa a ser um dos mais relevantes instrumentos normativos de inteligência artificial em escala global, e que define regras para desenvolvedores e usuários o uso de Inteligência Artificial baseada no risco no domínio da União Europeia.

justificativas do Regulamento Europeu de Inteligência Artificial³⁰. Por essa razão, como objetivo de política normativa, o Regulamento de IA articula obrigações legais uniformes para agentes econômicos nos Estado Membros da UE relativas à oferta, colocação em serviço e utilização de determinados sistemas de IA – igualmente comprometido com a premissa de que esses sistemas possam se beneficiar “do princípio de livre circulação dos produtos e dos serviços” no mercado interno europeu³¹.

Inexoravelmente, poder técnico e conhecimento legislativo, como os hoje concebidos pela União Europeia, serão dois componentes também relevantes para o exercício do poder jurisdicional do Estado e seus órgãos internos sobre IA, em especial quando levados adiante para um objetivo mais amplo de política internacional. Ele refere-se ao poder dos Estados de buscar contestar a influência geopolítica de outros atores estatais e não-estatais, como China, Estados Unidos e as ‘Big Techs’ e suas corridas tecnológicas assimetricamente desenfreadas.

4 Desafios para a jurisdição do Estado no ambiente digital

As reflexões anteriores buscaram indicar algumas possíveis abordagens para a jurisdição do Estado em matéria digital, recuperando as noções de ‘soberania digital’. Por mais discutível que possa parecer a apropriação do termo pelo espaço cibernético e o ‘digital’ como elemento qualificador, soberania e autonomia estratégica dos Estados são colocadas em risco na atualidade. Elas sofrem constrições e ameaças por um conjunto de forças, desde as crescentes tensões e conflitos internacionais (e.g. guerras entre Rússia e Ucrânia, Israel e Hamas, disputas entre Estados Unidos e China no campo comercial e tecnológico) e emprego de novas tecnologias beligerantes até o recurso a inovações profundas, levando ao considerável crescimento de incidentes e ataques de cibersegurança direcionados a governos, empresas e organizações em escala transnacional.

Se a soberania permanece como tradicional atributo da estatalidade e é expressa na jurisdição do Estado, parece ser evidente que os desafios postos dependem também de medidas de reação por parte de governos e organizações, como será examinado mais adiante. A

³⁰ PARLAMENTO EUROPEU. Regulamento (UE) 2024/206 do Parlamento Europeu e do Conselho, adotado em 13 de março de 2024 estabelecendo regras harmonizadas sobre inteligência artificial (‘Artificial Intelligence Act’) e alterando certos atos legislativos da União, Jornal Oficial da União Europeia, Estrasburgo: Parlamento Europeu, 2024. Disponível em: https://www.europarl.europa.eu/doceo/document/TA-9-2024-0138-FNL-COR01_PT.pdf. Acesso em: 19 de jun. 2024. (com referência à primeira parte do considerando 8 do Regulamento: “(...) é necessário adotar um regime jurídico da União que estabeleça regras harmonizadas em matéria de IA para promover o desenvolvimento, a utilização e a adoção da IA no mercado interno e que, ao mesmo tempo, proporcione um nível elevado de proteção de interesses públicos, como a saúde e a segurança e a defesa dos direitos fundamentais, incluindo a democracia, o Estado de direito e a proteção do ambiente, conforme reconhecido e protegido pelo direito da União”).

³¹ Cf. Regulamento de IA, *cit.* (versão corrigida em 24.04.2024).

combinação, por exemplo, entre IA e cibersegurança está na vanguarda dessas medidas, contudo ainda levanta muitas questões e dilemas éticos³². Além de potenciais violações a direitos fundamentais de cidadãos no território de um Estado, diferentemente daquele da origem ou sede do desenvolvedor, alguns desafios próprios aos estágios de desenvolvimento e uso descontrolados de IA podem ser identificados em linha com as observações críticas de Timmers:

i. Risco de perda de controle e autonomia pelo uso extensivo de IA na gestão de riscos cibernéticos: a frequente opacidade das decisões tomadas por sistemas de IA pode resultar em uma falsa sensação de segurança e minar a capacidade das pessoas de tomar decisões informadas, algo extremamente sensível em contextos democráticos, como a desinformação gerada para prejudicar sistemas eleitorais.

ii. Responsabilidade e confiança: qualquer eventual confiança cega na capacidade produtiva e gerativa sistemas de IA pode levar a uma alocação injusta de responsabilidade em caso de incidentes cibernéticos; a dependência excessiva de sistemas de IA pode resultar em omissões graves de responsabilidade pessoal e em omissões de assumir responsabilidade pelas ações.

iii. Desafios técnicos e de segurança: a complexidade dos sistemas de IA e a velocidade das ameaças cibernéticas passaram a representar desafios técnicos significativos; entre eles está a incapacidade de detecção de ameaças ocultas ou a presença de "kill switches" em sistemas ou infraestruturas críticas (e.g. energia, saneamento, saúde, transporte), o que comprometer a segurança e a soberania do Estado.

iv. Ética da transparência: a falta de transparência nos algoritmos de IA levanta preocupações éticas sobre como essas decisões são tomadas e quais dados são usados para treinar esses modelos; a opacidade dos algoritmos pode resultar em vieses e distorções indesejadas que afetam negativamente os direitos e liberdades individuais.

v. Cooperação internacional e governança: a abordagem de parceria estratégica entre atores estatais e não-estatais destaca a importância da colaboração internacional na defesa da segurança cibernética; contudo, questões de confiança e compartilhamento de soberania podem dificultar a implementação eficaz dessas parcerias, retrocedendo-se a batalhas tecnológicas.

³² TIMMERS, Paul. Ethics of AI and Cybersecurity When Sovereignty is at Stake. *Minds Mach*, v. 29, n. 4, p. 635–645, 2019. Disponível em: <https://link.springer.com/article/10.1007/s11023-019-09508-4>. Acesso em: 12 de abr. 2024.

vi. Bem comum global: a adoção de uma abordagem de bem comum global para a segurança cibernética enfrenta desafios significativos de governança e coordenação internacional; a falta de um quadro regulatório global e a resistência dos estados em compartilhar soberania nesse campo poderão limitar qualquer compreensão e alcance dessa abordagem³³.

Se existe o reconhecimento dos potenciais ganhos pelo uso de IA e a retórica frequente de que IA não somente aprendeu de modo humano (por emulação e simulação) como também capturou (ou se apropriou de) atributos humanos, a rejeição de argumentos tão mundanos pressiona pela necessidade de recalculer dois efeitos. Primeiro deles diz respeito aos impactos imediatos e invasivos do desenvolvimento tecnológico em IA sobre os espaços jurisdicionais dos Estados; o segundo se refere à destinação ou aplicação utilitária de tecnologias emergentes pelos atores estatais e não-estatais em seus espaços sociais e na vida social digital, que passa a ser moldada por modelos de negócios de Big Techs e seus algoritmos monoculturais e frequentemente excludentes. Aproveitando-se desse contexto, os itens a seguir exploram as principais nuances a respeito do (I) (neo)colonialismo de dados e reações possíveis do resgate ou reconstrução da soberania digital dos estados, (II) a dimensão transnacional da segurança cibernética como base para compreensão de novas manifestações do princípio de segurança internacional, e (III) a cooperação internacional digital diante da emergência e expansão da IA para fins civis e comerciais. Em todas elas existem desafios jurisdicionais a serem enfrentados.

