VII ENCONTRO VIRTUAL DO CONPEDI

DIREITO, GOVERNANÇA E NOVAS TECNOLOGIAS I

IRINEU FRANCISCO BARRETO JUNIOR

AIRES JOSE ROVER

MARISA CATARINA DA CONCEIÇÃO DINIS

D597

Direito, governança e novas tecnologias I [Recurso eletrônico on-line] organização CONPEDI

Coordenadores: Aires Jose Rover; Irineu Francisco Barreto Junior; Marisa Catarina da Conceição Dinis – Florianópolis: CONPEDI, 2024.

Inclui bibliografia
ISBN: 978-85-5505-889-9
Modo de acesso: www.conpedi.org.br em publicações
Tema: A pesquisa jurídica na perspectiva da transdisciplinaridade

1. Direito – Estudo e ensino (Pós-graduação) – Encontros Nacionais. 2. Direito. 3. Governança e novas tecnologias. VII Encontro Virtual do CONPEDI (1: 2024 : Florianópolis, Brasil).

CDU: 34

Conselho Nacional de Pesquisa
e Pós-Graduação em Direito Florianópolis
Santa Catarina – Brasil
www.conpedi.org.br

VII ENCONTRO VIRTUAL DO CONPEDI

DIREITO, GOVERNANÇA E NOVAS TECNOLOGIAS I

Apresentação

No VII Encontro Virtual do CONPEDI, o grupo de trabalho “Direito, Governança e Novas Tecnologias I”, se destacou não apenas pela qualidade dos trabalhos apresentados, mas também pela participação de renomados professores pesquisadores, acompanhados por seus alunos de pós-graduação e um graduando. O evento contou com a apresentação de 21 artigos, que foram objeto de um intenso debate conduzido pelos coordenadores e enriquecido pela participação do público na sala virtual.

Esse destaque evidencia o interesse e a relevância dos temas discutidos no âmbito jurídico. Conscientes disso, os programas de pós-graduação em direito promovem um diálogo que incentiva a interdisciplinaridade na pesquisa e visa enfrentar os desafios impostos pelas novas tecnologias ao direito. Para facilitar a apresentação e a discussão dos trabalhos sob essa perspectiva, os coordenadores do grupo de trabalho organizaram os artigos em blocos temáticos, que refletem em parte nessa publicação. Segue os três blocos temáticos gerais e palavras chave dos artigos apresentados.

Direito e Tecnologia

· Telemedicina, telessaúde, direito à saúde.

· Direitos fundamentais, era digital, privacidade.

· Avanço tecnológico, sistema judiciário, celeridade.

· Estado democrático de direito, vigilância, internet.

· Fintechs, transformação, direito bancário.

· Arcabouço normativo, cibersegurança, sociedade da informação.

· Direito à imagem, pessoa jurídica, novas tecnologias.

· Big Techs, tabelionato de notas, uso de dados.

A influência das tecnologias digitais no direito é evidente em diversas áreas, como na telemedicina e telessaúde, que ampliam o acesso à saúde através de consultas remotas, desafiando conceitos tradicionais de atendimento presencial. Em paralelo, direitos fundamentais como a privacidade se tornam cada vez mais cruciais na era digital, enquanto o avanço tecnológico promove a celeridade no sistema judiciário, buscando maior eficiência. O Estado democrático de direito enfrenta novos desafios com a vigilância na internet, colocando em debate a balança entre segurança e liberdade individual. As fintechs estão transformando o direito bancário, adaptando-o às necessidades de uma sociedade mais conectada. O arcabouço normativo de cibersegurança busca proteger a sociedade da informação, refletindo a necessidade de regulamentações claras e eficazes. O direito à imagem da pessoa jurídica também se redefine frente às novas tecnologias, enquanto Big Techs e tabelionato de notas são alvo de análises comparativas sobre a coleta e uso de dados na sociedade da informação.

Inteligência Artificial e Direito

· Regulamentação, inteligência artificial, direitos autorais.

· Estudo comparado, direitos autorais, pré-treinamento.

· Impacto, inteligência artificial, herança digital.

· Direito, inteligência artificial, ficção científica.

· Impacto, inteligência artificial, campo jurídico.

A interseção entre direito e inteligência artificial emerge como um campo dinâmico e complexo, abordando desde questões de regulamentação e direitos autorais até o impacto da IA na herança digital. Estudos comparados dos primeiros casos norte-americanos destacam o papel crucial do pré-treinamento da IA, enquanto debates éticos e a necessidade de políticas regulatórias são essenciais para orientar seu desenvolvimento. Além disso, a IA desafia conceitos tradicionais de direito, flertando entre ficção científica e realidade prática, influenciando tanto o ensino quanto a prática profissional no campo jurídico contemporâneo.

Diversos

· Tecnologia, Educação, Inclusão Digital

· Educação, Transformação Digital, Resistência

· Jurimetria, Competência, Saúde

· Transparência, Participação Cidadã, Governo

· Bolhas Virtuais, Democracia, Psicologia

· Tecnoceno, Biotecnologia, Sustentabilidade

· Agricultura Familiar, Políticas Públicas, Tecnologia

· Governança, Dados, Abordagem Quântica

Esses artigos abrangem uma ampla gama de áreas de interesse e preocupações contemporâneas. Eles refletem uma visão abrangente que inclui a interseção entre tecnologia, educação e inclusão digital, enfatizando a importância da transformação digital e da resistência educacional. Além disso, exploram temas como jurimetria e competência no contexto da saúde, assim como questões de transparência, participação cidadã e governança. Também abordam fenômenos contemporâneos como bolhas virtuais e democracia, com insights da psicologia, e discutem a interseção entre tecnoceno, biotecnologia e sustentabilidade. A agricultura familiar e as políticas públicas são vistas sob a lente da tecnologia, enquanto a governança de dados e abordagens quânticas refletem preocupações emergentes na era digital.

