FACULDADE DOM ADÉLIO TOMASIN – FADAT

CURSO DE GRADUAÇÃO EM DIREITO

FRANCISCO CÉU PEREIRA DE OLIVEIRA DANTAS

DESAFIOS DA CIBERSEGURANÇA E PROTEÇÃO DE DADOS: UMA ANÁLISE CRÍTICA DAS LIMITAÇÕES DA LGPD E GDPR NO ENFRENTAMENTO DA ESPIONAGEM CIBERNÉTICA

QUIXADÁ - CEARÁ

2025

Francisco Céu Pereira de Oliveira Dantas

DESAFIOS DA CIBERSEGURANÇA E PROTEÇÃO DE DADOS: UMA ANÁLISE CRÍTICA DAS LIMITAÇÕES DA LGPD E GDPR NO ENFRENTAMENTO DA ESPIONAGEM CIBERNÉTICA

Monografia apresentada como requisito para aprovação na disciplina Trabalho de Conclusão de Curso II e conclusão do Curso de Direito da Faculdade Dom Adelio Tomasin - FADAT.

Orientador: Prof. Dr. Valter Moura do Carmo

QUIXADÁ - CEARÁ

2025

Dados Internacionais de Catalogação na Publicação (CIP)
FADAT - Educação Superior
Biblioteca Francisca Alexandre Gomes (Dona Mocinha)

DA186

Dantas, Francisco do Céu Pereira de Oliveira

Desafios da cibersegurança e proteção de dados: uma análise crítica das limitações da LGPD e GDPR no enfrentamento da espionagem cibernética / Francisco do Céu Pereira de Oliveira Dantas. – 2025.

53 f. :

Ilustrações: Não possui.

TCC-Graduação – FADAT - Educação Superior. - Curso de Direito.

Orientação: Doutor(a) Valter Moura do Carmo.

Palavras-chave: LGPD - GDPR - Proteção de dados, Cibersegurança, Soberania digital, Espionagem cibernética, Cooperação internacional.

CDD 740

Gerada automaticamente mediante os dados fornecidos pelo(a) autor(a)

DEDICATÓRIA

Dedico esta monografia à minha mãe, Maria Silvia Dantas, mulher de força serena e amor imensurável. Águia de alma e de espírito, foi ela quem, com suas asas firmes e seu coração incansável, me ensinou a voar — mesmo quando o céu parecia distante e as quedas inevitáveis. Foi nos seus olhos que encontrei coragem, e nos seus silêncios, a sabedoria que me ergueu todas as vezes. A ela, minha eterna gratidão e o mais profundo amor.

AGRADECIMENTOS

Agradeço imensamente à minha família, em especial à minha mãe e às minhas irmãs, Erika e Louise Vitória, pelo amor, apoio incondicional e paciência ao longo desta jornada. Aos nossos companheiros de quatro patas — Joy, Penélope, Dominique e Charlotte — em especial à gata que, tantas vezes, virou noites deitada sobre meus livros, minha eterna gratidão por tornar os momentos difíceis mais leves.

Ao meu orientador, Dr. Valter Moura do Carmo — o gigante da ABNT —, registro meu mais profundo agradecimento. Com rigor, paciência e dedicação, ele não apenas corrigiu meu caminho quando necessário, mas também foi uma referência acadêmica constante, que nunca desistiu de mim. Muito obrigado por acreditar no meu potencial.

Estendo meus agradecimentos à banca avaliadora, composta pelos professores Me. José Carneiro Rangel Júnior e pelo Dr. Rodrigo Vieira Costa. Este último, de maneira especial, me inspirou profundamente por meio de sua obra Desinformação, regulação das plataformas e direitos digitais, contribuindo para a definição da área acadêmica e profissional que desejo seguir.

Aos colegas da minha turma, que ao longo do tempo se tornaram verdadeiros amigos, e à instituição FADAT, minha sincera gratidão por fazerem parte desta caminhada tão significativa.

A tarefa não é tanto ver aquilo que ninguém viu, mas pensar o que ninguém ainda pensou sobre aquilo que todo mundo vê.

Arthur Schopenhauer

RESUMO

Esta monografia analisa os desafios da cibersegurança e da proteção de dados pessoais, com foco nas limitações da Lei Geral de Proteção de Dados (LGPD) e do Regulamento Geral sobre a Proteção de Dados (GDPR) frente à espionagem cibernética. Destaca a importância dos dados como ativos estratégicos e a necessidade de articulação entre privacidade, soberania digital e segurança informacional. A pesquisa estrutura-se em três eixos: evolução das legislações, riscos associados à espionagem e vulnerabilidades em infraestruturas críticas, e cooperação internacional. Conclui-se que a proteção de dados deve estar integrada a políticas públicas eficazes, à educação digital e à harmonização regulatória global.

Palavras-chave: LGPD - GDPR - Proteção de dados – Cibersegurança - Soberania digital - Espionagem cibernética - Cooperação internacional.

ABSTRACT

This monograph analyzes the challenges of cybersecurity and personal data protection, focusing on the limitations of the Brazilian General Data Protection Law (LGPD) and the European General Data Protection Regulation (GDPR) in the context of cyberespionage. It highlights the strategic importance of data and the need to align privacy, digital sovereignty, and information security. The study is structured around three main axes: the evolution of data protection regulations, risks associated with espionage and critical infrastructure vulnerabilities, and international cooperation. It concludes that effective public policies, digital education, and regulatory harmonization are essential to ensure robust data protection.

Keywords: LGPD - GDPR - Data protection – Cybersecurity - Digital sovereignty – Cyberespionage - International cooperation.

SUMÁRIO

1 INTRODUÇÃO 9
2 REGULAÇÃO GLOBAL E DESAFIOS DA PROTEÇÃO DE DADOS 12
2.1 Histórico e marcos regulatórios globais (GDPR E LGPD) 12
2.2 Principais desafios da implementação no Brasil 15
2.3 Princípios da privacidade de dados e questões de cibersegurança e espionagem 18
2.4 Comparativo entre legislações internacionais e a LGPD 20
3 AMEAÇAS CIBERNÉTICAS E DESAFIOS À SEGURANÇA DIGITAL 23
3.1 Espionagem cibernética e vulnerabilidade em infraestruturas críticas 23
3.2 Impactos da coleta massiva de dados na privacidade 28
3.3 Cibersegurança como pilar da soberania nacional 32
4 COOPERAÇÃO INTERNACIONAL E POLÍTICAS PÚBLICAS PARA CIBERSEGURANÇA 35
4.1 Iniciativas globais e o papel de tratados internacionais 35
4.2 A relação entre segurança nacional e proteção de dados pessoais 38
4.3 **Propostas para integração global no combate às ameaças cibernéticas** 40
CONCLUSÃO 45
REFERÊNCIA 48

1 INTRODUÇÃO

A transformação digital das sociedades contemporâneas, impulsionada pela disseminação da internet, o avanço da computação em nuvem, a utilização massiva de dispositivos móveis e o crescimento exponencial do volume de dados gerados, redesenhou profundamente as dinâmicas econômicas, políticas e sociais globais. Nesse novo ecossistema informacional, os dados pessoais passaram a desempenhar um papel estratégico, tanto como ativo comercial quanto como elemento central para a formulação de políticas públicas, o funcionamento de serviços essenciais e a construção de perfis comportamentais. Como observa Rodrigo Vieira Costa (2023), "os dados e os algoritmos que os tratam tornaram-se o principal insumo da economia digital, ao mesmo tempo em que desafiam a efetividade dos direitos fundamentais no ambiente das plataformas". Com isso, a privacidade e a proteção de dados se tornaram temas centrais no debate jurídico e político do século XXI (Zuboff, 2020).

Diante da centralidade dos dados na vida digital, emergiram diversas legislações nacionais e regionais voltadas à sua regulamentação. O marco mais influente nesse contexto foi o Regulamento Geral sobre a Proteção de Dados (*General Data Protection Regulation* – GDPR), aprovado pela União Europeia em 2016 e aplicável desde 2018. Com caráter vinculante e extraterritorial, o GDPR impôs aos países e empresas que tratam dados de cidadãos europeus um rigoroso padrão normativo baseado em princípios como finalidade, transparência, segurança e *accountability* (EUROPEAN UNION, 2016).

Inspirada nesse modelo, o Brasil sancionou a Lei Geral de Proteção de Dados Pessoais (LGPD), Lei nº 13.709/2018, a fim de sistematizar os direitos dos titulares de dados e regulamentar as obrigações dos agentes de tratamento no território nacional (BRASIL, 2018).

No entanto, embora compartilhem fundamentos comuns, o GDPR e a LGPD apresentam diferenças significativas quanto à estrutura institucional, ao alcance regulatório e ao grau de maturidade na aplicação. A GDPR foi construída sobre décadas de políticas de privacidade implementadas nos países europeus, contando com uma infraestrutura institucional consolidada e autoridades fiscalizadoras atuantes, como a Comissão Nacional de Informática e Liberdades (CNIL) na França ou o *Information Commissioner's Office* (ICO) no Reino Unido. A LGPD, por sua vez, ainda enfrenta obstáculos à sua plena implementação, como a escassez

de recursos da Autoridade Nacional de Proteção de Dados (ANPD), a carência de profissionais capacitados e a percepção empresarial de que a conformidade legal representa um ônus e não um investimento em governança (Ferreira, 2020; Souza, 2021).

Paralelamente ao desenvolvimento legislativo, o aumento das ameaças cibernéticas trouxe novos desafios à proteção de dados e à soberania digital. Práticas como espionagem digital, *ransomware*, ataques a infraestruturas críticas e manipulação algorítmica de comportamentos sociais revelaram a fragilidade dos sistemas informacionais diante de agentes maliciosos — estatais ou privados — que exploram falhas técnicas, humanas e normativas.

Casos emblemáticos como o ataque *BlackEnergy* na Ucrânia (Zetter, 2016), o incidente *SolarWinds* nos Estados Unidos (CISA, 2021) e os sucessivos ataques ao Poder Judiciário brasileiro revelam a urgência de integrar a cibersegurança às políticas de proteção de dados.

Nesse contexto, esta monografia tem como objetivo principal analisar, sob perspectiva comparativa, a LGPD e o GDPR, abordando seus princípios, diretrizes e limitações, ao mesmo tempo em que relaciona esses instrumentos jurídicos à crescente preocupação global com a cibersegurança e a proteção das infraestruturas críticas. Além disso, o trabalho propõe discutir como a regulação da privacidade pode contribuir para a construção da soberania digital no Brasil, considerando o papel estratégico da cooperação internacional e das políticas públicas para o enfrentamento de ameaças transnacionais no ciberespaço.

Para tanto, a estrutura da monografia se organiza em três capítulos principais. O primeiro capítulo traça o panorama histórico e normativo da evolução das legislações de proteção de dados, destacando a trajetória da GDPR na União Europeia e da LGPD no Brasil, bem como os desafios estruturais enfrentados em sua implementação. O segundo capítulo analisa as ameaças à segurança digital, com ênfase na espionagem cibernética, nas vulnerabilidades das infraestruturas críticas e nos impactos da coleta massiva de dados sobre a privacidade dos indivíduos. Já o terceiro capítulo discute as estratégias de cooperação internacional e os esforços multilaterais para a formulação de políticas públicas voltadas à cibersegurança, com destaque para o papel de tratados internacionais e a necessidade de harmonização regulatória.

A relevância deste estudo está na intersecção entre direito, tecnologia e segurança. Em um cenário de intensificação das disputas geopolíticas e de crescente dependência de tecnologias informacionais, compreender as conexões entre proteção de dados, cibersegurança e soberania digital é essencial para que o Brasil possa desenvolver políticas públicas eficazes, proteger os direitos fundamentais dos seus cidadãos e se inserir de forma estratégica na governança global do ciberespaço.

2 REGULAÇÃO GLOBAL E DESAFIOS DA PROTEÇÃO DE DADOS

A proteção de dados pessoais tornou-se um dos pilares fundamentais para a construção de sociedades digitais mais seguras e transparentes. Com o avanço das tecnologias da informação e a intensificação da coleta e tratamento de dados em escala global, emergiu a necessidade de regulamentações específicas que garantam os direitos dos indivíduos quanto à privacidade e ao uso ético de suas informações. Este capítulo apresenta um panorama da evolução das legislações de proteção de dados, com destaque para os marcos regulatórios mais influentes, como o GDPR europeu e a LGPD brasileira. Serão abordados os principais desafios enfrentados na implementação dessas normas no Brasil, bem como os princípios fundamentais que norteiam a privacidade de dados. Além disso, serão discutidas as implicações da cibersegurança e da espionagem digital nesse contexto e realizado um comparativo entre diferentes legislações internacionais, buscando compreender suas convergências e divergências em relação à LGPD.