4.1 Colonialismo ou neocolonialismo de dados?

A jurisdição e a aptidão do Estado em fazer expressar sua própria soberania em matéria digital podem estar limitadas pelas ações deliberadas ou formas de colonialismo digital por outros Estados e atores não estatais, como os conglomerados de tecnologia. Esse aspecto se observa sobretudo quanto aos atores que detêm, como mencionado anteriormente, capital informacional e altamente tecnológico sobre o desenvolvimento de sistemas digitais e aplicações de IA³⁴. Nesse sentido, ‘colonialismo digital’ partirá de uma noção dedicada a descrever a exploração e o controle de dados de indivíduos ou regiões por parte de governos, organizações e conglomerados transnacionais que detenham esse poder de controlar o

³³ *Ibidem*, p. 635 e ss.

³⁴ Evidentemente, o capital informacional e altamente tecnológico concentra-se também na elevada detenção e apropriação de conhecimento gerado por dados pessoais e metadados extraídos de cidadãos em diferentes partes do globo, para além dos territórios e Estados em que indivíduos estão residentes ou domiciliados, e quer servem para informar comportamentos no ambiente digital e vulnerabilidades a serem atingidas por aplicações direcionadas ao aparato da guerra cibernética (ataques cibernéticos).

conhecimento sobre o desenvolvimento de sistemas digitais e aplicações de IA³⁵. O colonialismo digital minimiza as bases de afirmação da soberania do Estado em matéria digital, ao minar o controle e a autonomia de atores estatais sobre seus próprios dados, infraestruturas e sistemas digitais.

Desse modo, assim como o colonialismo tradicional envolveu a dominação de territórios, povos e recursos por potências coloniais europeias entre os séculos XVI a XX, o (neo)colonialismo de dados envolve uma dimensão mais ampla de dominação pelo capital informacional e concentração de conhecimento. Ele parte de sistemática coleta, armazenamento e utilização de dados originados sob a jurisdição de estados ou a partir de regiões menos desenvolvidos e de comunidades marginalizadas, de modo a beneficiar outros atores estatais e não estatais mais poderosos³⁶, incluindo todo o universo de interações humano-objeto e objeto-objeto que acompanham o desenvolvimento de novas tecnologias baseadas em “Internet das Coisas” (IoT)³⁷.

Todas essas restrições desafiam a soberania de Estados em matéria digital, sobretudo os que ainda permanecem nas franjas dos centros de conhecimento e de desenvolvimento de tecnologias emergentes e profundas, da tomada de decisões estratégicas pelos novos sistemas e aplicações de IA e do controle corporativo de modelos de negócios em plataformas digitais a transformar a vida social de populações nas diversas regiões do globo. Observa-se o potencial dos países e corporações ‘ricas em dados’ no Norte Global de efetivamente lucrar com os dados que são coletados em várias partes do globo, subsequentemente traduzidos em acúmulo e concentração; essas condutas tendem a minar a soberania – e, no limite, a produção de conhecimento – de países do Sul Global, particularmente mais suscetíveis aos tradicionais mecanismos de dominação e destituição (desposseção), não reconhecendo os contextos locais e suas demandas políticas, históricas e culturais (indiferença)³⁸. A apropriação de dados e a

³⁵ O conceito pode ser apropriado sob distintas perspectivas, como em estudos de comunicação, mídias e mais recentemente, na informática. Cf. COULDRY, Nick; MEJIAS, Ulises A. Data colonialism: Rethinking big data’s relation to the contemporary subject. *Television & New Media*, v. 20, n. 4, p. 336-349, 2019.

³⁶ NATAHNSON, Graciela; MORALES, Susana; RODRIGO. Colonialismo de dados e apropriação das tecnologias digitais: articulações e propostas a partir de uma perspectiva feminista. *Fronteiras: estudos midiáticos*, v. 24, n. 3, p. 1-34, 2022. Disponível em: <https://revistas.unisinos.br/index.php/fronteiras/article/view/25698>. Acesso em: 19 de jun. 2024.

³⁷ RICAURTE, Paola. Data Epistemologies, The Coloniality of Power, and Resistance. *Television & New Media*, v. 20, 2019, p. 350 e ss.

³⁸ Essa sequência de atos entre destituição de dados (‘despossession’) e indiferença radical, por exemplo, é revisitada por Zuboff, a partir da observação de que as ‘Big Techs’ e seus modelos de negócios baseados em extração e acúmulo de dados e monitoramento de usuários em plataformas digitais proporcionaram a clivagem de uma nova apresentação da era capitalista, a de vigilância. Em suma, ela consiste em “(...) uma nova ordem econômica que reivindica a experiência humana como matéria-prima gratuita para práticas comerciais dissimuladas de extração, previsão e vendas”. A esse respeito, ver ZUBOFF, Shoshana. *A Era do Capitalismo de Vigilância: A luta por um futuro humano na nova fronteira do poder*. São Paulo: Intrínseca, 2021, p. 14. A autora

sofisticação de técnicas de *Big Data* sobre larga parte do Sul Global torna-se prática crescente de grandes potências internacionais no espaço de dados, como os Estados Unidos e a China.

Importante ressaltar que, embora os modos, intensidades, escalas e contextos do colonialismo de dados sejam distintos de um modelo tradicional colonial, a função subjacente permanece a mesma, i.e., a de adquirir recursos em grande escala a partir dos quais o valor econômico pode ser extraído³⁹. Em sua essência, o colonialismo de dados instaura uma nova ordem social baseada no controle algorítmico, no rastreamento contínuo dos dispositivos e vidas on-line, a criar oportunidades sem precedentes para a discriminação, pontuação e perfilamento sociais e a influência comportamental das empresas sobre condutas online de cidadãos.

O fenômeno, portanto, vai muito além de plataformas de mídia social e dos serviços de busca e redes sociais que atraíram a maioria das críticas; ele compreende a reorganização completa da vida cotidiana digital de cidadãos e da interação da esfera vital com modelos de negócios ou serviços digitais gestados e oferecidos pelos conglomerados de tecnologias a partir de seus mecanismos de controle e tomada de decisões⁴⁰.