Os coordenadores responsáveis pelo Grupo de Trabalho cordialmente convidam os interessados a examinar integralmente os artigos em questão, confiantes de que a leitura será proveitosa. Encerramos esta apresentação expressando gratidão pela oportunidade de facilitar os diálogos entre pesquisadores de elevada competência.

Aires José Rover - Universidade Federal de Santa Catarina

Irineu Francisco Barreto Júnior - Mestrado em Direito das Faculdades Metropolitanas Unidas

Marisa Catarina da Conceição Dinis - Instituto Jurídico Portucalense

O ARCABOUÇO NORMATIVO BRASILEIRO DE CIBERSEGURANÇA E SEUS REFLEXOS NA SOCIEDADE DA INFORMAÇÃO

THE BRAZILIAN REGULATORY FRAMEWORK FOR CYBERSECURITY AND ITS IMPACTS ON THE INFORMATION SOCIETY

Claudio Luiz de Carvalho [1]
Thiago Henrique Rodrigues da Silva [2]
Irineu Francisco Barreto Junior [3]

Resumo

O presente artigo visa abordar inicialmente a evolução da internet e sua crescente importância na Sociedade da Informação, ao mesmo tempo em que destaca o aumento das atividades criminosas em meio digital, onde a cibersegurança á o principal meio de proteção contra as intentadas cibernéticas. Na presente era informacional o conceito de cibersegurança toma relevância particular desde o crescimento do ciberespaço como lugar virtual para interação social, resultado da evolução das tecnologias e a proliferação de dados serve como escopo para a revolução técnico científica ultra geracional, com impactos vertentes muito além da rede internacional de computadores. Propõe-se uma busca sobre aspectos técnicos e jurídicos do crime cibernético, com foco no contexto brasileiro, em legislações como o Marco Civil da Internet e a Lei Geral de Proteção de Dados, elementares para disciplinar o meio ambiente digital. Além disso, discute-se a relação entre segurança cibernética, proteção de dados e governança no ambiente privado, ressaltando a necessidade de cumprimento das leis e conscientização dos usuários. A pesquisa conclui que, conforme as tecnologias avançam, o lado obscuro dos meios informáticos e a participação desmedida de grupos extremistas torna-se mais exponencial em face dos ataques perpetrados às grandes empresas e corporações, órgãos de relevo dos Estados nacionais e segurança, educacional, saúde e infraestrutura energética, sem deixar de lado os próprios cidadãos.

Palavras-chave: Cibersegurança, Lgpd, Brasil, Cisa, pnciber

Abstract/Resumen/Résumé

This paper aims to initially address the evolution of the Internet and its growing importance

---

[1] Mestre em Economia Aplicada pela UFJF, graduado e mestrando em Direito pela FMU. Advogado e especialista em Gestão Tributária pela ESALQ-USP.

[2] Mestrando em Direito da Sociedade da Informação e Graduado em Direito pelo Centro Universitário das Faculdades Metropolitanas Unidas (FMU). Advogado.

[3] Pós Doutor em Sociologia pela USP. Docente do Programa de Mestrado em Direito da Sociedade da Informação da FMU-SP. Analista de Pesquisas da Fundação Seade-SP.

in the Information Society, while highlighting the increase in criminal activities in the digital environment, where cybersecurity is the main means of protection against cyber attacks. In the current informational age, the concept of cybersecurity gains particular relevance due to the growth of cyberspace as a virtual space for social interaction, a result of technological evolution and the proliferation of data. This serves as the scope for the ultra-generational technical-scientific revolution, with impacts extending far beyond the international network of computers. It proposes a search for technical and legal aspects of cybercrime, with a focus on the Brazilian context, on legislation such as the Marco Civil da Internet – Brazilian Internet Bill of Rights and the Lei Geral de Proteção de Dados – Brazilian General Data Protection Law, which is essential for disciplining the digital environment. In addition, the relationship between cybersecurity, data protection, and governance in the private environment is discussed, highlighting the need for compliance with the law and user awareness. The research concludes that, as technologies advance, the dark side of computerized means and the disproportionate involvement of extremist groups become increasingly exponential in the face of attacks perpetrated against large companies and corporations, relevant organs of national states, and security, educational, health, and energy infrastructure, without neglecting the citizens themselves.

Keywords/Palabras-claves/Mots-clés: Cybersecurity, Lgpd, Brazil, Cisa, pnciber

Introdução

O nascedouro da Internet remonta aos primórdios do século XX quando da grande arquitetura bélica, de posse dos estados nacionais e, décadas seguintes da sua insurgência, aporta o ciberespaço como palco de intrusão do imediatismo e do cotidiano acentuado, impactado pela revolução de maquinários cada vez mais sintetizados e ampla diversificação da sociedade da informação.

O conceito de cibersegurança toma relevância particular desde o crescimento do ciberespaço como lugar virtual para interação social, resultado da evolução das tecnologias. A proliferação de dados gerados e as informações mapeadas e gerenciadas servem de escopo para a uma revolução técnico científica ultra geracional, com impactos vertentes muito além da rede internacional de computadores.

No encontro de uma robótica que se assenta ante um poderio cibernético incalculável e defronte ela, um porvir de uma nova era, - eis que posiciona-se um importante dilema a ser sopesado: a evolução inigualável de distintas áreas do saber potencializadas pela tecnologia circuncidada por uma complexa logística e regulação legal com o crivo de alimentar uma cibersegurança necessária e capaz de combater o dissabor nefasto do cibercomando do crime, que arquiteta implosões e desestrutura as capacidades sistêmicas de corporações, governos e pessoas pelas mãos de criminosos e estados-nações com ganas de deter o controle financeiro e informacional para o fim deletério, ilegal e espúrio.