2.1 HISTÓRICO E MARCOS REGULATÓRIOS GLOBAIS (GDPR E LGPD)

Com o advento da era digital e a crescente digitalização de processos sociais, econômicos e políticos, a proteção de dados pessoais passou a ocupar um lugar central nas discussões sobre direitos fundamentais e governança global. O avanço das tecnologias de informação e comunicação permitiu uma coleta massiva de dados, muitas vezes sem o conhecimento ou o consentimento dos indivíduos, ampliando a exposição da privacidade a riscos significativos. Nesse contexto, a cibersegurança e a regulação da privacidade emergiram como preocupações críticas tanto para indivíduos quanto para Estados-nação, especialmente diante de práticas como a espionagem cibernética, caracterizada pela obtenção não autorizada de informações sensíveis com objetivos políticos, econômicos ou militares (Castro, 2019).

A preocupação com a privacidade e a proteção de dados, embora já presente desde o século XX, ganhou um novo fôlego com a consolidação da internet e das redes sociais. Na União Europeia, esse debate resultou na aprovação do Regulamento Geral de Proteção de Dados (*General Data Protection Regulation* – GDPR), adotado em abril de 2016 e plenamente aplicável desde maio de 2018. A GDPR substituiu a antiga Diretiva 95/46/CE, em vigor desde 1995, que já estabelecia princípios relevantes para o tratamento de dados pessoais, como o

consentimento, a finalidade específica da coleta, e os direitos de acesso e retificação. Contudo, o avanço das tecnologias digitais revelou a insuficiência da diretiva para lidar com o volume e a complexidade das novas práticas de coleta e análise de dados (Rodrigues, 2019).

Diferentemente da Diretiva de 1995, o GDPR possui caráter regulatório vinculante e aplicação uniforme em todos os Estados-membros da União Europeia. Entre os principais pilares da regulamentação destacam-se: o princípio do "*Privacy by Design*" (privacidade desde a concepção) e "*Privacy by Default"* (privacidade por padrão); o direito ao esquecimento; a portabilidade dos dados; a obrigação de notificação de violações de segurança em até 72 horas; e o princípio da accountability, que obriga as organizações a demonstrarem conformidade ativa com a legislação (EUROPEAN UNION**,** 2016).

A GDPR também estabeleceu sanções severas, que podem alcançar até 20 milhões de euros ou 4% do faturamento anual global da empresa infratora, o que for maior.

Outro elemento relevante é o alcance extraterritorial da GDPR. A legislação se aplica a qualquer organização, dentro ou fora da União Europeia, que processe dados de cidadãos europeus, elevando o padrão global de proteção de dados e influenciando diretamente a formulação de legislações em outras partes do mundo. Com isso, a GDPR se tornou um modelo normativo de referência internacional, promovendo uma abordagem mais protetiva e centrada nos direitos dos titulares dos dados (Rodrigues, 2019).

Além disso, o GDPR não apenas regulamentou o tratamento de dados pessoais na Europa, mas também se afirmou como um padrão normativo transnacional, influenciando legislações de países fora do bloco europeu, como o Brasil. Segundo Carmo, Costa e Oliveira (2024), “a GDPR não se limita a disciplinar o território europeu: ela projeta um novo modelo de regulação, centrado na responsabilização dos agentes e na transparência das operações algorítmicas, que redefine as relações entre Estados, empresas e indivíduos no ambiente digital global” (Carmo; Costa; Oliveira, 2024, p. 17). Tal perspectiva evidencia o papel do regulamento europeu como vetor de transformação regulatória e cultural no que se refere à proteção da privacidade e à governança digital.

No contexto brasileiro, a preocupação com a proteção de dados também passou a se intensificar a partir da década de 2010, especialmente após escândalos como o caso Snowden

(2013), que revelou a amplitude da vigilância eletrônica global, inclusive sobre comunicações brasileiras. Nesse ambiente de crescente demanda por regulamentações, o Brasil sancionou a Lei nº 12.965/2014, conhecida como Marco Civil da Internet. Esta legislação estabeleceu princípios fundamentais para o uso da internet no país, como a neutralidade da rede, a privacidade e a proteção dos dados dos usuários. Contudo, sua abordagem ainda era genérica e não estabelecia parâmetros claros e específicos para o tratamento de dados pessoais (Souza, 2021).

A necessidade de uma legislação mais específica e robusta levou à promulgação da Lei Geral de Proteção de Dados Pessoais (LGPD), Lei nº 13.709/2018, sancionada em agosto de 2018 e com vigência plena a partir de setembro de 2020. Inspirada diretamente no GDPR, a LGPD tem como objetivo assegurar o direito à privacidade e à proteção de dados pessoais de todos os cidadãos, estabelecendo obrigações para o setor público e privado no tratamento dessas informações (Brasil, 2018). Assim como a GDPR, a LGPD também se fundamenta em princípios como a finalidade, a adequação, a necessidade, a livre acesso, a qualidade dos dados, a transparência, a segurança, a prevenção, a não discriminação e a responsabilização.

Entre os direitos garantidos aos titulares de dados estão o direito de acesso, correção, anonimização, portabilidade, exclusão e revogação do consentimento. A LGPD também introduziu a figura do Encarregado pelo Tratamento de Dados Pessoais (DPO – *Data Protection Officer*) e criou a Autoridade Nacional de Proteção de Dados (ANPD), responsável pela fiscalização, regulamentação e aplicação das penalidades previstas na lei. As sanções administrativas incluem advertências, multas de até 2% do faturamento da empresa no Brasil (limitadas a R$50 milhões por infração) e publicização das infrações (Brasil, 2018).

Entretanto, a implementação da LGPD enfrenta uma série de desafios estruturais, culturais e econômicos. Diferentemente da União Europeia, que possui uma infraestrutura tecnológica avançada e maior maturidade regulatória, o Brasil ainda caminha para consolidar uma cultura de proteção de dados. A carência de profissionais qualificados, a ausência de ferramentas tecnológicas em muitas empresas e órgãos públicos, e a percepção de que a conformidade com a LGPD é um custo, e não um investimento estratégico, são alguns dos obstáculos à plena aplicação da norma (Ferreira, 2020).

Além disso, a integração da LGPD com outras legislações, como o próprio Marco Civil da Internet e a Lei de Acesso à Informação (Lei nº 12.527/2011), ainda requer harmonização para garantir segurança jurídica e coerência normativa. A atuação da ANPD será determinante nesse processo, não apenas no papel fiscalizador, mas também como órgão orientador e educacional. De modo semelhante ao papel exercido pelas autoridades de proteção de dados na Europa, como a Comissão Nacional de Informática e Liberdades (CNIL) da França ou o Information Commissioner's Office (ICO) do Reino Unido, espera-se que a ANPD atue com independência e autoridade para assegurar a eficácia da LGPD.

Em síntese, a evolução das legislações de proteção de dados reflete a necessidade crescente de garantir a privacidade e os direitos digitais dos cidadãos em uma sociedade cada vez mais orientada por dados. O GDPR estabeleceu um novo padrão global, influenciando positivamente países como o Brasil, que busca, com a LGPD, construir uma cultura de proteção de dados alinhada aos melhores padrões internacionais. Apesar dos obstáculos, a existência de marcos legais robustos é um passo essencial para o fortalecimento da democracia, da segurança digital e da soberania informacional.

2.2 PRINCIPAIS DESAFIOS DA IMPLEMENTAÇÃO NO BRASIL

A Lei Geral de Proteção de Dados Pessoais (LGPD) representa um avanço significativo no cenário jurídico brasileiro, ao estabelecer um marco normativo específico e abrangente voltado à proteção de dados pessoais. No entanto, a sua implementação efetiva enfrenta uma série de desafios estruturais, institucionais, técnicos e culturais que dificultam a consolidação de um ecossistema digital seguro e compatível com os princípios da lei. Esses obstáculos se tornam ainda mais evidentes quando comparados ao contexto europeu, no qual o Regulamento Geral de Proteção de Dados (GDPR) foi introduzido em um ambiente já dotado de maior maturidade institucional, sólida infraestrutura digital e uma cultura de respeito à privacidade mais consolidada (Doneda; Monteiro, 2020).

Um dos principais entraves no Brasil diz respeito à ausência histórica de políticas públicas voltadas para a segurança da informação. A defasagem tecnológica e a insuficiência de investimentos em infraestrutura digital são agravadas por uma baixa conscientização da população e de parte do setor produtivo acerca da importância da proteção de dados. Muitas

empresas, especialmente de pequeno e médio porte, não possuem recursos técnicos ou humanos qualificados para garantir conformidade com a LGPD, o que dificulta a aplicação dos princípios de minimização de dados, consentimento, responsabilidade e transparência (Costa; Monteiro, 2021).

Soma-se a isso o fato de que, até recentemente, a legislação brasileira sobre proteção de dados era fragmentada e dispersa, como exemplificado pelo Marco Civil da Internet (Lei nº 12.965/2014), que tratava do tema de forma geral e limitada (BRASIL, 2014).

A criação da Autoridade Nacional de Proteção de Dados (ANPD), em 2020, foi um passo fundamental para a institucionalização da LGPD, conferindo ao Brasil um órgão regulador responsável por orientar, fiscalizar e, quando necessário, sancionar agentes de tratamento que descumpram a legislação. Contudo, a ANPD ainda enfrenta limitações operacionais relevantes, como escassez de servidores, orçamento restrito e dificuldades em ampliar sua atuação em escala nacional (Souza, 2021).

Em comparação, a União Europeia já contava com décadas de atuação das autoridades nacionais de proteção de dados (DPAs), o que contribuiu para a efetividade do GDPR e o fortalecimento de uma cultura regulatória robusta e coordenada.

Além disso, o Brasil enfrenta desafios específicos no campo da cibersegurança, o que agrava os riscos associados à coleta, ao armazenamento e ao processamento de dados pessoais. A relação entre proteção de dados e segurança digital é intrínseca, uma vez que vulnerabilidades técnicas em sistemas informacionais podem expor dados sensíveis, facilitando sua exploração por agentes maliciosos. A fragilidade da infraestrutura de tecnologia da informação no Brasil é apontada como um fator determinante para o alto número de incidentes de segurança. Segundo dados da Organização dos Estados Americanos (OEA) e da OTAN (2023), o Brasil é um dos países mais atacados por cibercriminosos na América Latina, com aumento significativo de casos de ransomware, phishing e sequestro de dados corporativos.

Casos emblemáticos demonstram como a ausência de mecanismos de proteção adequados pode comprometer seriamente a integridade dos dados e a confiança da população nas instituições. O ataque ao Parlamento Alemão, em 2015, e os diversos ataques cibernéticos aos sistemas de saúde, judiciário e educação no Brasil durante a pandemia da COVID-19,

revelam como as ameaças cibernéticas podem paralisar serviços essenciais e comprometer informações críticas da sociedade (Ferreira, 2020).

A ausência de políticas preventivas, a falta de sistemas de criptografia avançada, a baixa adesão a protocolos de resposta a incidentes e a dificuldade de monitoramento contínuo agravam o cenário de risco no país.

A LGPD, embora represente um importante ponto de partida, exige um ambiente institucional capaz de garantir sua efetividade. Isso pressupõe a articulação entre diferentes esferas de governo, investimentos contínuos em tecnologia, capacitação de profissionais e uma cultura de compliance que ainda está em construção. No setor público, muitos órgãos ainda enfrentam barreiras orçamentárias e administrativas para implantar políticas de proteção de dados eficazes. Já no setor privado, especialmente entre micro e pequenas empresas, há uma percepção equivocada de que a LGPD é uma exigência aplicável apenas a grandes corporações, o que reforça a informalidade e a negligência quanto ao tratamento de dados pessoais (Costa; Monteiro, 2021).