O colonialismo de dados igualmente destaca a disparidade no acesso e controle de dados, a partir do qual empresas ou instituições em nações mais ricas ou tecnologicamente avançadas podem coletar informações de regiões menos desenvolvidas ou de grupos marginalizados, muitas vezes sem qualquer forma de explicação, de transparência ou de consentimento informado, e sem compartilhar quaisquer benefícios equitativamente. Essa forma mais refinada de ‘escambo informacional’ – recuperando-se uma noção típica do mercantilismo - pode levar a uma exploração dos recursos de dados dessas regiões ou grupos, resultando em desequilíbrios de poder e falta de autonomia para os Estados alvos dessas ações e estratégias.

analisa justamente aqueles eventos a partir da influência de conglomerados de tecnologias sediadas nos Estados Unidos (como empresas do Alphabet/Google, Meta/Facebook, Amazon, Apple, Microsoft e Twitter), sem entrar na crescente dominância de plataformas chinesas que tecnicamente exercem a mesma forma de controle.

³⁹ COULDRY, Nick; MEJÍAS, Ulises Ali. *The costs of connection: how data is colonizing human life and appropriating it for capitalism*. Stanford: Stanford University Press, 2019.

⁴⁰ COULDRY, Nick; MEJÍAS, Ulises Ali. Resistance to the new data colonialism must start now. *Al Jazeera*, Doha, 28 de abr. 2020. Disponível em:

<https://www.aljazeera.com/opinions/2020/4/28/resistance-to-the-new-data-colonialism-muststart-now/>. Acesso em: 14 de mai. 2024. Trata-se de nova forma de colonização por grandes conglomerados de tecnologia e computação, que atuam com sua capacidade tecnológica para oferecer recursos acessíveis com o objetivo de receber mais usuários, coletar os seus dados e influenciar seus comportamentos. Ver ainda KOERNER, Andrei. Capitalismo e vigilância digital na sociedade democrática. *Revista Brasileira de Ciências Sociais*, v. 36, n. 105, p. 1-6, 2021. Disponível em: <https://www.scielo.br/j/rbcsoc/a/3RSTj7mCYh6YcHRnM8QZcYD/?format=pdf&lang=pt>. Acesso em: 19 de jun. 2024.

4.2 Dimensão transnacional da segurança cibernética e IA

A noção de segurança nacional, que também traduz uma das expressões concretas da soberania do Estado, passa a ser revisitada a partir de sua pertinência com o espaço cibernético. Acompanhando a natureza transnacional da internet e do comportamento de agentes em mercados digitais integrados, a segurança nacional torna-se agenda de preocupação constante em ataques às redes e infraestruturas de dados direcionados a atores estatais por atores estatais e não estatais. Nesse sentido, as reações de um Estado podem ser erigidas a partir de um quadro normativo robusto e de instrumentos para ações de cibersegurança, por sua natureza também a transcender fronteiras e contemplar uma ampla gama de atores, incluindo entidades públicas e privadas, operando em diferentes jurisdições⁴¹.

De outro lado, a crescente existência de ameaças cibernéticas exige uma abordagem colaborativa e coordenada entre governos, empresas, organizações internacionais e sociedade civil para proteger as infraestruturas críticas e os dados sensíveis de cidadãos. A soberania digital do Estado, nesse caso, reclama a possibilidade de intervenção por mecanismo de defesa, como seria tradicionalmente em casos de ameaças potenciais ou concretas envolvendo integridade territorial e proteção das populações. Entretanto, como ameaças cibernéticas podem atravessar fronteiras e afetar múltiplas jurisdições e ordens estatais simultaneamente, evidenciam-se tanto uma dimensão transnacional dos mecanismos proativos e reativos de cibersegurança, como a consequente interdependência tecnológica existente entre os estados relativamente ao domínio e à exploração de conhecimentos tecnológicos aplicados à segurança cibernética. A noção de segurança internacional, portanto, entrelaçar-se-á com a de segurança nacional, exigindo bases de cooperação internacional ampla para enfrentar desafios comuns e garantir a proteção das infraestruturas críticas e dos dados sensíveis em escala global.

4.3 Cooperação internacional e emergência e consolidação de IA

O desenvolvimento e o uso intensivo de aplicações de IA remodelam as relações internacionais, desafiando a soberania estatal tradicional, seja pelo fato de IA trazer consigo implicações econômicas significativas, que afetam o funcionamento dos mercados, a dinâmica das relações laborais e a interdependência tecnológica entre países, seja por apresentarem desafios institucionais e legais. Esses desafios se manifestam especialmente em relação à

⁴¹ AMORIM, Daniela. Brasil precisa com urgência de Marco de Cibersegurança e Soberania Digital. *CNN*, São Paulo, 9 de mar. 2023. Disponível em: <https://www.cnnbrasil.com.br/economia/brasil-precisa-com-urgencia-de-marco-de-ciberseguranca-e-soberania-digital-diz-fgv/>. Acesso em: 14 de mai. 2024.

jurisdição do Estado (como, em que medida e até onde regular tecnologias emergentes invasivas e subordinantes) e à efetividade de normas internacionais e domésticas de direitos humanos, como as que exigem proteção das liberdades comunicativas e informativas e do direito à privacidade de cidadãos.

Organizações internacionais desempenham um papel crucial na articulação de políticas normativas para regulação de IA dentro de um objetivo sistêmico mais amplo no direito internacional, que é o de preservação da soberania estatal diante de uma competição acirrada em IA. No entanto, a própria geopolítica de IA veio reconfigurar as estruturas de poder entre os estados, com implicações significativas para a soberania estatal, como a respeito da divisão entre os países e regiões que concentram o conhecimento e tecnologias avançadas para o desenvolvimento de sistemas e aplicações de IA e aqueles outros que se qualificam meramente como adquirentes, importadores e consumidores de IA. A desigualdade na distribuição e implementação de IA em várias regiões do mundo, traduzida também como um “abismo” ou “brecha de IA”, será paulatinamente explicada com base nos distintos indicadores globais, como estatísticas, publicações científicas e número de patentes. Em geral, todos esses aspectos tendem a destacar a concentração de pesquisa, desenvolvimento e inovação em países como Estados Unidos, China e Europa, de modo a acentuar o desequilíbrio nas relações econômicas e tecnológicas internacionais em torno de IA⁴².

Se é verdade que a IA traz consigo benefícios potenciais consideráveis em áreas de indústria e na vida social, como nos campos da saúde, medicina e meio ambiente, a reflexão de que o uso de aplicações de IA para fragilizar a integridade territorial e a segurança nacional de estados e a ordem democrática não pode ser descartada. Essa nuance exige novas abordagens em cooperação internacional em matéria digital e cibernética, de modo a assegurar que o desenvolvimento, a implantação e o uso de sistemas de IA não sirvam para atores estatais e não estatais (eg. conglomerados e organizações criminosas transnacionais), como mais uma forma de atingir sistemas de governos, infraestruturas críticas e territórios, como o ataque direto à soberania e à segurança nacional. Um domínio renovado de cooperação internacional digital permite que estados e organizações internacionais atuem de modo orientado para garantir as bases do desenvolvimento responsável de IA em escala transnacional⁴³.