Tal qual o avanço tecnológico, há que se pautar a natureza do crime, que também evoluiu, o ganho da invasão que antes concentrava-se tão somente em uma potencial vítima torna-se agora inimaginável com a oportunidade de acesso múltiplo a uma infinidade de dispositivos, reféns do roubo, espionagem, alteração ou obliteração dos dados, ou mesmo extorsão.

Neste sentido, o trabalho tem como objetivos gerais investigar os aspectos técnicos e jurídicos envolvidos na temática crucial do crime cibernético, seu controle legal e ferramental necessário para o fortalecimento da cibersegurança. Estritamente, busca contribuir para o incurso de novas ações de cunho processual e legal, tendo por bojo avaliar qualitativamente o avanço nacional em face da ameaça cibercriminosa tanto nas esferas do direito privado quanto do direito público.

Metodologicamente, far-se-á uso da hermenêutica jurídica por meio de extensa técnica de pesquisa bibliográfica de cunho exploratório em abordagem qualitativa, extraindo-se

conteúdos à luz da legislação vertente e seus efeitos no seio da sociedade brasileira, abordando, por fim, as questões pertinentes no cenário nacional no que compete ao Marco Civil da Internet – MCI (Lei 12.965/2014), Lei Geral de Proteção de Dados – LGPD (Lei 13.709/2018), a Política Nacional de Cibersegurança - PNCiber (Decreto 11.856/2023) e demais legislações do microssistema jurídico.

1. O Marco Civil da Internet e a Lei Geral de Proteção de Dados: Agentes Precursores da Estruturação da Segurança Cibernética no Brasil?

A segurança cibernética é um dos maiores entraves e desafios enfrentados pelo Brasil na era digital contemporânea, uma questão que vai além das barreiras tecnológicas, caminhando para as dimensões social, econômica e jurídica de uma sociedade em alerta. O advento do Marco Civil da Internet (MCI) e da Lei Geral de Proteção de Dados (LGPD) consignam um esforço legislativo de enorme monta para a estruturação de uma base securitária consistente. Neste sentido, o presente capítulo possui por essência discutir a progressão destes instrumentos legais na amplitude do tecido digital brasileiro em seu critério epistemológico.

A promulgação do MCI em 2014 marcou um ponto de inflexão quando espraiado na regulamentação da Internet no Brasil. A abordagem ali contida para proteger os direitos fundamentais, como privacidade e liberdade de expressão, entremeada à uma obrigação de prover segurança por parte dos provedores de acesso e conteúdo, semeou as vigas de sustentação mestra de um ciberespaço mais seguro e resiliente.

A hiper conectividade satisfeita às mãos de uma sociedade global, donde os rastros de dados se movimentam em propulsão espacial, o novo petróleo – a segurança cibernética e a proteção de dados pessoais tornaram-se pauta crucial no que tange à salvaguarda de direitos individuais e coletivos. A sinergia, então entronizada pelo MCI e pela LGPD, acopla-se de forma segmentada, contribuindo para a sedimentação de um paradigma legal, cujo impacto sobreposto à seguridade da informação enseja ser examinado sob a lente jurídico sociológica. Como demonstrado por Barreto Junior (2015, p.2), esse novo estágio do desenvolvimento do capitalismo:

> Apresenta como marco inicial, a ruptura dos padrões de sociabilidade típicos do Século XX, provocada por uma série de eventos sistêmicos e concatenados em escala mundial, aos quais se convencionou denominar como Sociedade da Informação. Inaugura-se um novo estágio do modo de produção capitalista, instaurado pela convergência tecnológica e digital, pelo exponencial crescimento – e consequente diminuição dos custos – da produção de equipamentos informáticos e, principalmente, pela disseminação em escala mundial da Internet (Barreto Junior, 2015, p. 02).

Levy (2003) aponta o ciberespaço como o universo de redes digitais, fora da circunscrição dos livros e dos meios de comunicação em massa – um espaço aberto por meio da interconexão mundial de computadores. Sua virtual existência coexiste com a concretude moderna e como expectadora, a humanidade viu transpassar-se por entre os véus da informatização, presenciou a revolução das telecomunicações e a multiplicação em tempo recorde de informações.

Neto e Aguiar (2024) apontam a LGPD como elemento para a promoção de práticas da segurança da informação, traduzindo-a não apenas no sentido normativo do compêndio legal, mas sobretudo no que concerne à adequação dos procedimentos e conscientização do extrato conceitual que advém dos dados informáticos. Neste sentido, o trabalho dos autores caminha para um amadurecimento do sistema corporativista empresarial em face do mecanismo legislativo corporificado na última década, embora algumas arestas ainda careçam de aparagens fronte aos obstáculos estruturais e culturais do espaço tridimensional para a multidisciplinariedade organizacional do ciberespaço.

Em um contraste mais diluído à visão de Neto e Aguiar (2024), Corrêa Filho (2016) aponta para um processo ainda em desenvolvimento, isto é, carece ainda de maior burilamento legislativo para maior profusão e robustez no que tange à LGPD. Ainda que sejam diversos os avanços detidos na materialidade do circuito cibernético, muitas transformações sociotécnicas seguem um curso por definir na percepção do campo da segurança digital.