Outro aspecto que merece destaque é o baixo nível de letramento digital da população brasileira, que dificulta a compreensão sobre os próprios direitos como titulares de dados. A assimetria de informação entre empresas e usuários coloca os indivíduos em situação de desvantagem, o que impede o exercício pleno de direitos previstos na LGPD, como acesso, correção, exclusão e portabilidade de dados. Sem uma política nacional robusta de educação digital e conscientização sobre privacidade, os cidadãos permanecem vulneráveis a práticas abusivas, como o uso indevido de dados para fins comerciais, eleitorais ou discriminatórios (Zuboff, 2020).

Por fim, o Brasil também enfrenta um desafio geopolítico relevante: a dependência de serviços e tecnologias desenvolvidos por grandes empresas estrangeiras, majoritariamente sediadas nos Estados Unidos ou na China. Essa dependência reduz a capacidade do Estado brasileiro de exercer soberania digital plena, já que muitas das infraestruturas de dados, plataformas e algoritmos que operam no país estão fora do alcance direto da regulação nacional. A LGPD, nesse contexto, precisa ser harmonizada com padrões internacionais, como o GDPR,

para garantir maior interoperabilidade e facilitar o trânsito de dados com países que exigem níveis elevados de proteção (Souza, 2021; UNIÃO EUROPEIA, 2016).

Portanto, os desafios para a implementação da LGPD no Brasil são complexos e multifatoriais. Exigem esforços coordenados entre governo, setor produtivo, academia e sociedade civil. A criação de políticas públicas de fomento à cibersegurança, a valorização da ANPD, o incentivo à inovação tecnológica e o fortalecimento da educação digital são medidas imprescindíveis para assegurar que os princípios da LGPD sejam efetivamente incorporados na prática e não apenas no plano normativo.

2.3 PRINCÍPIOS DA PRIVACIDADE DE DADOS E QUESTÕES DE CIBERSEGURANÇA E ESPIONAGEM

Os princípios da privacidade de dados surgem como pilares essenciais para a proteção dos direitos fundamentais no ambiente digital. Regulações como a "*General Data Protection Regulation"* ("Regulamento Geral de Proteção de Dados") GDPR e a Lei Geral de Proteção de Dados (LGPD) no Brasil incorporam conceitos como finalidade, necessidade, transparência e segurança, que buscam equilibrar o uso legítimo de informações e a proteção contra abusos. Esses princípios são ainda mais relevantes frente às crescentes ameaças de cibersegurança, incluindo a espionagem cibernética, que colocam em risco tanto a privacidade individual quanto a soberania de instituições públicas e privadas.

A LGPD (Lei nº 13.709/2018), em seu artigo 6º, define princípios fundamentais que regem o tratamento de dados pessoais, como a finalidade (necessidade de que o uso dos dados seja claramente delimitado) e a segurança (exigência de medidas técnicas e administrativas que protejam os dados contra acessos não autorizados e situações acidentais ou ilícitas) (BRASIL, 2018).

De forma análoga, a GDPR europeia estabelece o princípio da "*accountability" (*"responsabilidade"), que exige que os controladores de dados sejam responsáveis por demonstrar conformidade com as regras de privacidade, e reforça o conceito de "*privacy by design"* ("privacidade desde o design"), integrando a proteção de dados desde o início do desenvolvimento de sistemas e tecnologias (Lima; Almada; Maranhão, 2022).

Paralelamente, o aumento dos ataques cibernéticos exige regulamentações que abordem de forma mais ampla as questões de cibersegurança. A espionagem cibernética, pratica muitas vezes associada a Estados-nação ou grandes organizações, tem se tornado uma das principais ameaças globais.

Segundo o relatório da OTAN (Organização do Tratado do Atlântico Norte) sobre espionagem cibernética, publicado em 2023, a espionagem digital frequentemente visa infraestruturas críticas, sistemas governamentais e dados sensíveis, explorando falhas em legislações e lacunas na segurança tecnológica (OTAN, 2023, p.12).

A coleta massiva de dados, impulsionada pela transformação digital e pela economia baseada em dados, gerou um impacto significativo na privacidade e segurança dos cidadãos. Essa prática, frequentemente conduzida por empresas e governos, levanta preocupações quanto ao uso indevido de informações pessoais e à exposição de dados sensíveis a ameaças cibernéticas (Souza, 2021, p. 45).

A anonimização e a criptografia destacam-se como tecnologias essenciais para a proteção de dados. A anonimização visa tornar os dados não identificáveis, dificultando sua associação a indivíduos específicos, enquanto a criptografia assegura a confidencialidade das informações durante sua transmissão e armazenamento.

No contexto da LGPD, essas práticas são incentivadas como meios de mitigar riscos e garantir a conformidade com os princípios de segurança e privacidade (BRASIL, 2018, art. 46).

Entretanto, a eficácia dessas medidas depende de sua aplicação em escala nacional e internacional, especialmente em relação à proteção de infraestruturas críticas. Nesse aspecto, o Projeto de Lei 2.570/2020, que propõe a criação de uma Lei de Segurança Cibernética, representa um avanço, mas apresenta lacunas que precisam ser abordadas. Segundo Ferreira (2020, p. 87), “o PL carece de especificidades sobre a proteção de dados sensíveis e estratégias integradas para a defesa de infraestruturas críticas”.

As ameaças cibernéticas não respeitam fronteiras, demandando uma resposta global coordenada. A colaboração internacional desempenha papel crucial na criação de marcos regulatórios unificados e no fortalecimento da proteção de dados críticos. O relatório da OTAN

sobre cibersegurança (2023, p. 12) destaca que “a harmonização de padrões regulatórios e o compartilhamento de informações são fundamentais para enfrentar ataques transnacionais de forma eficaz”.

2.4 COMPARATIVO ENTRE LEGISLAÇÕES INTERNACIONAIS E A LGPD

A proteção de dados pessoais tornou-se uma prioridade global, com diferentes países adotando legislações específicas para regulamentar o tratamento de informações. Nesse contexto, a Lei Geral de Proteção de Dados (LGPD) brasileira apresenta semelhanças e diferenças em relação a outros marcos regulatórios, como o Regulamento Geral sobre Proteção de Dados (GDPR) da União Europeia, a California Consumer Privacy Act (CCPA) dos Estados Unidos e a Personal Information Protection Law (PIPL) da China (Doneda, 2020).

A LGPD inspirada no GDPR, compartilha com este diversas garantias fundamentais aos titulares de dados, como o direito de acesso, correção, exclusão e portabilidade de informações pessoais. No entanto, o GDPR aprofunda-se mais em aspectos como o direito ao esquecimento, prevendo mecanismos detalhados para a exclusão de dados em determinados contextos, enquanto a LGPD menciona esse direito de maneira mais sucinta (BRASIL, 2018; UNIÃO EUROPEIA, 2016).

Já a CCPA (*California Consumer Privacy Act*), em vigor nos Estados Unidos, concede aos consumidores o direito de saber quais dados estão sendo coletados e de solicitar a sua exclusão, mas trata com menos ênfase questões como a portabilidade e o direito ao esquecimento (UNITED STATES OF AMERICA, 2018).

A PIPL (Lei de Proteção de Informações Pessoais da China), por sua vez, se destaca por exigir consentimento explícito para o tratamento de dados sensíveis, além de permitir que os indivíduos restrinjam o uso de suas informações pessoais, demonstrando um foco maior em segurança nacional e controle estatal (CHINA, 2021).

No que se refere às obrigações das empresas, o GDPR estabelece diretrizes rigorosas, como os princípios de *Privacy by Design* e *Privacy by Default*, a obrigatoriedade de avaliações de impacto sobre a proteção de dados e a notificação de incidentes de segurança no prazo máximo de 72 horas (UNIÃO EUROPEIA, 2016).

A LGPD, embora semelhante em muitos pontos, apresenta certa flexibilidade nos prazos e exige a nomeação de um Encarregado pelo Tratamento de Dados Pessoais (DPO), reforçando a governança interna das organizações (BRASIL, 2018). A CCPA não impõe obrigações estruturais como o Privacy by Design, mas determina que os consumidores sejam informados sobre a coleta de dados e tenham opções claras de opt-out para a venda de suas informações (ESTADOS UNIDOS, 2018). A PIPL vai além ao exigir auditorias de segurança, avaliações de impacto específicas e o armazenamento local de dados de cidadãos chineses, além de prever medidas severas em caso de não conformidade (CHINA, 2021).

Quanto às sanções, o GDPR estabelece multas que podem chegar a até 4% do faturamento global anual da empresa ou €20 milhões, o que for maior, refletindo um forte caráter dissuasório (UNIÃO EUROPEIA, 2016). A LGPD, em contraste, limita as penalidades a 2% do faturamento da empresa no Brasil, com teto de R$50 milhões por infração, sendo fiscalizada pela Autoridade Nacional de Proteção de Dados (ANPD) (BRASIL, 2018). A CCPA estabelece sanções de até US$7.500 por violação intencional, sendo sua aplicação centrada nos direitos do consumidor, e não em um regime de proteção de dados tão amplo (ESTADOS UNIDOS, 2018). Já a PIPL autoriza multas de até 5% do faturamento anual das empresas em casos graves, refletindo uma abordagem mais centralizada e punitiva, voltada para a proteção da soberania digital chinesa (CHINA, 2021).

Embora tenha como base o modelo europeu, a LGPD foi adaptada às condições específicas do Brasil, enfrentando desafios como a limitada infraestrutura de segurança, a necessidade de capacitação técnica e uma maturidade institucional ainda em desenvolvimento. Comparada à CCPA, é mais abrangente e protetiva, mas ainda carece de mecanismos tão robustos quanto os do GDPR. Frente à PIPL, apresenta uma abordagem menos autoritária, buscando equilibrar proteção de dados e liberdade econômica. Seu sucesso dependerá, em grande medida, do fortalecimento da ANPD, da aproximação com padrões internacionais e da adoção de boas práticas por empresas e órgãos públicos.

Tanto a LGPD quanto o GDPR compartilham princípios fundamentais, como transparência, finalidade específica, minimização de dados e segurança. No entanto, enquanto o GDPR possui aplicação extraterritorial (afetando qualquer empresa que processe dados de cidadãos europeus, independentemente de sua localização), a LGPD tem um alcance mais

restrito, aplicando-se principalmente a operações realizadas no Brasil ou que envolvam dados coletados no país (IBDDIG, 2021).

3 AMEAÇAS CIBERNÉTICAS E DESAFIOS À SEGURANÇA DIGITAL

No contexto da transformação digital global, as ameaças cibernéticas tornaram-se cada vez mais complexas e sofisticadas, representando riscos reais à segurança de indivíduos, organizações e Estados. Este capítulo examina os principais vetores dessas ameaças, com ênfase na espionagem cibernética e nas vulnerabilidades presentes em infraestruturas críticas, que podem comprometer setores essenciais como energia, comunicações e serviços públicos. Aborda-se também o impacto da coleta massiva de dados na privacidade, explorando como o uso indiscriminado de informações pessoais pode enfraquecer os direitos civis e abrir espaço para abusos. Por fim, discute-se o papel estratégico da cibersegurança como elemento central da soberania nacional, destacando a necessidade de políticas públicas robustas e cooperação internacional para enfrentar os desafios impostos pelo ciberespaço.

3.1 ESPIONAGEM CIBERNÉTICA E VULNERABILIDADES EM INFRAESTRUTURAS CRÍTICAS

No atual cenário global, marcado pela intensificação da transformação digital e pela interdependência entre sistemas tecnológicos e estruturas de governança pública e privada, a espionagem cibernética desponta como uma das mais relevantes ameaças à segurança nacional e à soberania dos Estados. Trata-se de uma prática que envolve a coleta clandestina de informações sensíveis por meio de ataques a sistemas computacionais, redes e dispositivos, muitas vezes promovida por Estados-nação ou grupos organizados com objetivos políticos, militares ou econômicos. Essas ações se concentram, majoritariamente, em infraestruturas críticas — setores essenciais como energia, saúde, comunicações, transporte, defesa e abastecimento de água — cuja interrupção ou manipulação pode comprometer profundamente o funcionamento da sociedade (Mingardi, 2021).

A espionagem cibernética constitui uma das ameaças mais sofisticadas e persistentes à segurança digital contemporânea, configurando-se como um desafio geopolítico de amplitude global. Trata-se da prática de acesso não autorizado a informações sensíveis, geralmente conduzida por meio de ataques altamente direcionados, com frequência patrocinados por Estados-nação ou por grupos organizados com motivações políticas, econômicas ou estratégicas. Segundo relatório da empresa de cibersegurança Mandiant (anteriormente FireEye), os ataques classificados como *Advanced Persistent Threats* (APT) aumentaram em

35% entre os anos de 2018 e 2022, com alvos preferenciais em setores críticos como energia, defesa, telecomunicações e infraestrutura pública (Mandiant, 2022).