⁴² A esse respeito, ver KITSARA, Irene. Artificial intelligence and the digital divide: From an innovation perspective. In: BOUNFOUR, Ahmed. *Platforms and Artificial Intelligence: The Next Generation of Competences*. Cham: Springer International Publishing, 2022, p. 245-265. Disponível em: https://doi.org/10.1007/978-3-030-90192-9_12. Acesso em: 19 de jun. 2024.

⁴³ USMAN, Hazrat; NAWAZ, Bushra; NASSER, Saiqa. The Future of State Sovereignty in the Age of Artificial Intelligence. *Journal of Law & Social Studies*, v. 5, n. 2, p. 142-152, 2023. Disponível em: <https://www.advancelrf.org/wp-content/uploads/2023/04/Vol-5-No.-2-1.pdf>. Acesso em: 12 de abr. 2024.

A partir da complexa interação entre soberania digital do Estado e IA, é ainda possível investigar como as políticas domésticas nesse campo – na ausência de padrões normativos uniformes e harmônicos em nível internacional – influenciam o próprio desenvolvimento de IA e vice-versa⁴⁴. Na atualidade, como observa Woods, essa interação reconhece a variedade de leis e regulamentos de privacidade e proteção de dados em diferentes países e seu potencial para expandir ou reduzir o crescimento da indústria de IA. Enquanto políticas de privacidade rigorosas tendem a inibir práticas excessivas de coleta e tratamento de dados necessários para o treinamento de sistemas de IA, elas também podem incentivar as bases da indústria doméstica de IA ao assegurar que os dados disponíveis sejam acessíveis como recursos de pesquisa, desenvolvimento e inovação locais⁴⁵.

Por isso, não seria possível deixar de discutir os aspectos normativos de IA em perspectiva transnacional, seja porque padrões regulatórios têm sido forjados por estados dentro de suas respectivas esferas de soberania digital e por atores não estatais (como em princípios, códigos de conduta e instrumentos não vinculantes), seja porque os efeitos aplicativos de sistemas de IA são sentidos em diferentes jurisdições simultaneamente, como no caso do uso do Chat GPT, desenvolvido pela OpenAI, e o ‘aquecimento global’ provocado pela corrida das tecnologias em IA gerativa. Em outro possível eixo analítico, uma vez admitidos três modelos preponderantes de jurisdição prescritiva em matéria digital, como China, União Europeia e Estados Unidos, será possível verificar como suas políticas continuarão a influenciar os rumos tecnológicos no campo de IA⁴⁶. A expansão de tecnologias baseadas em IA (analítica, preditiva, gerativa e comportamental) poderá moldar as próprias bases da soberania digital, como quando um estado decidir, por exemplo, escolher entre campos prioritários para indução e uso de IA e outros para desincentivo e restrições (particularmente aqueles modelos legislativos centrados em ricos, como em certa medida propostos no Regulamento Europeu de IA e na futura Lei brasileira de IA).

Em possível síntese, a interdependência entre soberania digital dos estados e os sistemas de IA em larga escala ao redor do globo forçará estados e organizações internacionais a empreender medidas de intervenção no design tecnológico e na proteção dos próprios componentes ou atributos clássicos da estatalidade no direito internacional – governo, população e território. Por isso mesmo, o equilíbrio entre objetivo de proteção a soberania em

⁴⁴ WOODS, Andrew Keane. *Digital Sovereignty + Artificial Intelligence*, cit. p. 115-17. Disponível em: <https://academic.oup.com/book/55328/chapter/428796733>. Acesso em: 12 de abr. 2024.

⁴⁵ *Idem*.

⁴⁶ *Idem*.

matéria digital sem desincentivar tecnologias emergentes, como IA, e o respeito aos valores democráticos é também um objetivo sistêmico a ser reconhecido no direito internacional. A proposta de adoção de novas normas internacionais, regionais ou domésticas em matéria de IA a enfatizar direitos, obrigações, responsabilidades de agentes e transparência não será desprezível. Ao contrário, ela nasce de uma das linhas mestras para cooperação internacional dedicada a enfrentar os desafios trazidos por sistemas e aplicações de IA à soberania do Estado e de estabelecer regras globais para regular sua implementação⁴⁷.

4.4 Resposta dos Estados e estratégias para reforçar a soberania digital

É possível que Estados recuperem algum espaço em suas atribuições legislativas e judiciais relativamente à matéria digital, especialmente em questões de cibersegurança e IA? A resposta depende muito das reações e medidas de fortalecimento dos próprios instrumentos do direito internacional e dos espaços jurisdicionais compartilhados para propósitos de cooperação em matéria digital. A soberania digital não poderia ser tomada como modismo ou um verbete aleatório, mas antes como expressão apta a reivindicar o reconhecimento de um poder que historicamente os estados puderam exercer para as mais variadas finalidades, desde as mais reprováveis (como nos processos coloniais de dominação e escravização de povos), até as mais funcionalmente desejáveis no campo civil, político, social, econômico e cultural, hoje igualmente estendidas e aplicadas à vida digital.

Reações ao neocolonialismo de dados, por exemplo, passam pela consideração dos processos de revisão e reforma das estruturas, normas e instituições do direito internacional para torná-lo mais equitativo, inclusivo e sensível às realidades e necessidades dos Estados historicamente colonizados, seus sistemas e culturas jurídicas. Essa mesma resposta refere-se à conduta de estados e organizações internacionais, e seus respectivos sistemas de governança presumidamente democráticos, de contestar o poder corporativo transnacional que pode submeter diferentes governos, sociedades e populações a padrões tecnológicos invasivos (e intrusivos) e sistematicamente violadores de direitos fundamentais.

O exemplo brasileiro, por sua vez, pode ser tomado como referência. Recentemente tem se discutido sobre a criação de um marco legal para cibersegurança e soberania digital⁴⁸. Apesar de tecnicamente impreciso, o objetivo de política normativa doméstica a articular o

⁴⁷ TIMMERS, Paul. AI Challenging Sovereignty and Democracy. *Turkish Policy Quarterly*, v. 20, 4 ed, p. 45–55, 2021.

⁴⁸ CONFERÊNCIA internacional debate cibersegurança e soberania digital. *FGV Direito Rio*, Rio de Janeiro, 15 de mar. 2023. Disponível em: <https://diretorio.fgv.br/noticia/conferencia-internacional-debate-ciberseguranca-e-soberania-digital>. Acesso em: 12 de abr. 2024.

desejável fortalecimento de medidas de segurança cibernética a partir do posicionamento do Estado e suas instituições domésticas toma em consideração elementos contextuais relevantes, como o número ou incidência de ataques cibernéticos no Brasil nos últimos anos⁴⁹ e o necessário alinhamento de uma estratégia nacional para cibersegurança⁵⁰.