Na dialética global, Brustolin, Nunes e Assunção (2022) navegam de ponta a ponta por entre as fibras de segurança cibernética alcançadas por Brasil e Estados Unidos em entendimento comparativo. Nesta toada, as singularidades brasileiras sobressaltam aos olhares atentos dos autores, pois uma integração nativa evidencia o código de defesa do consumidor entremeado pela proteção de dados e a marcação da segurança cibernética como capa protetiva, aludindo uma convergência com os padrões internacionais, mas, ao mesmo tempo, delimitando uma subjetividade particular do contexto nacional à adaptação das realidades sociais, econômico e culturais do país, em estrita associação à teoria de “globalização”, termo apresentado por Roland Robertson (1995) – donde as particularidades locais coexistem e se moldam dentro de uma crescente interconexão global, elastecida pela complexa e dinâmica relação associada entre forças globais e locais.

Diante do conceito já articulado, Bioni (2020) assevera a proteção de dados sob o olhar da função e dos limites do consentimento por parte do usuário, trazendo à baila as complexidades inerentes ao conceito maior de consentimento ante um ambiente digital profundamente modificado e com múltiplas facetas, sugerindo uma intersecção de ordem crítica advindo das imposições regulatórias e as experiências vivenciadas pelos inúmeros usuários, onde muitos destes se encontram em condição vulnerável, tal como apresentado na obra de Zygmunt Bauman (2001) em sua detida análise da "modernidade líquida".

Na concepção dos diálogos exercidos ante as mais diversas legislações que compõem o microssistema jurídico, destaque para o Código de Defasa do Consumidor – CDC, como já debatido por Brustolin, Nunes e Assunção (2022) e para os mecanismos que albergam o aparelhamento informático digital, a saber o MCI e a LGPD (Guimaraes-Filho; Ferneda; Ferraz, 2020), o reforço mútuo ali exercido entre os marcos de proteção também cooperam para melhor tratamento dos dados digitais – o que *per se* nos prontifica a contemplar o universo da teoria dos sistemas sociais, ante a abordagem sistêmica e integrada, tal como defendido por Niklas Luhmann (1995) em Sistemas Sociais.

Para tanto, a cibersegurança, converge em consonância para a sociedade do risco, proposta por Ulrich Beck (1992), na qual os riscos em seu sentido global são individualizados e o contexto de distribuição de riquezas é amoldado por imprevisibilidades afeitas ao novo condicionamento, aqui em discussão o contexto do ciberespaço, donde a sociedade do risco surge de uma sociedade reflexiva, que cada vez mais orienta-se nos apelos constantes de maior ciberseguridade nos mecanismos de informação. O ambiente digital melhor protegido, para Szinvelski e Arceno (2022), é possibilitado pela efetividade do tratamento de dados, constituído, de fato, pela LGPD.

Passa-se então para uma conceitualização mais abrangente, nos termos do filósofo Luciano Floridi (2014), de uma "ética da informação", código que transcende a natureza onipresente e onisciente das tecnologias da informação e comunicação emergidas na sociedade atual. A eticidade condiz a um tratamento equilibrado entre os princípios da privacidade e bem-estar geral, encartados tanto no MCI quanto na LGPD. Desta maneira, não se pode omitir o quanto defendido pelo jurista Lawrence Lessig (1999) em seu trabalho renomado intitulado "Código e Outras Leis do Ciberespaço" – o comportamento humano se completa ante as leis, normais sociais, o mercado e o exercício computacional exercido em seu controle. No todo e no sentido global, a regulamentação adequada permite garantir a segurança e proteção dos direitos fundamentais no ambiente digital.

Como desenvolvimento vertido em consequência das interações sociais e econômicas, a sociedade em rede e a cultura de virtualidade real, contidas em Castells (2006), são acometidas em um universo de tecnologia e comunicação e a segurança cibernética conjunta à necessária proteção de dados muralham a confiança e estabilidade social ensejada pela vontade plural dos indivíduos, o que adentro à pertinência deste objeto abarca maior conscientização e capacitação de todos os autores envolvidos, mediante uma abordagem multidisciplinar e colaborativa.

Como medida inserta em um páreo evolutivo, os marcos do MCI e LGDP são agentes precursores, mas, no entanto, não se pode olvidar que há sempre uma constante evolutiva nos preceitos normativos no sentido de atualização legislativa, no acompanhamento e evolução dos crimes cibernéticos. Nesta seara, a Lei de Crimes Cibernéticos (Lei nº 14.155/2021) representa um avanço significativo com lacunas ainda por serem preenchidas, em especial na cooperação internacional e harmonização das leis entre as mais distintas jurisdições.

Assim, a literatura permite demonstrar uma evolução a partir dos marcos do MCI e da LGPD em solo brasileiro mediante toda transformação sociotécnica comportada no último decênio, em especial. Para além, o término deste capítulo permite sintetizar de forma breve, a consequência advinda da multiplicidade dos diversos microssistemas legais, donde a colaboração e contribuição emergem como estrutura prática para melhor gestão da informação, cibersegurança e proteção dos dados pessoais, refletindo para o que contido na teoria da complexidade, por Edgar Morin (2001): Morin critica o pensamento fragmentador, reducionista e simplificador que prevaleceu na modernidade e argumenta que satisfazê-lo seria cair na insuficiência ante a complexidade inerente aos fenômenos naturais, sociais e humanos. Para o autor, não apenas a parte está no todo, mas o todo está inscrito na parte.

2. Políticas Regulatórias e a Convergência dos Mecanismos de Governança na Ordem Privada

Na complexa rede intrincada que entrelaça a segurança cibernética e a proteção de dados, um olhar atento ao caráter multidisciplinar dos critérios de governança não pode ser subdimensionado. O presente ensaio tem por fim descortinar as inúmeras camadas pertinentes ao tema, trazendo uma análise atinente do impacto regulatório sob a esfera do ambiente privado, as implicações oriundas das transformações tecnológicas e a necessária governança robusta e concernente aos mecanismos do microssistema legal jurídico advindos do MCI e da própria LGPD.