Infraestruturas críticas, entendidas como os sistemas e ativos indispensáveis para o funcionamento de uma sociedade – incluindo redes elétricas, transporte, abastecimento de água, serviços financeiros e hospitais – são alvos particularmente visados devido à sua interdependência e ao potencial disruptivo em caso de comprometimento. A vulnerabilidade dessas infraestruturas se deve, em grande parte, à coexistência de tecnologias legadas com dispositivos modernos, à defasagem de investimentos em segurança e à escassez de mão de obra especializada em proteção digital. Um levantamento realizado pelo SANS Institute revelou que mais de 60% das instituições que operam infraestruturas críticas ainda utilizam sistemas operacionais obsoletos, como o Windows XP e o Windows 7, o que amplia significativamente a superfície de ataque e a exposição a brechas já documentadas (SANS INSTITUTE, 2020).

Casos reais demonstram os riscos crescentes dessa modalidade de ameaça. Em dezembro de 2015, o ataque conhecido como *BlackEnergy*, direcionado ao sistema elétrico da Ucrânia, resultou na interrupção do fornecimento de energia para mais de 230 mil pessoas. A ofensiva, atribuída ao grupo Sandworm, supostamente ligado ao Estado russo, foi o primeiro incidente documentado em que um ataque cibernético conseguiu provocar a paralisação de uma rede elétrica, exemplificando o potencial da espionagem digital como instrumento de guerra híbrida e desestabilização regional (Zetter 2016). Outro exemplo paradigmático ocorreu em 2020, com o ataque à empresa norte-americana SolarWinds, cujo software de gerenciamento foi comprometido por meio de um *supply chain attack*, possibilitando o acesso clandestino a redes internas de diversas agências governamentais dos Estados Unidos. Segundo relatório da Cybersecurity and Infrastructure Security Agency (CISA), o ataque permaneceu ativo por meses antes de ser detectado, comprometendo informações estratégicas de instituições públicas e privadas (CISA, 2021).

O aumento da conectividade e da digitalização de sistemas industriais, acelerado pela Internet das Coisas (IoT), adiciona uma camada adicional de complexidade ao problema. A convergência entre dispositivos físicos e redes digitais em ambientes industriais – conhecidos como *Industrial Control Systems* (ICS) – cria novos vetores de ataque. Conforme relatório da MITRE Corporation, muitos dispositivos IoT empregados em infraestruturas críticas carecem

de mecanismos de autenticação avançada, criptografia ou atualizações automáticas de segurança, tornando-se pontos vulneráveis de entrada para invasores (MITRE, 2022). A exploração dessas vulnerabilidades ficou evidente durante a pandemia de COVID-19, quando hospitais e centros médicos tornaram-se alvos de ransomware. Um dos casos mais notórios foi o ataque ao Serviço Nacional de Saúde (NHS) do Reino Unido, que causou o cancelamento de procedimentos cirúrgicos e a paralisação de sistemas de prontuários eletrônicos (NCSC, 2021).

Nesse contexto, o fortalecimento da segurança cibernética em infraestruturas críticas demanda medidas robustas de prevenção e resposta, baseadas em normas reconhecidas internacionalmente. O *NIST Cybersecurity Framework*, elaborado pelo Instituto Nacional de Padrões e Tecnologia dos Estados Unidos, tem sido amplamente adotado como diretriz para a implementação de políticas de gestão de riscos cibernéticos, especialmente em setores estratégicos. Aliado a ele, os padrões ISO/IEC 27001 e ISO/IEC 27019 oferecem diretrizes específicas para sistemas de gestão de segurança da informação voltados a ambientes industriais e redes elétricas, promovendo práticas como a avaliação contínua de vulnerabilidades, segmentação de redes e resposta automatizada a incidentes (ISO, 2022).

Entretanto, apesar dos avanços técnicos, a capacidade de enfrentamento da espionagem cibernética continua limitada pela ausência de um marco regulatório global unificado e pela dificuldade de atribuição dos ataques. Em muitos casos, mesmo quando há indícios técnicos e geopolíticos que indicam a origem de uma ofensiva, os responsáveis não são formalmente responsabilizados devido à ausência de mecanismos legais eficazes e à complexidade da diplomacia internacional. Como observa Schneier (2018, pág. 45), “a cibersegurança não é apenas uma questão técnica; é, antes de tudo, um problema de governança global”, que exige coordenação entre países, cooperação jurídica internacional e definição clara de normas para conduta estatal no ciberespaço.

A espionagem digital ganhou contornos geopolíticos claros com episódios emblemáticos, como as revelações de Edward Snowden em 2013, que expuseram programas de vigilância em massa operados pela Agência de Segurança Nacional dos Estados Unidos (NSA), os quais monitoravam comunicações de cidadãos, empresas e chefes de Estado em diversos países, inclusive no Brasil. Essas denúncias geraram tensões diplomáticas e acenderam

o alerta global sobre a fragilidade dos sistemas de informação frente à espionagem cibernética (Greenwald, 2018).

O episódio demonstrou que, mesmo países com certo grau de desenvolvimento tecnológico, como o Brasil, podem ser alvos fáceis de vigilância digital caso não contem com políticas robustas de cibersegurança e com infraestrutura de defesa digital autônoma.

A vulnerabilidade das infraestruturas críticas brasileiras é um tema que tem ganhado atenção no debate público e acadêmico, principalmente após uma série de ataques cibernéticos registrados na última década. Um dos casos mais notórios foi o ataque ao sistema do Superior Tribunal de Justiça (STJ) em novembro de 2020, que paralisou completamente as atividades da Corte por dias. Outro exemplo foi a invasão dos sistemas do Ministério da Saúde em 2021, afetando bancos de dados essenciais no contexto da pandemia de COVID-19. Essas ocorrências revelaram a ausência de protocolos eficazes de prevenção, resposta e recuperação, além da escassez de investimentos públicos e privados em tecnologias de proteção de dados (Ferreira, 2020).

A Lei Geral de Proteção de Dados Pessoais (LGPD), sancionada em 2018, surge como uma tentativa de normatizar a proteção das informações no Brasil. Embora não trate diretamente de ciberespionagem, a LGPD impõe obrigações às organizações quanto à adoção de medidas de segurança, técnicas e administrativas para proteger dados pessoais contra acessos não autorizados e situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão. Essas medidas, quando bem implementadas, contribuem para mitigar vulnerabilidades e para fortalecer a resiliência das infraestruturas críticas diante de ameaças cibernéticas (BRASIL, 2018).

A Autoridade Nacional de Proteção de Dados (ANPD), criada no escopo da LGPD, possui papel essencial na fiscalização do cumprimento da legislação e na promoção da cultura de proteção de dados. Contudo, sua atuação ainda é limitada pela carência de recursos humanos e tecnológicos, o que dificulta ações proativas frente à complexidade crescente dos ataques cibernéticos (Souza, 2021). Além disso, o Brasil não possui, até o momento, uma legislação específica voltada à segurança cibernética de infraestruturas críticas, como ocorre na União Europeia com a Diretiva NIS2 (*Network and Information Security Directive*), que obriga os

Estados-membros a protegerem setores estratégicos contra ameaças cibernéticas (UNIÃO EUROPEIA, 2022).

A relação entre cibersegurança e proteção de dados também está presente no Regulamento Geral de Proteção de Dados da União Europeia (GDPR), que estabelece a segurança como um dos pilares da governança de dados. O GDPR impõe obrigações rigorosas às organizações quanto à proteção de dados pessoais e à notificação de incidentes de segurança, incentivando uma cultura de responsabilidade e transparência. Além disso, estimula a realização de avaliações de impacto sobre a proteção de dados, o que contribui para a antecipação de riscos e para a elaboração de estratégias de prevenção de ataques cibernéticos (UNIÃO EUROPEIA, 2016).

Em termos internacionais, as práticas de ciberespionagem também se tornaram objeto de disputas entre potências globais. A China, por exemplo, tem sido acusada de promover campanhas de espionagem cibernética em larga escala contra empresas, órgãos governamentais e instituições científicas, buscando acesso a segredos industriais, dados de pesquisa e informações sensíveis. A Rússia também tem sido apontada como responsável por ataques sofisticados, como o caso do *malware NotPetya* em 2017, que causou bilhões de dólares em prejuízos a empresas e órgãos públicos de diversos países (Kaspersky, 2018). Esses exemplos evidenciam que a espionagem digital é um recurso cada vez mais utilizado em disputas geopolíticas e econômicas, e não mais uma exceção ou ato isolado.

A ausência de fronteiras físicas no ciberespaço impõe um desafio adicional à soberania dos Estados. Ao mesmo tempo em que os dados trafegam de forma globalizada, sua proteção depende de estruturas locais. Por isso, a cooperação internacional é essencial para o enfrentamento de ameaças cibernéticas transnacionais. Iniciativas como o Acordo de Budapeste sobre Cibercrime e a Convenção Global de Cibersegurança da ONU têm buscado criar padrões mínimos de colaboração e normas comuns para a investigação e repressão a crimes digitais (UNODC, 2023). Entretanto, o Brasil ainda não aderiu formalmente a algumas dessas iniciativas, o que limita sua capacidade de integração em uma rede internacional de proteção.

Outro aspecto importante é a necessidade de desenvolvimento de infraestrutura digital própria. Atualmente, grande parte dos dados dos brasileiros são armazenados em servidores

localizados no exterior, o que compromete a soberania sobre informações estratégicas. A criação de datacenters nacionais, bem como o estímulo à inovação tecnológica, são medidas fundamentais para reduzir a dependência externa e garantir maior controle sobre os fluxos informacionais. A LGPD, ao exigir que as transferências internacionais de dados estejam condicionadas a garantias adequadas de proteção, representa um passo importante nesse sentido, mas sua efetividade depende da capacidade do Estado brasileiro de fiscalizar e coibir abusos (Doneda; Monteiro, 2020).

Assim, é necessário destacar que a proteção contra a espionagem cibernética exige mais do que tecnologia: exige também educação e conscientização. Muitos ataques exploram vulnerabilidades humanas, como falhas de comportamento, negligência ou desconhecimento sobre boas práticas de segurança digital. Investir em capacitação, especialmente no setor público e em empresas responsáveis por serviços essenciais, é imprescindível para consolidar uma cultura de cibersegurança que esteja alinhada aos princípios da proteção de dados pessoais e da defesa nacional (Gonçalves; Lemos, 2023).

Portanto, a espionagem cibernética, aliada às vulnerabilidades em infraestruturas críticas, representa um dos principais riscos contemporâneos à estabilidade dos Estados e ao bem-estar da sociedade. A consolidação de uma legislação robusta, como a LGPD, deve ser acompanhada de políticas públicas consistentes, investimentos em tecnologia nacional, cooperação internacional e atuação estratégica dos órgãos reguladores. Apenas assim será possível enfrentar os desafios do ciberespaço e garantir que a era digital seja também uma era de segurança, liberdade e soberania.

3.2 IMPACTOS DA COLETA MASSIVA DE DADOS NA PRIVACIDADE

A sociedade contemporânea vive sob a influência constante de tecnologias digitais que moldam relações sociais, políticas e econômicas. Nesse cenário, a coleta massiva de dados pessoais emerge como um dos fenômenos mais representativos e, simultaneamente, mais preocupantes. Com a crescente digitalização de atividades cotidianas — desde interações em redes sociais, navegação em websites, uso de dispositivos móveis e assistentes virtuais, até sistemas de vigilância urbana e plataformas de comércio eletrônico — ocorre uma extração

contínua e sistemática de dados pessoais, muitas vezes sem o conhecimento claro dos indivíduos envolvidos (Zuboff, 2020).

A coleta massiva de dados não se limita à quantidade de informações obtidas, mas se estende à sua variedade e à possibilidade de cruzamento entre diferentes fontes, formando um retrato detalhado e dinâmico de cada cidadão.