Nesse caso, não seria suficiente apenas um conjunto programático de medidas de atuação do poder público e de agentes privados, mas antes a adoção de leis e regulamentos que ofereçam padrões mínimos para os níveis operacionais em matéria de cibersegurança, organizando suas dimensões e estabelecendo princípios, governança e formas de cooperação entre os diferentes setores. No Brasil, a Política Nacional de Cibersegurança (PNCiber), foi estabelecida pelo Decreto 11.856/2023, editado pelo Executivo brasileiro, que também instituiu o Comitê Nacional de Cibersegurança⁵¹. Curiosamente, o objetivo da Política seria o de uniformizar a diversidade regulatória vigente no Brasil, reduzir os danos infligidos à sociedade decorrentes dos incidentes cibernéticos, diminuir o déficit tecnológico nacional no setor e ampliar a participação brasileira no âmbito internacional⁵². Examinadas as regiões mais significativas para a expansão das estratégias nacionais de IA e de segurança cibernética, as abordagens de estratégias nacionais têm sido muito distintas, variando entre preocupações com uso confiável de tecnologias digitais, transição digital, defesa de infraestruturas críticas e barreiras à atuação de empresas estrangeiras em território nacional:

- *União Europeia:* Em 2022, a União Europeia lançou sua Estratégia de Cibersegurança para aumentar a resiliência contra ameaças cibernéticas e garantir o uso confiável de tecnologias digitais. Com ênfase em ‘soberania tecnológica’ e cooperação global, a estratégia da UE objetiva fortalecer a resiliência e capacidade operacional, além de promover iniciativas regulatórias e de investimento

⁴⁹ Somente no Brasil, em 2022, houve 103,16 bilhões de tentativas de ataques cibernéticos, conforme estudo produzido pelo Centro de Tecnologia e Sociedade (CTS) da Escola de Direito do Rio de Janeiro da Fundação Getúlio Vargas (FGV Direito Rio): BELLI, Luca *et al.* *Cibersegurança: uma visão sistêmica rumo a uma Proposta de Marco Regulatório para um Brasil Digitalmente soberano*. Rio de Janeiro: FGV Direito Rio, 2023. Disponível em: <https://cyberbrics.info/ciberseguranca-uma-visao-sistematica-rumo-a-uma-proposta-de-marco-regulatorio-para-um-brasil-digitalmente-soberano/>. Acesso em: 12 de abr. 2024.

⁵⁰ *Ibidem*, nota 48 supra.

⁵¹ O CNCiber é estabelecido no âmbito da Câmara de Relações Exteriores e Defesa Nacional do Conselho de Governo, com a finalidade de acompanhar a implementação e a evolução da PNCiber. O comitê será composto por representantes do governo, sociedade civil, instituições científicas e de entidades do setor empresarial e terá como missão propor atualizações para a PNCiber e sugerir estratégias de cooperação técnica internacional. A esse respeito, ver: SECRETARIA DE COMUNICAÇÃO SOCIAL. O que é a Política Nacional de Cibersegurança, marco no combate aos crimes virtuais. Disponível em: <https://www.gov.br/secom/pt-br/fatos/brasil-contrafake/noticias/2023/3/o-que-e-a-politica-nacional-de-ciberseguranca-marco-no-combate-aos-crimes-virtuais>. Acesso em: 12 de mai. 2024.

⁵² PINHEIRO, Patrícia Peck. O que é esperado com a Política Nacional de Cibersegurança (PNCiber). *FEBRABAN Tech*, São Paulo, 15 de jan. 2024. Disponível em: <https://febrabantech.febraban.org.br/especialista/patricia-peck-pinheiro/o-que-e-esperado-com-a-politica-nacional-de-ciberseguranca-pnciber>. Acesso em: 12 mai. 2024.

alinhadas com a transição digital e a agenda de recuperação da UE, sendo parte integrante do Programa ‘Shaping Europe's Digital Future’ e da Estratégia de Segurança da União 2020-2025⁵³.

- *Estados Unidos:* Em 2023, o país lançou a Estratégia Nacional de Segurança Cibernética (NCSIP), com o objetivo de fortalecer a defesa das infraestruturas críticas, integrar agências federais, dismantelar ameaças, prevenir abusos, e promover colaboração público-privada, investimentos em pesquisa e desenvolvimento, parcerias internacionais e normas globais, fornecendo diretrizes para uma abordagem holística e resiliente à segurança cibernética⁵⁴.

- *China:* em novembro de 2016, a China havia aprovado a Lei de Cibersegurança, que concedeu um poder maior ao governo central para registrar e controlar informações disseminadas na internet que fossem consideradas ilegais. A Lei foi introduzida pela Autoridade de Administração do Ciberespaço da China (‘Cyberspace Administration of China’ -CAC), subordinada a uma Comissão de Relações do Ciberespaço. A política chinesa se caracteriza pela centralização da governança cibernética, criação de barreiras para empresas estrangeiras de tecnologia, controle do fluxo de informação na internet, exigência de armazenamento local de dados críticos e estabelecimento de normas de segurança cibernética com punições por não conformidade⁵⁵.

Em outros cenários, estados e organizações reagem diretamente a determinadas aplicações de inteligência artificial que têm sido utilizadas por governos, como dentro de um regime autoritário e de monitoramento de cidadãos. O exemplo dos sistemas de pontuação social (‘social scoring’) na China trouxe uma resposta mais enérgica da União Europeia e Estados Unidos, com a proposta atribuída ao Conselho de Comércio e Tecnologia (‘CCT’) em setembro de 2021. Ambos expressaram oposição ao uso massivo de IA para desrespeitar direitos humanos, como em decorrência desses sistemas empregados pelo governo central chinês. O CCT representa uma tentativa de formar uma aliança em torno de uma abordagem de direitos humanos para o desenvolvimento da IA, a contrastar regimes autoritários que frequentemente empregam tecnologias para monitoramento e perseguição de cidadãos e opositores políticos, além de práticas e políticas discriminatórias.

⁵³ THE Cybersecurity Strategy. European Commission, 2022. Disponível em: <https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-strategy>. Acesso em: 12 de mai. 2024.

⁵⁴ THE WHITE HOUSE WASHINGTON. *National Cybersecurity Strategy*. Washington D.C.: 2023. <https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf>. Acesso em: 12 de mai. 2024.

⁵⁵ XINXCHUCHU, Gao. Sovereignty and Cyberspace: China’s Ambition to Shape Cyber Norms. *LSE Blogs*, Londres, 18 de ago. 2022. Disponível em: <https://blogs.lse.ac.uk/cff/2022/08/18/sovereignty-and-cyberspace-chinas-ambition-to-shape-cyber-norms/>. Acesso em: 14 de mai. 2024.