Os avanços obtidos com o progresso tecnológico também dimensionam um universo repleto de riscos igualmente ou majoritariamente significativos para consignar um planejamento consistente e defensivo por parte das estruturas de mercado nas pessoas de direito público e privado. Nesse diapasão, *mister* informar, segundo dados das Nações Unidas, reportados pela Forbes[1] (2021) que naquele ano, um aumento de 59% nos ciberataques perpetrou-se mediante o universo de usuários num clarão alarmante, ano a ano, para o levante cibernético defensivo por parte de governos e setor privado em face das ameaças prevalentes oriundas de um ciberespaço pouco regulado no sentido de conter, punir e lançar medidas de prevenção aos crimes cibernéticos.

Em solo brasileiro, como discutido anteriormente, a LGPD consubstanciou-se como instrumento legal essencial, de inspiração ao modelo europeu de Regulação Geral de Proteção de Dados – RGPD, que lançou suas bases um biênio antes do marco legal nacional. Neste sentido, ainda que proponha a criação de um ambiente de tratamento de dados sob os princípios da privacidade e segurança (Doneda; Sarlet; Mendes; Bioni, 2021) reporta que a problemática da LGPD está em sua conformidade e execução. Para Solove e Hartzog (2014), as organizações enfrentam uma complexa tarefa de atendimento às regulamentações já em exercício, tornando o cumprimento das exigências um exercício hercúleo ante a novidade e ausência de precedentes.

Neste sentido, em atendimento às normas já postas em circulação, o *compliance* nasce como ponto de convergência entre a governança corporativa e a segurança da informação. As tecnologias de *compliance*, nas palavras de Bamberger (2009) agem no intuito de integrar a gestão de riscos, assegurando o cumprimento do arcabouço legal. Essa interlocução gerida pelos agentes das instituições privadas e públicas planifica o caminho para a sobrevivência em um mundo articulado, competitivo e inseguro.

Para adiante, a capacidade de autodefesa instituiu-se como essencial no mundo corporativo emergente das inovações tecnológicas. Kesan e Hayes (2011) argumentam que os mecanismos de defesa e segurança cibernética são inerentes às práticas das novas estratégias de negócios, tendo em vista os frequentes e sofisticados ataques orquestrados e implodidos nas redes e dispositivos informáticos. A segurança cibernética e a proteção de dados são institutos de uma estratégia integrada nas visões de Mitterlehner (2014) e Gottschalk Nolasco e Maciel Silva (2022), donde a Lei de Crimes Cibernéticos (Lei 14.155/2021) reforça a necessária

[1] FORBES. Brazil Is The World's Second Most Vulnerable Country To Cyberattacks. Disponível em: https://www.forbes.com/sites/angelicamarideoliveira/2023/09/27/brazil-is-the-worlds-second-most-vulnerable-country-to-cyberattacks/?sh=531fbbfb27a4. Acesso em: 02 abr. 2024.

interpretação harmônica dos dispositivos legais existentes para uma operação coordenada das leis que englobam o microssistema jurídico brasileiro atual.

Informações divulgadas pelo Security Report [2](2023) apontam para um aumento de 16% nas tentativas de ataques cibernéticos no Brasil. O percentual implica em mais de 103,16 bilhões de tentativas de ataques, - levando o país a ocupar o ranking de segundo lugar dentre os países da América Latina. Essa vulnerabilidade, aqui em comento, não prospera somente com a adoção de padrões internacionais e maior cooperação no contingenciamento e fortalecimento dos sistemas críticos – ainda que bem observados por Abeyratne (2019). O indicador do CERT.br é corroborado pelo ranking de cibersegurança do *MIT Technology Review Insights*, divulgado pela Exame[3], mensurando o Brasil em 18º lugar dentre as 20 economias avaliadas – resultado obtido ante a baixa pontuação em todos os critérios utilizados, como infraestrutura crítica, recursos de segurança cibernética, capacidade organizacional e comprometimento com as políticas públicas de relevo à temática.

Sendo assim, há que se falar em uma conscientização múltipla tanto por parte dos usuários domésticos quanto aqueles oriundos da casta empresarial, uma vez que 19,9% dos usuários brasileiros, segundo o mesmo reporte Exame, tentou abrir links maliciosos de origem cibercriminosa e por vertente semelhante no que perfaz o mundo corporativo, detém-se que apenas 10% dos investimentos em tecnologia das empresas brasileiras concentram-se no canal de cibersegurança, o que distancia o perfil brasileiro, se comparado aos 25% - 30% sequenciados em outros países, segundo dados da Perallis Security[4], culminando em ataques concentrados, sobretudo no comprometimento de dados confidenciais, propriedade intelectual e reputação empresarial, donde: *ransomware*, *phishing*, *malwares*, ataques DDoS e roubo de dados e identidade estão entre os crimes mais acometidos – o que representa grave ameaça à continuidade dos negócios e estabilidade econômica.

Adentrando o ambiente micro das empresas, há que se considerar a conscientização por parte de suas hierarquias gestoras como também o provimento da capacitação dos funcionários como forma de garantir melhor sistema de governança em segurança cibernética.

---

[2] SECURITY LEADERS. Brasil sofreu 103,16 bilhões de tentativas de ataques cibernéticos no ano passado. Disponível em: https://securityleaders.com.br/brasil-sofreu-10316-bilhoes-de-tentativas-de-ataques-ciberneticos-em-2022/. Acesso em: 02 abr. 2024.