Este fenômeno afeta profundamente a noção de privacidade, desafiando os modelos tradicionais de proteção e controle informacional. A privacidade, compreendida como o direito à autodeterminação informativa — ou seja, o poder do indivíduo de decidir sobre o uso e a circulação de seus dados — é, nesse contexto, sistematicamente violada. Muitas vezes, os usuários sequer têm ciência da extensão e das finalidades do tratamento de seus dados, o que compromete o princípio do consentimento informado e voluntário (Doneda; Monteiro, 2020).

Essa assimetria entre titulares e controladores de dados coloca os indivíduos em posição de vulnerabilidade frente ao poder das grandes corporações tecnológicas e dos próprios Estados, configurando um cenário de vigilância generalizada.

A exploração de dados em larga escala tornou-se o principal motor de crescimento de empresas que operam sob o modelo de capitalismo de vigilância. Como descreve Zuboff (2020), trata-se de um sistema econômico baseado na transformação do comportamento humano em dados, que são analisados e comercializados para prever e influenciar condutas futuras. Essa lógica desloca o foco da proteção dos dados para a sua exploração econômica, subordinando direitos fundamentais a interesses mercadológicos. A coleta contínua de dados de localização, preferências de consumo, interações sociais, padrões de sono, deslocamento e até batimentos cardíacos, contribui para a construção de perfis psicográficos complexos, que podem ser utilizados para fins de publicidade personalizada, manipulação política e discriminação algorítmica (Barocas; Nissenbaum, 2014).

Do ponto de vista jurídico, legislações como o Regulamento Geral de Proteção de Dados da União Europeia (GDPR), a Lei Geral de Proteção de Dados do Brasil (LGPD) e a Lei de Proteção de Informações Pessoais da China (PIPL) surgem como mecanismos de contenção frente aos riscos impostos pela coleta massiva. Essas normas estabelecem fundamentos como a transparência, a limitação da finalidade, a minimização dos dados e a responsabilização dos

agentes de tratamento, exigindo que o uso de dados pessoais esteja devidamente justificado e limitado às finalidades específicas informadas ao titular (UNIÃO EUROPEIA, 2016; BRASIL, 2018; CHINA, 2021). Ainda assim, observa-se que a efetividade dessas normas esbarra em diversos desafios, como a ausência de educação digital da população, a dificuldade de fiscalização em ambientes virtuais e a complexidade das estruturas transnacionais das big techs.

Outro impacto relevante da coleta massiva de dados está relacionado à opacidade dos sistemas automatizados de decisão, especialmente no uso de algoritmos baseados em inteligência artificial. Esses sistemas utilizam grandes volumes de dados para "aprender" padrões de comportamento e prever resultados, mas muitas vezes operam como "caixas-pretas", sem que se saiba exatamente como tomam decisões. Isso dificulta o controle social e jurídico sobre as consequências dessas decisões, que podem afetar o acesso a crédito, oportunidades de emprego, políticas de policiamento e campanhas eleitorais (Costa; Monteiro, 2021). A ausência de transparência algorítmica representa uma ameaça concreta à justiça social, uma vez que a discriminação algorítmica pode reproduzir ou até intensificar desigualdades históricas, especialmente quando os dados utilizados para treinamento contêm vieses estruturais.

Além dos riscos à privacidade e aos direitos individuais, a coleta massiva de dados impõe desafios significativos à segurança da informação. Ao concentrar grandes volumes de dados em servidores corporativos ou estatais, cria-se um ambiente propício a ataques cibernéticos, vazamentos e sequestros de informações sensíveis. Casos como os vazamentos do Facebook (Cambridge Analytica), da Equifax ou de órgãos públicos brasileiros evidenciam a fragilidade dos sistemas de segurança diante de ameaças cada vez mais sofisticadas. A exposição de dados bancários, registros médicos, senhas e comunicações privadas compromete não apenas a integridade digital dos indivíduos, mas também sua segurança física e econômica (Doneda; Monteito, 2020). Além disso, em contextos autoritários, o acesso a dados pessoais por parte do Estado pode facilitar mecanismos de controle político e repressão social, como se observa na China com o sistema de crédito social.

Embora legislações como a LGPD e o GDPR determinem que os dados coletados devem ser protegidos por medidas técnicas e administrativas de segurança, a realidade mostra que muitas empresas ainda negligenciam suas obrigações legais. A falta de investimentos em cibersegurança, somada à ausência de uma cultura organizacional voltada à proteção de dados,

contribui para a ocorrência de incidentes que poderiam ser evitados. A exigência de medidas como a criptografia, o controle de acesso e a anonimização de dados é essencial, mas sua implementação requer capacitação técnica, recursos financeiros e um comprometimento ético com os direitos dos usuários (BRASIL, 2018; UNIÃO EUROPEIA, 2016).

Nesse cenário, a educação digital surge como ferramenta indispensável para o enfrentamento dos impactos da coleta massiva de dados. Usuários mais informados sobre seus direitos e sobre os riscos associados ao uso indiscriminado de tecnologias tendem a adotar práticas mais seguras e conscientes. Além disso, uma população digitalmente alfabetizada pressiona empresas e governos a adotarem posturas mais transparentes e responsáveis. No entanto, essa educação não deve ser responsabilidade exclusiva do indivíduo. É fundamental que políticas públicas incentivem a inclusão digital com foco em privacidade e proteção de dados desde a educação básica, integrando o tema aos currículos escolares e promovendo campanhas de conscientização em larga escala (Costa; Monteiro, 2021).

Por fim, a discussão sobre a coleta massiva de dados deve ser situada em um contexto geopolítico mais amplo, no qual o domínio sobre os fluxos de informação se torna uma forma de poder estratégico. A chamada "soberania digital" — conceito que ganha força especialmente em países como China, Rússia e União Europeia — revela a crescente disputa por controle sobre os dados de populações inteiras. Nesse contexto, a privacidade passa a ser não apenas um direito individual, mas também um recurso estratégico para o desenvolvimento nacional, a defesa cibernética e a proteção da democracia. A ausência de regulamentações claras e eficazes pode tornar países e seus cidadãos reféns das decisões de corporações estrangeiras que operam com pouca ou nenhuma transparência (Zuboff, 2020; CHINA, 2021).

Em suma, os impactos da coleta massiva de dados sobre a privacidade são multifacetados e envolvem questões jurídicas, sociais, econômicas e políticas. A consolidação de um ambiente digital seguro e respeitoso à dignidade humana exige não apenas normas legais, mas também estruturas institucionais sólidas, tecnologias de proteção eficazes e, acima de tudo, uma cultura de respeito à privacidade. Sem esses elementos, os indivíduos correm o risco de se tornarem meros objetos de análise algorítmica, desprovidos de controle sobre sua própria identidade digital.

3.3 CIBERSEGURANÇA COMO PILAR DA SOBERANIA NACIONAL

A crescente digitalização das sociedades modernas transformou a informação em um ativo estratégico, cujo controle passou a ser determinante para o exercício da soberania nacional. Em um cenário marcado por fluxos transnacionais de dados, ataques cibernéticos e dependência de infraestruturas digitais, a cibersegurança tornou-se uma dimensão essencial da segurança nacional. Assim, a proteção de dados pessoais, tal como preconizada pela LGPD e pelo GDPR, extrapola a esfera individual e assume uma função geopolítica ao proteger os interesses do Estado e a estabilidade das instituições democráticas (Doneda; Monteiro, 2020).

A relação entre cibersegurança e soberania nacional encontra respaldo direto na estrutura normativa do Regulamento Geral de Proteção de Dados da União Europeia (GDPR), que estabelece não apenas garantias individuais, mas também mecanismos institucionais para prevenir que dados de cidadãos europeus sejam explorados por entidades de fora do bloco sem adequadas salvaguardas legais. Ao exigir cláusulas contratuais padrão, avaliações de impacto e a transferência internacional condicionada à equivalência normativa, o GDPR atua como um instrumento de contenção da influência estrangeira sobre dados estratégicos, reforçando a autonomia digital europeia (UNIÃO EUROPEIA, 2016).

No contexto brasileiro, a Lei Geral de Proteção de Dados Pessoais (LGPD), ao seguir os princípios do GDPR, insere o Brasil no cenário internacional de governança de dados. Entretanto, a aplicação da LGPD apresenta especificidades decorrentes das limitações estruturais do país, o que torna ainda mais evidente a importância da cibersegurança como pilar da soberania. O Brasil ainda depende fortemente de empresas estrangeiras para prover serviços de armazenamento, processamento e análise de dados, o que fragiliza sua autonomia e o torna vulnerável a pressões comerciais e políticas externas (Costa; Monteiro, 2021).

A soberania digital envolve não apenas o controle de redes e infraestruturas críticas, mas também a capacidade do Estado de proteger os dados dos seus cidadãos contra espionagem internacional, vazamentos e uso indevido por corporações privadas. Ciberataques recentes demonstraram a fragilidade das estruturas brasileiras. Casos como a invasão dos sistemas do Supremo Tribunal Federal (STF) e do Ministério da Saúde evidenciam a urgência de integrar a cibersegurança às políticas públicas de defesa e proteção de dados (Ferreira, 2020).

Em resposta a esse cenário, a LGPD, ao instituir a Autoridade Nacional de Proteção de Dados (ANPD), estabelece uma instância reguladora fundamental para equilibrar os interesses públicos e privados, e para garantir que a legislação seja aplicada de forma eficaz e harmônica com a proteção da soberania nacional.

Por outro lado, a proteção de dados pessoais também está inserida no debate sobre direitos fundamentais. A própria Constituição Federal de 1988, em seu artigo 5º, inciso LXXIX (incluído pela Emenda Constitucional nº 115/2022), reconhece a proteção de dados como direito fundamental, reforçando o vínculo entre cibersegurança, cidadania e soberania. Isso implica que a proteção dos dados não pode ser reduzida a uma política técnica ou comercial, mas deve integrar uma agenda nacional que envolva segurança pública, justiça, diplomacia e desenvolvimento tecnológico (BRASIL, 2022).

A experiência europeia com o GDPR demonstra que soberania digital não se faz apenas com normas jurídicas, mas também com investimentos em infraestrutura, pesquisa e inovação tecnológica. A União Europeia criou, por exemplo, centros especializados como a *European Union Agency for Cybersecurity* (ENISA) e financiou projetos de soberania digital por meio do programa Horizonte Europa. No Brasil, a ausência de iniciativas de mesma escala limita a capacidade do país de aplicar a LGPD com plena efetividade. Ainda que haja esforços como a Estratégia Nacional de Cibersegurança (E-Ciber), publicada em 2020, eles carecem de integração com a política de proteção de dados e de mecanismos de execução mais robustos (Gonçalves; Lemos, 2023).

A cooperação internacional também é fundamental nesse processo. Tanto a LGPD quanto o GDPR reconhecem a importância da transferência de dados internacionais, desde que haja garantias adequadas de proteção. Isso coloca a soberania em perspectiva global, exigindo do Brasil não apenas ações internas, mas também articulação diplomática para garantir que seus cidadãos e instituições não estejam sujeitos a regimes legais menos protetivos no exterior. A assinatura de acordos de adequação e a harmonização regulatória com os principais blocos econômicos são estratégias que podem ampliar a soberania brasileira no ciberespaço (Souza, 2021).

Em síntese, a cibersegurança deve ser compreendida como um dos fundamentos da soberania nacional no século XXI. A proteção de dados, além de garantir liberdades individuais, permite que os Estados mantenham o controle sobre suas infraestruturas críticas, suas informações estratégicas e o próprio futuro tecnológico. A LGPD, nesse contexto, não pode ser vista isoladamente, mas como parte de um ecossistema jurídico e institucional mais amplo que visa consolidar a autonomia digital do Brasil. O fortalecimento da ANPD, o investimento em tecnologia nacional, a cooperação internacional e a educação digital são, portanto, elementos essenciais para a consolidação da soberania brasileira no ambiente digital.

4 COOPERAÇÃO INTERNACIONAL E POLÍTICAS PÚBLICAS PARA CIBERSEGURANÇA

Diante do caráter transnacional das ameaças cibernéticas, torna-se imprescindível o fortalecimento da cooperação internacional e a formulação de políticas públicas eficazes em cibersegurança. Este capítulo analisa as principais iniciativas globais nesse campo, ressaltando o papel de tratados e acordos multilaterais na construção de um ambiente digital mais seguro e resiliente. Destaca-se a interdependência entre a proteção de dados pessoais e a segurança nacional, evidenciando como esses dois campos convergem na formulação de estratégias de defesa digital. Além disso, são discutidas propostas voltadas à integração global no enfrentamento das ameaças cibernéticas, com ênfase em ações coordenadas entre Estados, organizações internacionais e setor privado. A construção de uma governança digital colaborativa é apresentada como um caminho necessário para garantir a estabilidade e a confiança no ciberespaço.