No entanto, essas abordagens divergentes podem levar a um desacoplamento tecnológico, não apenas contrapondo estados e suas políticas tecnológicas, mas também a fragmentar os mercados de alta tecnologia. A União Europeia adotou abordagem mais holística para a governança da IA, exemplificada pelo Regulamento de IA da UE⁵⁶ a mesclar um modelo baseado em risco e em direitos fundamentais dos cidadãos no mercado interno e domínio intracomunitário, enquanto os EUA favorecem uma abordagem leve de regulamentação. Enquanto isso, a China segue a fortalecer suas regulamentações de IA e dados, buscando alcançar a autossuficiência tecnológica e fincar as bases de uma expressão de soberania digital que pode evidentemente ser objeto de escrutínio à luz das normas internacionais de direitos humanos. Paradoxalmente, o contraste ideológico pode também levar à divisão dos ecossistemas digitais entre EUA, UE e China, dificultando a harmonização da regulamentação da IA internacionalmente⁵⁷ e truncando o globo em três grandes macrorregiões de IA.

5 Conclusão

Com base nas discussões apresentadas ao longo deste artigo, é evidente que a soberania digital do Estado e a expansão de tecnologias emergentes estão profundamente interligadas, contemplando questões complexas na interação entre direito internacional, segurança cibernética e inteligência artificial. Os desafios éticos e práticos enfrentados pelos Estados no exercício da jurisdição em matéria digital demandam respostas eficazes e cooperativas do ponto de vista multilateral e bilateral. Sugerem revisão de normas e instituições do direito internacional para abordar questões como soberania digital, neocolonialismo de dados e a crescente concentração de poder por parte de empresas de tecnologia em escala global, a representar a própria configuração de ordem transnacional digital revestida de assimetrias. A necessidade de cooperação entre atores estatais e não estatais será crucial para garantir o fortalecimento das bases de segurança cibernética e promover o uso ético da inteligência artificial.

Em última análise, a manutenção da soberania estatal em um mundo digitalizado, tecnológica e digitalmente interdependente exige uma abordagem holística, considerando não apenas os avanços científicos, tecnológicos e de inovação, mas também princípios éticos e cooperativos que regem a atuação dos Estados na ordem internacional. Cada vez mais, a

⁵⁶ PARLAMENTO EUROPEU, Regulamento (UE) 2024/206 do Parlamento Europeu e do Conselho de 21 de abril de 2021, *cit.*, (nota 30 supra).

⁵⁷ LARSEN, Benjamin Cedric. The geopolitics of AI and the rise of digital sovereignty. *Brookings*, Washington D.C., 8 de dez. 2022. Disponível em: <https://www.brookings.edu/articles/the-geopolitics-of-ai-and-the-rise-of-digital-sovereignty/>. Acesso em: 15 de abr. 2024.

cooperação entre governos, organizações, sociedade civil, indústria e academia torna-se fundamental para enfrentar os desafios emergentes. Ao recuperar o caráter central da soberania digital do Estado como compromisso democrático e de garantias de direitos fundamentais da cidadania digital, instituições internacionais terão condições de construir uma ‘ordem transnacional digital’ equitativa, centrada em direitos humanos e preocupações humanas que transcendam interesses pragmáticos ou meramente econômicos de atores estatais e não-estatais.

Agradecimentos

O presente trabalho foi realizado com apoio da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior - Brasil (CAPES) - Código de Financiamento 001- Programa Institucional de Internacionalização dos Programas de Pós-Graduação - Edital CAPES/PRINT nº 41/2017- e parte de atividades de investigação conduzidas pelo autor no projetos “Cultura, Direito Comparado e os desafios do Direito Internacional na Ordem Global” e “Estudos Europeus em perspectivas comparadas: a sustentabilidade e a integração regional em contexto de politicidade, governança e inteligência artificial” do Programa de Pós-Graduação em Direito da Universidade Federal de Minas Gerais, e seminários da Cátedra PhiloTech – Filosofia da Tecnologia e Direito Digital da UFMG e do Grupo Interinstitucional de Pesquisa em Ciberdireito (DGP/CNPq). O autor agradece imensamente à acadêmica Carolina Britski Puga (Direito SP/FGV) pela assistência de pesquisa e revisão do texto e à gentil acolhida de toda equipe do Departamento de Filosofia da Universidade de Barcelona -UB, em especial ao estimado Professor Titular Gonçal Mayos Solsona, recorrente entusiasta da cooperação internacional de pesquisa e mobilidade docente entre UB e UFMG.

Referências Bibliográficas

- AMORIM, Daniela. Brasil precisa com urgência de Marco de Cibersegurança e Soberania Digital. *CNN*, São Paulo, 9 de mar. 2023. Disponível em: <https://www.cnnbrasil.com.br/economia/brasil-precisa-com-urgencia-de-marco-de-ciberseguranca-e-soberania-digital-diz-fgv/>. Acesso em: 14 de mai. 2024.
- AVILA PINTO, Renata. Digital Sovereignty or Digital Colonialism. *International Journal on Human Rights*. v. 15, n.27, p.15-28, 2018. Disponível em: <https://sur.conectas.org/en/digital-sovereignty-or-digital-colonialism/>. Acesso em: 19 de jun. 2024.
- BELLI, Luca. To Get Its AI Foothold, Brazil Needs to Apply the Key AI Sovereignty Enablers (KASE). In: FELDSTEIN, Steven (eds.). *New Digital Dilemmas: Resisting Autocrats, Navigating Geopolitics, Confronting Platforms*. Washington, DC, Carnegie Endowment for International Peace, p. 27-34, 2023.
- BELLI, Luca *et al.* *Cibersegurança: uma visão sistêmica rumo a uma Proposta de Marco Regulatório para um Brasil Digitalmente soberano*. Rio de Janeiro: FGV Direito Rio, 2023. Disponível em: <https://cyberbrics.info/ciberseguranca-uma-visao-sistemica-rumo-a-uma-proposta-de-marco-regulatorio-para-um-brasil-digitalmente-soberano/>. Acesso em: 12 de abr. 2024.
- BRATTON, Benjamin H. *The stack: On software and sovereignty*. MIT press, 2016.
- CINTRA et. All. *Plataformização, inteligência artificial e soberania de dados: tecnologia no Brasil 2020-2030*, 2023. Disponível em: <https://portolivree.fiocruz.br/plataformizacao-inteligencia-artificial-e-soberania-de-dados-tecnologia-no-brasil-2020-2030>. Acesso em: 12 de abr. 2024.
- CNN. *Brasil precisa com urgência de Marco de Cibersegurança e Soberania Digital, diz FGV*. Disponível em: <https://www.cnnbrasil.com.br/economia/brasil-precisa-com-urgencia-de-marco-de-ciberseguranca-e-soberania-digital-diz-fgv/>. Acesso em: 12 de abr. 2024.
- CONFERÊNCIA internacional debate cibersegurança e soberania digital. *FGV Direito Rio*, Rio de Janeiro, 15 de mar. 2023. Disponível em: <https://diretorio.fgv.br/noticia/conferencia-internacional-debate-ciberseguranca-e-soberania-digital>. Acesso em: 12 de abr. 2024.
- COULDRY, Nick; MEJIAS, Ulises A. Data colonialism: Rethinking big data's relation to the contemporary subject. *Television & New Media*, v. 20, n. 4, p. 336-349, 2019. Disponível em: <https://journals.sagepub.com/doi/full/10.1177/1527476418796632>. Acesso em: 19 de jun. 2024.
- COULDRY, Nick; MEJÍAS, Ulises Ali. Resistance to the new data colonialism must start now. *Al Jazeera*, Doha, 28 de abr. 2020. Disponível em: <https://www.aljazeera.com/opinions/2020/4/28/resistance-to-the-new-data-colonialism-muststart-now/>. Acesso em: 14 de mai. 2024.
- COULDRY, Nick; MEJÍAS, Ulises Ali. *The costs of connection: how data is colonizing human life and appropriating it for capitalism*. Stanford: Stanford University Press, 2019.
- CRISTIANO LIMA-STRONG. *Biden signs bill that could ban TikTok, a strike years in the making*. Disponível em: <https://www.washingtonpost.com/technology/2024/04/23/tiktok-ban-senate-vote-sale-biden/>. Acesso em: 14 de mai. 2024.
- DOMESTIC SURVEILLANCE DIRECTORATE. *Surveillance Techniques: How Your Data Becomes Our Data*. Disponível em: <https://nsa.gov/1.info/surveillance/>. Acesso em: 17 de abr. 2024.
- ELON Musk is feuding with Brazil's powerful Supreme Court. *The Economist*, Londres, 14 de abr. 2024. Disponível: <https://www.economist.com/the-americas/2024/04/14/elon-musk-is-feuding-with-brazils-powerful-supreme-court>. Acesso: 14 de mai. 2024.