3 EXAME. Brasil está entre os 5 países com progresso mais lento em cibersegurança, diz MIT. Disponível em: https://exame.com/future-of-money/brasil-esta-entre-os-5-paises-com-progresso-mais-lento-em-ciberseguranca-diz-mit/. Acesso em: 02 abr. 2024.

[4] PERALLIS. Brasil, o país do cibercrime? Um panorama do cenário. Disponível em: https://www.perallis.com/news/brasil-o-pais-do-cibercrime-um-panorama-do-cenario. Acesso em: 03 abr. 2024.

A Conferência Internacional das Nações Unidas para o Comércio e Desenvolvimento [5](2022) também assinala a necessidade de investimento em capital humano como vórtice de superação para o preenchimento de lacunas vitais que ensejem maior segurança cibernética nos países de maior vulnerabilidade digital.

Em completude aos critérios de governança, a complementariedade entre abordagens tecnológicas e ciberlegais é apropriada, uma vez que para Harris e Martin (2019), tais critérios devem se aplicar às leis e regulamentações existentes no cumprimento de se desenvolver políticas e controles de segurança cibernética, promotores de um ambiente defensável, tanto resiliente quanto flexível para Melaku (2023), diante das crescentes ameaças em volume e complexidade. No que diz respeito à ênfase da LGPD, Lomas (2020) reporta a importância da governança como alcance de gestão de ativos de informação para a privacidade e proteção de dados de forma legal e ética.

Clark, Espinosa e Delone (2020) reforçam a importância do conhecimento organizacional alinhado aos preceitos de segurança cibernética, encontrando subsídio nos estudos de Kesan e Hayes (2011) quanto à integração do planejamento empresarial. Os desafios neste modelo de governança, segundo Yusif e Abdul Hafeez-Baig (2021), devem se ater à estratégia, processos e conformidade, fornecendo uma estrutura de enfrentamento às ameaças cibernéticas. Já Gottschalk Nolasco e Maciel Silva (2022) evidenciam a importância da estratégia integrada, demonstrando a inter-relação entre a segurança cibernética e a proteção de dados. Por fim e não menos importante, paira o entendimento de Jagadish e Shanbhog (2023) sobre as soluções de segurança nos ambientes de *cloud computing* (nuvem) tal como o avanço de estrutura tecnológica sobressaltado na última década, apoiando à ideia de adaptabilidade de Shackelford (2019) no âmbito da governança da Internet das Coisas (IoT).

A governabilidade do ciberespaço se mostra assertiva aos dispositivos trazidos pela LGPD quanto à proteção em face de acesso não autorizado e situações ilícitas ou acidentais de destruição, perda, alteração, comunicação e difusão (Art. 6º, VII); à determinação de que os agentes de tratamento tomem medidas de segurança, técnicas e administrativas para a proteção de dados pessoais em conformidade ao já exposto em sede do artigo supramencionado (Art. 46); à instituição da figura do encarregado, responsável por aceitar reclamações e comunicações

[5] UNCTAD. 2022 OUTCOME REPORT. Disponível em: https://unctad.org/system/files/information-document/eWeek-2022-Outcome-Report-FINAL.eng_.pdf. Acesso em: 04 abr. 2024.

dos titulares, prestar esclarecimentos e adotar providências concernentes ao tratamento dos dados (Art. 50).

Todos os feitos, acima discutidos, devem ser administrados de tal forma que não cadenciem para a concatenação de crimes cibernéticos como os prescritos em sede dos art. 154-A, 154-B e 171, §2º, VIII, da Lei de Crimes Cibernéticos (Lei 14.155/2021), a saber na seguinte ordem: crime de invasão de dispositivo informático; crime de interrupção ou perturbação de serviço informático ou transmissão de dados legítimos; agravante para o crime de estelionato: a disseminação de dados confidenciais ou privados com dano à vítima.

Na esteira da conclusão deste capítulo e defronte os trabalhos analisados, compreende-se o conceito de que a governança corporativa se integra ao ciberespaço e a proteção de dados, sendo política uníssona em suas políticas e estratégias, consignando a ética na gestão dos dados e provisão de crescente investimento em capital humano para melhor registro e incorporação dos aspectos legais às questões essenciais de segurança cibernética.

3. A Política Nacional de Cibersegurança (PNCiber) e a Cybersecurity e Infrastructure Security Agency (CISA): Uma Comparação Necessária

A segurança cibernética cravejou-se como prioridade última e estratégica para as nações do globo, ante as constantes ameaças do cibercrime e a dependência das instituições em face dos sistemas e infraestruturas críticas. Neste interim, tanto os Estados Unidos quanto o Brasil houveram de se inserir no contexto de busca por soluções a fornecer estruturas institucionais robustas para lidar com os infortúnios da criminalidade no ciberespaço, abrindo caminhos para a criação da Cybersecurity and Infrastructure Security Agency (CISA), nos EUA, como também da Política Nacional de Cibersegurança (PNCiber), no caso do Brasil.

Cronologicamente, criou-se a CISA nos EUA, em 2018, - uma agência federal subordinada ao Departamento de Segurança Interna, tendo por efetivo operacional a proteção de sistemas e infraestruturas críticas do governo federal, assim como provendo orientações e assistência técnica a parceiros externos. De outro modo, a PNCiber, instituída pelo Decreto 11.856/2023, constitui-se como política de âmbito nacional ao estabelecer diretrizes, princípios e instrumentos de modo a fortalecer a segurança cibernética no Brasil.