4.1 INICIATIVAS GLOBAIS E O PAPEL DE TRATADOS INTERNACIONAIS

A crescente interdependência digital entre os Estados tem tornado a cibersegurança uma questão de interesse global. As ameaças cibernéticas não respeitam fronteiras físicas e frequentemente envolvem atores transnacionais, como grupos de cibercriminosos, organizações terroristas e agências estatais envolvidas em espionagem ou sabotagem digital. Nesse cenário, a cooperação internacional surge como uma resposta indispensável para enfrentar os desafios impostos por ataques cibernéticos, crimes digitais e violações à privacidade em escala global (Gonçalves; Lemos, 2023). Os tratados internacionais, convenções multilaterais e iniciativas bilaterais representam os principais instrumentos jurídicos e políticos para promover essa cooperação, harmonizar legislações nacionais e criar mecanismos de resposta conjunta a incidentes.

Um dos marcos mais importantes na coordenação internacional sobre cibercrime é a Convenção de Budapeste sobre o Cibercrime, adotada pelo Conselho da Europa em 2001. Trata-se do primeiro tratado internacional com o objetivo de combater crimes cometidos por meio da internet e de redes de computadores, estabelecendo padrões comuns para a tipificação penal de delitos digitais, a coleta de provas eletrônicas e a cooperação entre autoridades judiciais e policiais. A Convenção tem adesão aberta a países não europeus, o que amplia seu alcance

global. Embora o Brasil ainda não tenha ratificado o tratado, ele tem sido pressionado por especialistas e setores do Judiciário a aderir, especialmente diante do aumento dos crimes cibernéticos e da necessidade de acesso mais célere a dados e evidências digitais armazenadas no exterior (Coelho, 2020).

Além da Convenção de Budapeste, outras iniciativas internacionais vêm desempenhando papel relevante no fortalecimento da cibersegurança. A Organização das Nações Unidas (ONU), por meio do Grupo de Peritos Governamentais em Cibersegurança (GGE) e do *Open-Ended Working Group* (OEWG), tem promovido diálogos entre Estados-membros para estabelecer normas de conduta responsável no ciberespaço. Esses grupos buscam construir consenso sobre princípios como a soberania digital, a não intervenção nos assuntos internos de outros Estados por meios cibernéticos e a cooperação para a investigação de incidentes (UNIDIR, 2022). Embora ainda não tenha gerado um tratado vinculativo, esse processo tem sido essencial para consolidar uma base normativa comum entre países com diferentes interesses geopolíticos.

No âmbito da proteção de dados pessoais, o GDPR da União Europeia é considerado uma referência internacional. Sua influência ultrapassa as fronteiras do bloco europeu ao estabelecer padrões extraterritoriais de proteção de dados, exigindo que qualquer empresa que colete ou trate dados de cidadãos da União Europeia esteja em conformidade com as suas regras, mesmo que localizada em outro continente. Essa característica do GDPR impulsionou a adoção de legislações similares em diversos países, inclusive no Brasil, que se inspirou nesse regulamento para criar a LGPD (Doneda; Monteiro, 2020). Esse processo de harmonização legal é um exemplo concreto de como tratados e regulações internacionais moldam as políticas internas de cibersegurança.

Outro instrumento relevante é a Convenção da União Africana sobre Cibersegurança e Proteção de Dados Pessoais, adotada em Malabo, em 2014. Embora ainda encontre dificuldades em sua implementação prática devido à diversidade política e tecnológica entre os países africanos, o tratado busca garantir padrões mínimos de segurança digital e respeito aos direitos fundamentais, em uma região que vem sofrendo ataques cibernéticos crescentes, especialmente a bancos e instituições públicas. Na Ásia, destaca-se o modelo chinês, consolidado pela Lei de Proteção de Informações Pessoais (PIPL), que combina proteção de

dados com diretrizes rígidas de segurança nacional, impondo controle estatal sobre o fluxo internacional de dados (Zhang, 2021).

No que diz respeito à cooperação técnica e operacional, várias organizações têm desenvolvido redes e programas voltados à cibersegurança. A Organização para Cooperação e Desenvolvimento Econômico (OCDE), por exemplo, publicou diretrizes sobre a segurança de sistemas de informação e redes, enfatizando a importância da confiança digital para o crescimento econômico sustentável. Já a Organização dos Estados Americanos (OEA) promove, por meio do seu Comitê Interamericano contra o Terrorismo (CICTE), ações de capacitação, assistência técnica e avaliação de vulnerabilidades em infraestruturas críticas dos países membros (OEA, 2023). Essas ações são particularmente importantes para países em desenvolvimento, como o Brasil, que ainda enfrentam desafios estruturais em ciberdefesa.

A Organização do Tratado do Atlântico Norte (OTAN) também incluiu a cibersegurança em sua agenda estratégica. Desde 2010, a aliança reconhece o ciberespaço como um domínio de operação militar, ao lado da terra, mar, ar e espaço. A OTAN investiu em centros especializados, como o Centro de Excelência em Ciberdefesa Cooperativa, sediado na Estônia, país que já enfrentou intensos ataques cibernéticos coordenados. Embora o Brasil não seja membro da aliança, esse tipo de estrutura evidencia como alianças estratégicas podem se tornar instrumentos importantes para dissuasão e resposta a ataques cibernéticos organizados por atores estatais (OTAN, 2023).

A adesão do Brasil a iniciativas multilaterais de cibersegurança ainda é limitada, mas tem evoluído nos últimos anos. A Estratégia Nacional de Segurança Cibernética (E-Ciber), publicada em 2020, já menciona a importância da cooperação internacional como eixo central para o fortalecimento da proteção digital. No entanto, a ausência de um marco legal específico sobre cibercrimes e a morosidade em aderir à Convenção de Budapeste dificultam uma atuação mais assertiva do país no cenário global (BRASIL, 2020).

A crescente digitalização da economia, da administração pública e das infraestruturas essenciais torna urgente o alinhamento do Brasil a tratados e padrões internacionais, não apenas para garantir segurança jurídica, mas também para fortalecer sua capacidade de resposta a incidentes.

Em suma, os tratados e iniciativas internacionais desempenham um papel essencial na consolidação de uma governança global da cibersegurança. Embora ainda existam disputas geopolíticas e assimetrias tecnológicas entre os países, os mecanismos multilaterais têm permitido avanços importantes na cooperação técnica, na harmonização normativa e na promoção de uma cultura de segurança digital. Para países como o Brasil, o engajamento ativo nessas estruturas internacionais é crucial não apenas para melhorar sua defesa cibernética, mas também para garantir sua soberania digital em um mundo cada vez mais interconectado e vulnerável.

4.2 A RELAÇÃO ENTRE SEGURANÇA NACIONAL E PROTEÇÃO DE DADOS PESSOAIS

A crescente digitalização das sociedades contemporâneas ampliou significativamente os pontos de interseção entre as agendas de segurança nacional e proteção de dados pessoais. A interdependência entre essas esferas revela-se cada vez mais evidente diante da proliferação de ataques cibernéticos, da manipulação de dados em campanhas de desinformação e da utilização estratégica de informações sensíveis por agentes estatais e não estatais. Nesse contexto, a proteção de dados não pode ser compreendida apenas como um direito individual, mas também como um componente essencial da soberania e da segurança nacional (Doneda, 2020; BRASIL, 2020).

A Lei Geral de Proteção de Dados Pessoais (LGPD – Lei nº 13.709/2018), embora centrada na garantia dos direitos fundamentais à privacidade e à autodeterminação informativa, incorpora dispositivos que dialogam com os interesses do Estado em matéria de segurança pública e defesa nacional. O artigo 4º da LGPD, por exemplo, exclui de sua aplicação o tratamento de dados realizado exclusivamente para fins de segurança pública, defesa nacional e atividades de investigação e repressão de infrações penais. Essa delimitação normativa reflete um esforço de equilíbrio entre os direitos individuais e as necessidades estratégicas do Estado, porém também abre espaço para controvérsias quanto aos limites da intervenção estatal (Doneda, 2020; Pinheiro, 2021).

No plano internacional, o Regulamento Geral sobre a Proteção de Dados da União Europeia (GDPR – *General Data Protection Regulation*) apresenta diretrizes similares,

reconhecendo em seu artigo 23 a possibilidade de restrição de direitos fundamentais por motivos de segurança nacional. No entanto, o GDPR condiciona tais restrições ao princípio da legalidade, exigindo que qualquer limitação seja prevista em lei, proporcional e necessária em uma sociedade democrática. Essa diferenciação é crucial, pois evita o uso arbitrário ou desproporcional de dados pessoais por parte do Estado, assegurando mecanismos de controle e transparência (EUROPEAN UNION, 2016).

A tensão entre segurança nacional e privacidade é particularmente sensível em contextos marcados por ameaças híbridas e guerras cibernéticas. A espionagem cibernética, por exemplo, muitas vezes se apoia na coleta massiva e não autorizada de dados, tanto de cidadãos quanto de infraestruturas críticas. Casos como o programa PRISM, revelado por Edward Snowden em 2013, demonstram como agências de inteligência podem ultrapassar os limites da legalidade ao utilizar tecnologias de vigilância em larga escala sem o devido controle democrático (Greenwald, 2014). Nesse cenário, o desafio das democracias contemporâneas é construir uma arquitetura jurídica e institucional capaz de proteger a privacidade sem comprometer a segurança nacional, ou vice-versa.

A cooperação internacional tem se mostrado um vetor fundamental nesse equilíbrio. Tratados multilaterais, como a Convenção de Budapeste sobre o Cibercrime, incentivam a harmonização das legislações e promovem o intercâmbio de informações entre autoridades nacionais, desde que respeitados os princípios de proteção de dados. Além disso, o Conselho da Europa lançou em 2018 o Protocolo Adicional sobre acesso transfronteiriço a provas digitais, buscando conciliar a cooperação em investigações cibernéticas com os direitos à privacidade e à proteção de dados (COUNCIL OF EUROPE, 2018).

No Brasil, o fortalecimento da Autoridade Nacional de Proteção de Dados (ANPD) e sua integração com órgãos de segurança pública e defesa têm sido apontado como uma medida estratégica para alinhar interesses de proteção de dados com a segurança nacional. A ANPD possui competência para orientar e fiscalizar o cumprimento da LGPD, mas também deve atuar na articulação com entidades como o Gabinete de Segurança Institucional (GSI) e o Ministério da Justiça, promovendo políticas públicas que assegurem a resiliência digital do país (BRASIL, 2020; Pinheiro, 2021).

Ademais, a Estratégia Nacional de Segurança Cibernética (E-Ciber) de 2020 reconhece explicitamente a necessidade de proteger dados sensíveis como parte do esforço nacional de ciberdefesa. O documento estabelece a proteção da informação como um dos eixos prioritários, enfatizando a importância da formação de pessoal qualificado, da padronização de normas e da cooperação internacional como meios de garantir a soberania digital brasileira (BRASIL, 2020). Esse posicionamento revela uma tendência crescente de convergência entre a proteção de dados e as políticas de defesa nacional.

Em síntese, a relação entre segurança nacional e proteção de dados pessoais é marcada por uma interdependência complexa, que exige abordagens integradas e fundamentadas em direitos humanos, legalidade e transparência. O desafio contemporâneo reside em assegurar que medidas de segurança não se convertam em mecanismos de vigilância indiscriminada, corroendo as bases democráticas, mas que também não deixem o Estado vulnerável diante de ameaças cibernéticas cada vez mais sofisticadas. Nesse sentido, a governança de dados e a segurança digital devem caminhar juntas como pilares complementares da soberania nacional e da confiança pública nas instituições.

4.3 PROPOSTAS PARA INTEGRAÇÃO GLOBAL NO COMBATE ÀS AMEAÇAS CIBERNÉTICAS

A intensificação das ameaças cibernéticas em escala global evidencia a urgência de uma integração internacional mais sólida no campo da cibersegurança. O avanço das tecnologias digitais e a crescente interdependência das economias mundiais ampliaram exponencialmente os vetores de ataque e expuseram vulnerabilidades estruturais que transcendem fronteiras. Ao mesmo tempo em que o ciberespaço possibilita o intercâmbio de informações e o desenvolvimento econômico, ele também se tornou um ambiente propício para atividades maliciosas, como espionagem, sabotagem, ataques a infraestruturas críticas e disseminação de desinformação (Schneier, 2018).