- FGV. *Conferência internacional debate cibersegurança e soberania digital*. Rio de Janeiro: Fundação Getúlio Vargas. Disponível em: <https://diretorio.fgv.br/noticia/conferencia-internacional-debate-ciberseguranca-e-soberania-digital>. Acesso em: 12 de abr. 2024.
- FIDLER, David P. Whither the Web? International Law, Cybersecurity, and Critical Infrastructure Protection. *Georgetown Journal of International Affairs*. v. 16, n. 3, p. 8-20, 2015. Disponível em: <https://www.repository.law.indiana.edu/cgi/viewcontent.cgi?article=3452&context=facpub>. Acesso em: 19 de jun. 2024.
- FUNG, Brian. Biden just signed a potential TikTok ban into law. Here's what happens next. *CNN*, Atlanta, 24 de abr. 2024. Disponível em: <https://edition.cnn.com/2024/04/23/tech/congress-tiktok-ban-what-next/index.html>. Acesso em: 15 de mai. 2024.
- GAGLIARDONE, Iginio. A Postcolonial Perspective on Digital Sovereignty. In: FELDSTEIN, Steven (eds.). *New Digital Dilemmas: Resisting Autocrats, Navigating Geopolitics, Confronting Platforms*. Washington, DC: Carnegie Endowment for International Peace, 2023.
- GRAVETT, Willem. Digital neo-colonialism: The Chinese model of internet sovereignty in Africa. *African Human Rights Law Journal*, v. 20, n. 1, p. 125-146, 2020.
- KITSARA, Irene. Artificial intelligence and the digital divide: From an innovation perspective. In: BOUNFOUR, Ahmed. *Platforms and Artificial Intelligence: The Next Generation of Competences*. Cham: Springer International Publishing, 2022, p. 245-265. Disponível em: https://doi.org/10.1007/978-3-030-90192-9_12. Acesso em: 19 de jun. 2024.
- KOERNER, Andrei. Capitalismo e vigilância digital na sociedade democrática. *Revista Brasileira de Ciências Sociais*, v. 36, n. 105, p. 1-6, 2021. Disponível em: <https://www.scielo.br/j/rbcsoc/a/3RSTj7mCYh6YcHRnM8QZcYD/?format=pdf&lang=pt>. Acesso em: 19 de jun. 2024.
- LANGAN, Mark. *Neo-Colonialism and the Poverty of 'Development in Africa*. Cham: Springer/Palgrave, p. 1-261, 2018.
- LARSEN, Benjamin Cedric. The geopolitics of AI and the rise of digital sovereignty. *Brookings*, Washington D.C., 8 de dez. 2022. Disponível em: <https://www.brookings.edu/articles/the-geopolitics-of-ai-and-the-rise-of-digital-sovereignty/>. Acesso em: 15 de abr. 2024.
- LAVANIA, Ankit. The need to fill legal vacuum in international law to deal with non-state actors in cyber operations. *International Journal of Law Management & Humanities*, vol.5, p. 462-478, 2022.
- LIMA-STRONG, Cristiano. Biden signs bill that could ban TikTok, a strike years in the making. *The Washington Post*, Washington D.C., 24 de abr. 2024. Disponível em: <https://www.washingtonpost.com/technology/2024/04/23/tiktok-ban-senate-vote-sale-biden/>. Acesso em: 14 mai. 2024.
- MACHADO, Léia; SOUSA, Juliana. Especial security leaders: Soberania de dados além da Segurança - Security Leaders. *Security Leaders*, São Paulo, 23 de jan. 2024. Disponível em: <https://securityleaders.com.br/especial-security-leaders-soberania-de-dados-alem-da-seguranca/>. Acesso em: 12 de abr. 2024.
- MITCHELL, Andrew D.; SAMLIDIS, Theodore. Cloud services and government digital sovereignty in Australia and beyond. *International Journal of Law and Information Technology*, vol. 29, n. 4, p. 364-394, 2021. Disponível em: <https://academic.oup.com/ijlit/article/29/4/364/6516411?login=false>. Acesso em: 19 de jun. 2024.