Apresentadas uma e outra, ainda que possuam naturezas institucionais distintas, ambas possuem o objetivo fundamental de fortalecer a segurança cibernética nacional, protegendo as

infraestruturas críticas de cada país. Deste modo, como disposto por Soni; Kaur; Gupta e Sharma (2023), o universo da cibersegurança confronta desafios múltiplos e complexos, o que exige uma abordagem em larga escala, com inúmeros atores e tecnologias.

Para tanto, ambos os organismos instituídos reconhecem a necessidade de uma abordagem colaborativa, o que demanda ação conjunta da sociedade civil, dos setores público e privado. Neste viés, a PNCiber possui um caráter mais abrangente, ao estabelecer princípios e diretrizes gerais, donde a CISA, por outro lado, apresenta um enfoque operacional, agindo diretamente na resposta aos incidentes e danos provocados como também na proteção das redes e sistemas governamentais.

Uma particularidade da PNCiber diz respeito à criação de um Comitê de Cibersegurança (CNCiber), cuja função será a de acompanhar a implementação e evolução da política instituída. O CNCiber possui composição de diversos setores, o que envolve desde representantes de ministérios governamentais, agências reguladoras, setor privado e sociedade civil em prol de uma abordagem colaborativa e inclusiva, como destacado pelo próprio Decreto de 26/12/2023.

Apesar da CISA agir como estrutura do governo federal, também busca cooperação com o setor privado e demais partes interessadas. A atuação do órgão está mais restrita à proteção de sistemas e infraestruturas críticas do governo dos EUA, orientar e dar assistência aos parceiros externos, tal como descrito por Alshemeili; Hertelendy; Hart; Alburaid; Benmoussa; Digregorio; Issa e Ciottone (2023) em seu trabalho de avaliação dos planos de interoperabilidade de comunicações nos estados norte-americanos.

Outro ponto de convergência entre a PNCiber e a CISA é o reconhecimento da importância da cooperação internacional em matéria de segurança cibernética. Ambas as iniciativas enfatizam a necessidade de colaboração técnica e o compartilhamento de informações com outros países e organizações internacionais, refletindo a natureza transnacional das ameaças cibernéticas, conforme art. 2º, VII, art. 3º, XI e art. 6, VI, do Decreto 11.856/2023.

Por se tratar de uma política recém-lançada pelo governo brasileiro, a efetividade da PNCiber dependerá de sua regulamentação e operabilidade nos próximos anos, assim como do engajamento e cooperação de todos os atores envolvidos no cenário nacional, tal como evidenciado por McMurrough, Fein e Skeath (2022) ao discutirem as recomendações da CISA sobre tendências de *ransomware*.

A abrangência mais ampla da PNCiber atua não apenas no que tange às infraestruturas críticas, como também na promoção de segurança cibernética nos mais diversos setores da sociedade brasileira, buscando estimular o desenvolvimento de produtos, serviços e tecnologias nacionais endereçadas à segurança cibernética como previsto no art. 3º, I, do Decreto 11.856/2023 – o que permite o incentivo à inovação e o fortalecimento da indústria nacional nessa área estratégica.

Na sequência do argumento nacional, a PNCiber possui aplicação direta na educação e desenvolvimento tecnológico em cibersegurança (art. 2, V), buscando adotar medidas de proteção cibernética e o desenvolvimento de situações de capacitação técnico-profissional nas áreas de tecnologia e segurança. A abordagem nacional reconhece o investimento em capital humano e o desenvolvimento de soluções tecnológicas que visem o enfrentamento de ameaças de modo sustentável, assim como proposto por Sterns (2019) quando verificou a harmonização entre as regulamentações da CISA e do Departamento de Serviços Financeiros de New York.

Neste sentido, contraponto diverso pode ser verificando no estudo de Lucas (2020) ao questionar se a CISA seria uma espécie de salvadora da cibersegurança estadual e local nos EUA. Em resposta ao achado, apesar de a CISA promover medidas de conscientização e treinamento, o foco principal da agência é a proteção de sistemas e infraestruturas críticas, o que diverge da PNCiber que possui abordagem mais abrangente, detendo em seu poder aspectos educacionais, tecnológicos e de desenvolvimento de capacidades nacionais.

Na esfera de uma abordagem integrada e coordenada entre as autoridades responsáveis pela segurança cibernética e aplicação da lei, tanto a PNCiber quanto a CISA convergem no mesmo plano. Ambas agem no intuito de combater os crimes cibernéticos e ações perniciosas no ciberespaço, ainda que possam adotar estratégias e mecanismos distintos para alcançar seus objetivos. Tal enfoque pode ser aplicado no conflito russo-ucraniano, como visto por Locascio (2022).

Um outro enfoque convergente entre a PNCiber e a CISA diz respeito à importância da proteção dos dados pessoais e à privacidade no contexto da segurança cibernética. A operação de ambas se estrutura mediante um ambiente regulatório como a Lei Geral de Proteção de Dados (LGPD) no caso brasileiro e o Privacy Act nos EUA, tal como evidencia Lanz (2022) para o caso norte-americano em uma análise de alertas e avisos do governo federal dos EUA sobre riscos em infraestruturas críticas.

No fato mais recente, que diz respeito ao ataque à cadeia de suprimentos de software da Solar Winds em 2020, que gerou impactos nos EUA, em todo o globo, inclusive no Brasil, há que se pautar que as políticas desenvolvidas pela CISA e PNCiber são complementares e não concorrentes. O objetivo de ambas é o fortalecimento da segurança cibernética nacional, levando-se em consideração suas matrizes institucionais, marcos regulatórios e necessidades particulares, como apontado por Martínez e Duran (2021) nas ações tomadas pela CISA diante do ataque de grande impacto que assolou vítimas tanto pertencentes à esfera pública quanto privada em solo dos EUA. Se existente à época dos fatos, medidas próprias teriam sido tomadas e discutidas pela PNCiber às empresas afetadas em solo brasileiro.