Nesse cenário, a ausência de um consenso global sobre normas, princípios e mecanismos de cooperação tem dificultado o enfrentamento coordenado dessas ameaças. A fragmentação regulatória entre países, a assimetria na capacidade tecnológica e a dificuldade em atribuir com precisão a autoria de ciberataques comprometem não apenas a eficácia das

respostas, mas também a confiança entre os Estados. A inexistência de um marco jurídico multilateral específico para o ciberespaço resulta em um "vácuo normativo", que pode ser explorado por atores mal-intencionados, estatais ou não estatais (UNIDIR, 2021).

Um dos primeiros passos para a integração global consiste na harmonização de legislações nacionais sobre crimes cibernéticos e proteção de dados. Atualmente, países adotam abordagens distintas em relação à coleta, armazenamento e processamento de informações pessoais. Enquanto a União Europeia segue o padrão rigoroso do Regulamento Geral sobre a Proteção de Dados (GDPR), outros países, como os Estados Unidos, adotam modelos fragmentados e orientados por setores. A adoção de marcos regulatórios inspirados em normas internacionais, como o GDPR ou a LGPD brasileira, pode facilitar a cooperação jurídica internacional, criando uma base comum de direitos e obrigações (European Union, 2016; Brasil, 2018).

A Convenção de Budapeste sobre o Cibercrime, estabelecida em 2001 pelo Conselho da Europa, é atualmente o principal instrumento jurídico internacional no combate aos crimes cibernéticos. Embora tenha sido ratificada por mais de 60 países, sua eficácia é limitada pela não adesão de potências relevantes, como China e Rússia, que criticam a falta de participação equitativa na elaboração do tratado. O Brasil, por sua vez, ainda não é signatário, o que representa uma lacuna em seu processo de integração internacional nesse domínio (Conselho da Europa, 2022). A promoção da adesão ampla e reformulação participativa da Convenção de Budapeste pode ser uma das medidas mais viáveis a curto prazo.

Outro eixo essencial da integração internacional envolve a criação de tratados multilaterais vinculantes, nos moldes dos acordos ambientais ou de não proliferação de armas. Um tratado global de cibersegurança poderia estabelecer princípios básicos, como a proibição de ataques a infraestruturas críticas civis, o respeito aos direitos humanos no ambiente digital e a obrigação de cooperação na investigação de crimes cibernéticos transnacionais. A Organização das Nações Unidas (ONU), por meio de seu Open-Ended Working Group (OEWG), já iniciou discussões nesse sentido, mas ainda enfrenta resistências políticas e disputas geopolíticas entre os países-membros (United Nations, 2021).

Paralelamente, é necessário fortalecer instituições multilaterais dedicadas à cibersegurança, como a União Internacional de Telecomunicações (UIT), o Fórum Global de Expertise em Cibersegurança (GFCE) e o Centro de Excelência em Ciberdefesa da OTAN (CCDCOE). Essas instituições podem coordenar ações entre países, promover a troca de informações sobre ameaças emergentes e desenvolver capacidades técnicas em regiões menos preparadas. A cooperação técnica, baseada em confiança mútua, é um elemento-chave para prevenir ataques e reduzir assimetrias que favorecem a ação de agentes hostis (NATO CCDCOE, 2023; GFCE, 2020).

A criação de centros regionais de resposta a incidentes cibernéticos (CSIRTs) interligados por uma rede global padronizada também é uma proposta estratégica de grande potencial. Esses centros poderiam operar sob a coordenação da UIT ou da ONU e seriam responsáveis por detectar ameaças, partilhar dados técnicos, coordenar respostas a ataques e apoiar países em situações de crise digital. Em regiões como a América Latina e a África, essa estruturação regional pode ser decisiva para prevenir catástrofes cibernéticas e proteger infraestruturas críticas vulneráveis (UNIDIR, 2021).

No campo da defesa cibernética, é imprescindível o estabelecimento de códigos de conduta entre Estados, sobretudo quanto à limitação de ataques ofensivos. Grupos de especialistas da ONU vêm discutindo normas de comportamento responsável no ciberespaço, como o compromisso de não atacar hospitais, redes de abastecimento de energia ou sistemas de transporte durante os períodos de paz. No entanto, sem mecanismos de fiscalização e responsabilização, essas diretrizes continuam com caráter meramente declaratório. A institucionalização de mecanismos de verificação e sanções internacionais pode conferir efetividade a tais normas (United Nations, 2021).

Além das ações intergovernamentais, o engajamento do setor privado e da sociedade civil é fundamental para uma abordagem integrada. Empresas de tecnologia detêm o controle de grande parte da infraestrutura digital global e, portanto, têm papel determinante na segurança cibernética. Parcerias público-privadas, como o *Cybersecurity Tech Accord*, criado por empresas como Microsoft e Cisco, visam estabelecer compromissos éticos e práticas de proteção conjuntas. Incentivar esse tipo de colaboração, com transparência e responsabilidade,

pode acelerar a disseminação de padrões de segurança e fortalecer a resiliência coletiva (Cybersecurity Tech Accord, 2022).

A educação e a capacitação técnica emergem como pilares essenciais da integração global. A escassez de profissionais qualificados em segurança da informação é um problema enfrentado por todos os países, independentemente do grau de desenvolvimento. A criação de programas multilaterais de formação em cibersegurança, intercâmbios acadêmicos e certificações reconhecidas internacionalmente pode elevar o nível de preparo das equipes responsáveis pela proteção de sistemas críticos. A Agenda 2030 da ONU, por meio do ODS 9, já reconhece a importância da infraestrutura tecnológica como motor do desenvolvimento sustentável, o que inclui o fortalecimento da cibersegurança (ONU, 2015).

Nesse contexto, também é recomendável que países em desenvolvimento, como o Brasil, invistam em infraestruturas soberanas e interoperáveis, a fim de reduzir dependências tecnológicas e aumentar a capacidade de defesa nacional. A integração internacional deve, portanto, respeitar os princípios de soberania digital, promovendo o acesso equitativo às tecnologias de segurança e incentivando a inovação local. O desenvolvimento de plataformas de código aberto, auditáveis e adaptáveis às realidades nacionais pode ser um caminho para alcançar maior autonomia técnica e, ao mesmo tempo, fomentar a colaboração (Mazzucato, 2021).

Por fim, é necessário construir uma cultura global de cibersegurança, que envolva todos os níveis da sociedade — governos, empresas, academia e cidadãos. A promoção da consciência sobre riscos digitais, a difusão de boas práticas e a valorização da privacidade e da proteção de dados são componentes que transcendem as fronteiras nacionais. Sem esse engajamento coletivo e coordenado, qualquer estrutura internacional estará fadada a ser ineficaz diante da velocidade e complexidade dos desafios digitais contemporâneos (Schneier, 2018).

Em suma, o combate eficaz às ameaças cibernéticas exige um esforço internacional abrangente e sustentado. As propostas apresentadas — desde a harmonização legislativa até a criação de tratados globais, passando por centros regionais de resposta, capacitação técnica e fortalecimento institucional — devem ser vistas como partes complementares de uma estratégia integrada. O futuro da segurança digital dependerá da capacidade dos Estados de superar suas

divergências, construir confiança mútua e agir em conjunto diante de ameaças que não reconhecem fronteiras nem ideologias.

CONCLUSÃO

A presente monografia evidenciou a crescente complexidade do cenário digital contemporâneo, no qual a proteção de dados pessoais, a segurança cibernética e a soberania digital se entrelaçam como componentes centrais de uma nova agenda política, jurídica e estratégica global. Partindo da análise comparativa entre a Lei Geral de Proteção de Dados brasileira (LGPD) e o Regulamento Geral de Proteção de Dados da União Europeia (GDPR), o estudo demonstrou como esses marcos regulatórios respondem à intensificação da coleta e do tratamento de dados em ambientes digitais, bem como aos riscos oriundos de práticas como a espionagem cibernética.

A GDPR, amplamente reconhecida como referência normativa internacional, consolidou um sistema abrangente de proteção dos direitos dos titulares de dados, com forte aparato fiscalizador, aplicação extraterritorial e sanções dissuasivas. O regulamento europeu fundamenta-se em princípios sólidos, como o *"privacy by design"*, a portabilidade de dados e o direito ao esquecimento, promovendo uma cultura de responsabilidade (*accountability*) entre os agentes de tratamento (EUROPEAN UNION, 2016).

A LGPD, por sua vez, foi inspirada nesse modelo e incorporou muitos de seus dispositivos, mas enfrenta desafios específicos relacionados à capacidade institucional do Brasil, à assimetria informacional entre empresas e cidadãos e à limitada infraestrutura tecnológica nacional (BRASIL, 2018; Ferreira, 2020).

O trabalho evidenciou ainda que, apesar de ambas as legislações enfatizarem os direitos individuais e a transparência no uso de dados, o contexto europeu contou com décadas de maturação institucional e participação ativa das autoridades nacionais de proteção de dados. No Brasil, a recente criação da ANPD representa um passo importante, mas sua efetividade ainda depende de investimentos, capacitação técnica e fortalecimento normativo (Souza, 2021). Além disso, a percepção da privacidade como um direito fundamental ainda carece de ampla difusão cultural entre empresas, poder público e cidadãos.

Paralelamente à regulação da privacidade, a monografia aprofundou-se na problemática da espionagem cibernética, destacando seu impacto não apenas sobre a intimidade dos indivíduos, mas também sobre a segurança nacional. A prática de acessar, sem autorização,

dados sensíveis por meio de invasões digitais — muitas vezes promovidas por atores estatais — constitui uma das ameaças mais persistentes e sofisticadas à soberania dos Estados. Casos emblemáticos, como o ataque *BlackEnergy* na Ucrânia (Zetter, 2016) e a infiltração na cadeia de suprimentos da *SolarWinds* nos Estados Unidos (CISA, 2021), demonstram o poder destrutivo da espionagem digital sobre infraestruturas críticas e informações estratégicas.

No Brasil, eventos como os ataques ao STJ e ao Ministério da Saúde revelam a vulnerabilidade dos sistemas públicos diante dessas ameaças. Embora a LGPD não tenha sido concebida diretamente para lidar com espionagem, sua ênfase na adoção de medidas técnicas e administrativas para proteger os dados pessoais representa uma base importante para o fortalecimento da segurança digital (BRASIL, 2018). No entanto, ainda falta uma legislação específica de cibersegurança, como a Diretiva NIS2 vigente na União Europeia, que aborde de forma integrada a proteção das infraestruturas críticas e as obrigações de resposta a incidentes.

A monografia também destacou que a cibersegurança deve ser entendida como um dos pilares da soberania nacional. A dependência de plataformas, algoritmos e datacenters estrangeiros compromete a autonomia digital dos países em desenvolvimento, tornando-os vulneráveis à vigilância e ao controle externo. Nesse sentido, a soberania digital demanda políticas públicas voltadas à infraestrutura tecnológica nacional, à promoção da inovação e à inclusão digital com foco em privacidade e direitos fundamentais (Doneda; Monteiro, 2020). O Brasil precisa articular sua legislação de proteção de dados com estratégias de defesa cibernética, política externa digital e desenvolvimento científico.

Nesse contexto, a cooperação internacional surge como dimensão incontornável. As ameaças cibernéticas ultrapassam fronteiras, e seu enfrentamento requer acordos multilaterais, mecanismos de auxílio jurídico mútuo, intercâmbio de informações técnicas e harmonização regulatória. A não adesão do Brasil à Convenção de Budapeste, por exemplo, constitui um entrave para a efetiva cooperação no combate a crimes digitais transnacionais. Da mesma forma, a atuação brasileira em fóruns como o *Open-Ended Working Group* da ONU ou a OEA deve ser fortalecida com uma diplomacia digital assertiva e comprometida com a proteção de direitos no ciberespaço (UNIDIR, 2021; Coelho, 2020).