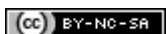
- MUELLER, Milton, Communications and the Internet. In: COGAN, Jacob Katz; HURD, Ian; JOHNSTONE, Ian (Ed.). *The Oxford handbook of international organizations*. Oxford: Oxford University Press, 2016, pp.535-56.
- NATAHNSON, Graciela; MORALES, Susana; RODRIGO. Colonialismo de dados e apropriação das tecnologias digitais: articulações e propostas a partir de uma perspectiva feminista. *Fronteiras: estudos midiáticos*, v. 24, n. 3, p. 1-34, 2022. Disponível em: <https://revistas.unisinos.br/index.php/fronteiras/article/view/25698>. Acesso em: 19 de jun. 2024.
- PARLAMENTO EUROPEU. Regulamento (UE) 2024/206 do Parlamento Europeu e do Conselho, adotado em 13 de março de 2024 estabelecendo regras harmonizadas sobre inteligência artificial ('Artificial Intelligence Act') e alterando certos atos legislativos da União, Jornal Oficial da União Europeia, Estrasburgo: Parlamento Europeu, 2024. Disponível em: https://www.europarl.europa.eu/doceo/document/TA-9-2024-0138-FNL-COR01_PT.pdf. Acesso em: 19 de jun. 2024.
- PELLEGRINI, Jerônimo *et al.* Inteligência local, soberania digital e soberania de dados. In: PENTEADO, Cláudio; PELLEGRINI, Jerônimo; SILVEIRA, Sérgio Amadeu da (org.). *Plataformização, inteligência artificial e soberania de dados: tecnologia no Brasil 2020-2030*. São Paulo: Ação Educativa, 2023. Disponível em: <https://portolivre.fiocruz.br/plataformizacao-inteligencia-artificial-e-soberania-de-dados-tecnologia-no-brasil-2020-2030>. Acesso em: 12 de abr. 2024.
- PINHEIRO, Patrícia Peck. O que é esperado com a Política Nacional de Cibersegurança (PNCiber). *FEBRABAN Tech*, São Paulo, 15 de jan. 2024. Disponível em: <https://febrabantech.febraban.org.br/especialista/patricia-peck-pinheiro/o-que-e-esperado-com-a-politica-nacional-de-ciberseguranca-pnciber>. Acesso em: 12 mai. 2024.
- POLIDO, Fabrício B.P. *Direito Internacional Privado nas Fronteiras do Trabalho e Tecnologias*. 2ª ed. Rio de Janeiro: Lumen Juris, 2021.
- RICARTE, Paola. Data Epistemologies, The Coloniality of Power, and Resistance. *Television & New Media*, v. 20, p. 350-365, 2019. Disponível em: <https://journals.sagepub.com/doi/epub/10.1177/1527476419831640>. Acesso em: 19 de jun. 2024.
- SECRETARIA DE COMUNICAÇÃO SOCIAL. O que é a Política Nacional de Cibersegurança, marco no combate aos crimes virtuais. Disponível em: <https://www.gov.br/secom/pt-br/fatos/brasil-contrafake/noticias/2023/3/o-que-e-a-politica-nacional-de-ciberseguranca-marco-no-combate-aos-crimes-virtuais>. Acesso em: 12 de mai. 2024.
- SHAW, Malcolm N. *International law*. 5th ed, Cambridge: Cambridge Univ. Press. 2003.
- SINGER, Peter W.; FRIEDMAN, Allan. *Cybersecurity and Cyberwar: what everyone needs to know*. Oxford: Oxford University Press, 2014.
- SOVEREIGNTY in Cyberspace: Theory and Practice (Version 4.0). *World Internet Conference*, Wuzhen, 16 de jan. 2024. Disponível em: https://subsites.chinadaily.com.cn/wic/2024-01/16/c_956165.htm. Acesso em: 15 de abr. 2024.
- SURVEILLANCE Techniques: How Your Data Becomes Our Data. *Domestic Surveillance Directorate*, [s. l.], 2021. Disponível em: <https://nsa.gov/1.info/surveillance/>. Acesso em: 19 de jun. 2024
- TAITZ, Sarah. Five Things to Know About NSA Mass Surveillance and the Coming Fight in Congress. *ACLU*, Nova Iorque, 11 de abr. 2023. Disponível em: <https://www.aclu.org/news/national-security/five-things-to-know-about-nsa-mass-surveillance-and-the-coming-fight-in-congress>. Acesso em: 17 de abr. 2024.

- THE Cybersecurity Strategy. European Commission, 2022. Disponível em: <https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-strategy>. Acesso em: 12 de mai. 2024.
- THE WHITE HOUSE WASHINGTON. *National Cybersecurity Strategy*. Washington D.C.: 2023. <https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf>. Acesso em: 12 de mai. 2024.
- TIKTOK vows legal fight after Biden signs sell-or-ban bill. *Deutsche Welle*, Bonn, 24 de abr. 2024. Disponível: <https://www.dw.com/en/tiktok-vows-legal-fight-after-biden-signs-sell-or-ban-bill/a-68912207>. Acesso em: 14 de mai. 2024.
- TIMMERS, Paul. AI Challenging Sovereignty and Democracy. *Turkish Policy Quarterly*, v. 20, 4 ed, p. 45–55, 2021.
- TIMMERS, Paul. Ethics of AI and Cybersecurity When Sovereignty is at Stake. *Minds Mach*, v. 29, n. 4, p. 635–645, 2019. Disponível em: <https://link.springer.com/article/10.1007/s11023-019-09508-4>. Acesso em: 12 de abr. 2024.
- USMAN, Hazrat; NAWAZ, Bushra; NASSER, Saiqa. The Future of State Sovereignty in the Age of Artificial Intelligence. *Journal of Law & Social Studies*, v. 5, n. 2, p. 142-152, 2023. Disponível em: <https://www.advancelrf.org/wp-content/uploads/2023/04/Vol-5-No.-2-1.pdf>. Acesso em: 12 de abr. 2024.
- WOODS, Andrew Keane. Digital Sovereignty + Artificial Intelligence. In: CHANDER, Anupam; SUN, Haochen (eds). *Data Sovereignty: From the Digital Silk Road to the Return of the State* New York. Oxford: Oxford University Press, 2023. p.115-136. Disponível em: <https://academic.oup.com/book/55328/chapter/428796733>. Acesso em: 12 de abr. 2024.
- WORLD ECONOMIC FORUM. The Global Risk Report 2024. Coligny/Genebra: World Economic Forum, 2024. Disponível em: https://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2024.pdf. Acesso em: 19 de jun. 2024.
- XINXCHUCHU, Gao. Sovereignty and Cyberspace: China's Ambition to Shape Cyber Norms. *LSE Blogs*, Londres, 18 de ago. 2022. Disponível em: <https://blogs.lse.ac.uk/cff/2022/08/18/sovereignty-and-cyberspace-chinas-ambition-to-shape-cyber-norms/>. Acesso em: 14 de mai. 2024.
- ZUBOFF, Shoshana. We make them dance: surveillance capitalism, the rise of instrumental power, and the threat to human rights. In: JØRGENSEN, Rikke Frank (ed.) *Human Rights in the Age of Platforms*. Cambridge: MIT Press, p. 3-51, 2019. Disponível em: <https://direct.mit.edu/books/oa-edited-volume/4531/Human-Rights-in-the-Age-of-Platforms>. Acesso: 14 de mai. 2024.
- ZUBOFF, Shoshana. *A Era do Capitalismo de Vigilância: A luta por um futuro humano na nova fronteira do poder*. São Paulo: Intrínseca, 2021.

Como citar este artigo: POLIDO, Fabrcio Bertini Pasquot. Estado, soberania digital e tecnologias emergentes: interaões entre direito internacional, segurana ciberntica e inteligncia artificial. *Revista de Cincias do Estado*, Belo Horizonte, v. 9, n. 1, p. 1-30, 2024.

Recebido em 17.05.2024

Publicado em 20.06.2024



Atribuião-NãoComercial-CompartilhaIguat 4.0 Internacional