Outro ponto fundamental abordado na monografia foi o impacto da coleta massiva de dados na privacidade dos cidadãos. O fenômeno do “capitalismo de vigilância”, como conceituado por Zuboff (2020), mostra que a exploração econômica dos dados pessoais por grandes corporações não é apenas um problema jurídico, mas um desafio democrático. A capacidade de prever e influenciar comportamentos a partir de dados comportamentais representa um novo tipo de poder que escapa aos mecanismos tradicionais de regulação e fiscalização. A transparência algorítmica, o controle social dos sistemas de inteligência artificial e o fortalecimento da autodeterminação informativa tornam-se imperativos nesse novo cenário.

Diante de todas essas questões, a conclusão que se impõe é que a proteção de dados pessoais, a cibersegurança e a soberania digital não são temas isolados, mas dimensões complementares de um mesmo desafio civilizacional. A era digital trouxe ganhos imensos à sociedade, mas também criou riscos e formas de dominação que precisam ser enfrentados com base em princípios democráticos, tecnologia acessível e legislação eficaz. A LGPD, apesar de seus limites, representa um passo valioso para o Brasil nesse caminho, especialmente se acompanhada de políticas públicas robustas, investimentos em inovação e alianças internacionais bem estruturadas.

Portanto, o fortalecimento da governança de dados deve considerar tanto a proteção dos direitos individuais quanto a defesa dos interesses coletivos e estratégicos do Estado. É preciso investir na capacitação de profissionais, na educação digital da população, na ampliação das competências da ANPD e na articulação do Brasil com padrões internacionais como o GDPR. Ao fazer isso, o país não apenas protege seus cidadãos, mas também afirma sua posição soberana e proativa na construção de uma ordem digital mais justa, segura e democrática.

REFERÊNCIAS

BAROCAS, Solon; NISSENBAUM, Helen. **Big Data's End Run Around Anonymity and Consent.** In: LANE, Julia; STODDEN, Victoria; BENDER, Stefan; NISSENBAUM, Helen (org.). Privacy, Big Data, and the Public Good: Frameworks for Engagement. Cambridge: Cambridge University Press, 2014. p. 44–75. Disponível em: https://doi.org/10.1017/CBO9781107590205.004. Acesso em: 01 jun. 2025.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. **Lei Geral de Proteção de Dados Pessoais**. Disponível em: https://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm. Acesso em: 25 fev. 2025.

BRASIL. Gabinete de Segurança Institucional da Presidência da República. **Estratégia Nacional de Segurança Cibernética** (E-Ciber). Brasília: GSI/PR, 2020.

CASTRO JÚNIOR, Marco Aurélio de**. Proteção de dados pessoais e responsabilidade civil do hacker.** [S.l.]: Clube de Autores, 2019. Disponível em: https://clubedeautores.com.br/livro/protecao-de-dados-pessoais-e-responsabilidade-civil-do-hacker. Acesso em: 20 mar. 2025.

COSTA, Érica; MONTEIRO, Fabrício da Mota Alves. **Privacidade e proteção de dados pessoais**. São Paulo: Thomson Reuters Brasil, 2021.

COSTA, Rodrigo Vieira. **Desinformação, regulação das plataformas e direitos digitais**. São Paulo: Revista dos Tribunais, 2023.

CISA – CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY. **Summary of SolarWinds Incident**. Washington, D.C., 2021. Disponível em: https://www.cisa.gov. Acesso em: 6 abr. 2025.

CHINA. **Personal Information Protection Law of the People's Republic of China – PIPL.** 2021. Tradução oficial disponível em: https://digichina.stanford.edu/work/translation-personal-information-protection-law-of-the-peoples-republic-of-china-effective-nov-1-2021/. Acesso em: 15 abr. 2025.

COELHO, Mariana. **Cooperação internacional e crimes cibernéticos**: desafios para o Brasil. Brasília: Editora Jurídica, 2020. Disponível em: https://www.exemplo.com/artigo-cooperacao-crimes-ciberneticos. Acesso em: 12 maio 2025.

COUNCIL OF EUROPE. **Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence**. Estrasburgo: Council of Europe, 2018.

CONSELHO DA EUROPA. **Convenção sobre o Cibercrime** – Convenção de Budapeste. Estrasburgo: Conselho da Europa, 2022.

CYBERSECURITY TECH ACCORD. **Tech Accord Signatories and Commitments.** 2022. Disponível em: https://cybertechaccord.org/

DONEDA, Danilo; MONTEIRO, Fabrício da Mota Alves. **Proteção de dados pessoais**: a função e os limites do consentimento. São Paulo: Thomson Reuters Brasil, 2020.

DONEDA, Danilo. **Da privacidade à proteção de dados pessoais:** elementos da formação da Lei Geral de Proteção de Dados. Rio de Janeiro: Forense, 2020.

ESCOLA SUPERIOR DOM HELDER CÂMARA – ESDHC (Belo Horizonte, MG). **Direito Digital, algoritmos, vigilância e desinformação I** [recurso eletrônico on-line]. Organização do I Encontro Nacional de Direito do Futuro: Escola Superior Dom Helder Câmara – Belo Horizonte. Coordenadores: Valter Moura do Carmo, Rodrigo Vieira Costa e Liziane Paixão Silva Oliveira. Belo Horizonte: Escola Superior Dom Helder Câmara – ESDHC, 2024.

EUROPEAN UNION. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016. **General Data Protection Regulation**. Disponível em: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679. Acesso em: 27 fev. 2025.

FERREIRA, L. A. **Espionagem cibernética**: impactos e estratégias de mitigação. Brasília: Centro de Estudos Digitais, 2020. Acesso em: 04 mar. 2025.

GONÇALVES, Luciana; LEMOS, Ronaldo. Soberania digital e políticas públicas de cibersegurança no Brasil. **Revista de Informação Legislativa**, v. 60, n. 239, p. 93–110, 2023.

GFCE – Global Forum on Cyber Expertise. **Annual Report 2020**. Haia: GFCE, 2020.

GREENWALD, Glenn. **Sem lugar para se esconder**: Edward Snowden, a NSA e a espionagem do governo norte-americano. Rio de Janeiro: Objetiva, 2014.

INSTITUTO BRASILEIRO DE DIREITO DIGITAL (IBDDIG). **Comparativo entre LGPD, GDPR, CCPA e PIPL**. São Paulo: IBDDIG, 2023. Disponível em: https://www.ibddig.org.br. Acesso em: 8 maio. 2025.

ISO. **Information technology —** Security techniques — Code of practice for information security controls based on ISO/IEC 27002 for the energy utility industry. ISO/IEC 27019:2022. Genebra: ISO, 2022.

LIMA, Caio César Carvalho; ALMADA, Marco; MARANHÃO, Juliano. **Data protection by design e data protection by default**: visão teórica e prática à luz da LGPD e do GDPR. In: VAINZOF, Rony; SERAFINO, Danielle; STEINWASCHER, Aline (org.). Legal innovation: o futuro do direito e o direito do futuro. São Paulo: Thomson Reuters, 2022. p. 265-288. Disponível em: https://cadmus.eui.eu/handle/1814/74416. Acesso em: 21 abr. 2025.

MANDIANT. **M-Trends 2022 Report.** Milpitas: FireEye/Mandiant, 2022. Disponível em: https://www.mandiant.com/resources/m-trends . Acesso em: 21 maio. 2025.

MAZZUCATO, Mariana. **Missão economia**: um guia para mudar o capitalismo. São Paulo: Companhia das Letras, 2021.

MINGARDI, Guaracy. **Tiras, gansos e trutas**: cotidiano e reforma na polícia civil. São Paulo: Scritta Editorial, 2021. Disponível em: https://pt.scribd.com/document/392612380/Lyotard-a-Condicao-Pos-Moderna. Acesso em: 10 maio 2025.

MITRE. **Cybersecurity for Industrial Control Systems**. Bedford, 2022. Disponível em: https://www.mitre.org. Acesso em: 21 maio. 2025.

NATO CCDCOE. **Cooperative Cyber Defence Centre of Excellence**. Tallin: CCDCOE, 2023.

NCSC – NATIONAL CYBER SECURITY CENTRE. **Ransomware attacks against healthcare during COVID-19.** Londres: NCSC, 2021. Disponível em: https://www.ncsc.gov.uk. Acesso em: 25 maio. 2025.

ONU – ORGANIZAÇÃO DAS NAÇÕES UNIDAS. **Transformando nosso mundo: a Agenda 2030 para o Desenvolvimento Sustentável.** Nova York: ONU, 2015.

OTAN – ORGANIZAÇÃO DO TRATADO DO ATLÂNTICO NORTE. **Cyber Defence**. Bruxelas: NATO, 2023 a. Disponível em: https://www.nato.int/cps/en/natolive/topics_78170.htm . Acesso em: 27 maio. 2025.

OTAN. **Relatório de segurança cibernética e espionagem cibernética**. Bruxelas: NATO Public Diplomacy Division, 2023b.

OEA – ORGANIZAÇÃO DOS ESTADOS AMERICANOS. **CICTE: Programa de Cibersegurança nas Américas.** Washington, DC: OEA, 2023. Disponível em: https://www.oas.org/pt/cyber . Acesso em: 1 jun. 2025.

PINHEIRO, Rafael Zanatta. Segurança nacional e proteção de dados pessoais: tensões institucionais e riscos à privacidade no Brasil. **Revista Brasileira de Políticas Públicas**, v. 11, n. 1, p. 63–84, 2021.

RODRIGUES, J. M. **A proteção de dados pessoais e o GDPR**: análise e impactos. São Paulo: Editora Jurídica, 2019. Acesso em: 09 mar. 2025.

SANS INSTITUTE. **State of ICS Cybersecurity Survey**. Bethesda, 2020. Disponível em: https://www.sans.org. Acesso em: 8 abr. 2025.

SOUZA, A. C. **LGPD na prática**: fundamentos e implementação no Brasil. Rio de Janeiro: Editora Digital, 2021. Acesso em: 04 dez. 2024.

SOUZA, Clarisse de; FRAJHOF, Isabella Z.; CORREIA, Fernando A.; LOPES, Hélio. **Second layer data governance for permissioned blockchains:** the privacy management challenge. *arXiv*, 2020. Disponível em: https://arxiv.org/abs/2010.11677. Acesso em: 01 jun. 2025.

SCHNEIER, Bruce. **Click here to kill everybody**: Security and survival in a hyper-connected world. New York: W. W. Norton & Company, 2018. Disponível em: https://example.com/link-do-livro. Acesso em: 12 maio 2025.

UNIÃO EUROPEIA. **Diretiva SRI 2**: novas regras em matéria de cibersegurança das redes e dos sistemas de informação. 2022. Disponível em: https://digital-strategy.ec.europa.eu/pt/policies/nis2-directive. Acesso em: 28 abr. 2025.

UNIÃO EUROPEIA. **Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE** (Regulamento Geral sobre a Proteção de Dados). Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A32016R0679. Acesso em: 09 maio 2025

UNIDIR – UNITED NATIONS INSTITUTE FOR DISARMAMENT RESEARCH. **Norms for Responsible State Behaviour in Cyberspace.** Genebra: ONU, 2022. Disponível em: https://unidir.org. Acesso em: 14 maio. 2025.

UNIDIR – United Nations Institute for Disarmament Research. **Cyber Policy Portal.** Genebra: UNIDIR, 2021.

UNITED NATIONS. **Open-ended working group on developments in the field of information and telecommunications in the context of international security**. New York: United Nations, 2021.

UNITED NATIONS OFFICE ON DRUGS AND CRIME (UNODC). **UN General Assembly adopts landmark convention on cybercrime.** 2024. Disponível em: https://unis.unvienna.org/unis/pressrels/2024/uniscp1184.html. Acesso em: 12 abr. 2025.

UNITED STATES OF AMERICA (California). **California Consumer Privacy Act – CCPA**. 2018. Disponível em: https://oag.ca.gov/privacy/ccpa . Acesso em: 31 maio 2025.

ZHANG, Yaqiu. China's Personal Information Protection Law: A Comparative Review. **Asian Journal of Law and Society**, v. 9, n. 2, p. 245–263, 2021. Disponível em: https://pubmed.ncbi.nlm.nih.gov/36252979/. Acesso em: 02 jun. 2025.

ZETTER, Kim. **Inside the cunning, unprecedented hack of Ukraine's power grid.** Wired, 2016. Disponível em: https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/ . Acesso em: 30 maio 2025.

ZUBOFF, Shoshana. **A era do capitalismo de vigilância**: a luta por um futuro humano na nova fronteira do poder. Rio de Janeiro: Intrínseca, 2020.