Ao cabo e ao fim, torna-se fundamental reconhecer que a segurança cibernética se apresenta como desafio constante e contínuo ante a incomensurável evolução do ambiente digital e novas tecnologias, o que exige reforços coordenados e amparados por todos os atores envolvidos. Deve-se, então, segundo Rich (2022) aprimorar continuamente a cibersegurança para a proteção dos dados e interesses nacionais, o que se aplica não somente aos EUA como a todos os países do globo. Neste sentido, embora a PNCiber quanto a CISA compartilhem objetivos gerais semelhantes, importante e notório destacar o diferencial de ambas em sua natureza institucional, escopo de atuação e estágio de maturidade.

A PNCiber representa um esforço brasileiro em estabelecer um arcabouço legal e institucional abrangente para a segurança cibernética ao passo que a CISA é uma agência federal operacional atuante nos EUA. Ambos reconhecem a importância de cooperação entre os setores público e privado, como também a cooperação internacional como medida de enfrentamento dos desafios crescentes da segurança no ciberespaço. Por conseguinte, é fundamental que essas políticas e estruturas sejam continuamente avaliadas, atualizadas e aprimoradas para lidar com as constantes ameaças que emergem em face das constantes evoluções tecnológicas para essa massa crítica em questão.

Conclusão

No escopo das observações trazidas nos capítulos anteriores da revisão literária, resta notório que um dos grandes desafios a ser gerenciado na Sociedade da Informação amplia-se no aprofundamento e compreensão dos crimes cibernéticos à luz dos mecanismos legais, cujos efeitos impactam profundamente o meio ambiente digital e os usuários de todo o ciberespaço,

haja vista que a proteção dos dados informáticos são itens de máximo quilate no contexto de cibersegurança. Os canais legal-normativos dessa nova sociedade, a Lei Geral de Proteção de Dados e o Marco Civil da Internet, alinhados com a Política Nacional de Cibersegurança da brasileira (mais recente e específica) objetivam fornecer camada extra de proteção, mormente no que diz respeito a proteção de dados sob a tutela de empresas no alcance do substanciado no art. 19 do próprio Marco Civil da Internet e a responsabilização dos agentes provedores de internet e provedores de aplicação para o funcionamento das redes sociais existentes.

Uma vez que as tecnologias avançam, o lado penumbroso dos meios informáticos e a participação desmedida de grupos extremistas torna-se maior exponenciado em face dos ataques perpetrados às grandes empresas e corporações, aos órgãos de relevo dos Estados nacionais no que tange ao gerenciamento de estruturas de natureza tecnológica e segurança, educacional, saúde e infraestrutura energética, sem deixar de lado os próprios usuários residenciais.

Dentre os sujeitos mais atingidos, hasteiam-se as corporações e empresas no sistema privado, eis que a preocupação com a guarida dos negócios, que não raras vezes transpassam as fronteiras, configura-se elemento internacionalmente integrado. A conscientização de funcionários vinculados a tais corporações mediante treinamentos, como uma forma preventiva de afastar e plausivelmente identificar os ataques "camuflados" em e-mails e spams (*phishings*), denota-se uma prática efetiva, a fim de se lograr eficaz governança empresarial, além de prever procedimentos diligentes de tratamento de dados, eloquente em virtude da LGPD, e em casos de "contaminação" ou “vazamento”.

Dentre os países que se debruçam sobre a temática em voga, destacam-se de forma positiva para o presente estudo os casos norte-americano e brasileiro, eis que a criação da agência CISA em vista a proteção dos sistemas governamentais e a PNCiber no Brasil se demonstram similares em seus objetivos, mesmo que distintos em sua atuação e abrangência, e perspectivas. Os profusos pontos comuns de cada ente se convergem e complementam, especialmente porque a globalização dos negócios e de atividades entre governos urgem por integração normatizada além dos tratados internacionais, sendo a analogia apresentada exitosa nesse sentido.

Assim, houve robusto avanço da legislação brasileira na finalidade de proteger o meio ambiente técnico informático empresarial, particularmente no tocante aos negócios e atividades corporativas, havendo uma parceria entre o poder público e empresas privadas a fim de evitar o sucesso dos ataques dirigidos a estas instituições, sendo a CISA um modelo a ser seguido

naquilo que abrange de forma diferente o exercido pela PNCiber. Desta senda, é indispensável atestar que a cooperação internacional é crucial para que os países se agasalhem diante dos mais criativos e perspicazes crimes no Ciberespaço.

Referências

ABEYRATNE, Ruwantissa. Regu/lating Cyber Security. **Legal Priorities in Air Transport**, p. 157-194, 2019.

ALSHEMEILI, Ahmed; Hertelendy, A.; Hart, A.; Alburaid, A.; Benmoussa, G.; Digregorio, D; Caneva, D.; Issa, F.; Ciottone, G. Assessment of Statewide Communication Interoperability Plans (SCIP) Across the United States Using the Cybersecurity e Infrastructure Security Agency (CISA) Interoperability Markers. **Prehospital and Disaster Medicine**, v. 38, n. S1, p. s95-s95, 2023.

BAMBERGER, Kenneth A. Technologies of compliance: Risk and regulation in a digital age. **Tex. L. Rev.**, v. 88, p. 669, 2009.

BARRETO JUNIOR, Irineu Francisco. Proteção da Privacidade e de Dados Pessoais na Internet: O Marco Civil da rede examinado com fundamento nas teorias de Zygmunt Bauman e Manuel Castells. DE LUCCA, Newton; SIMÃO FILHO; Adalberto; DE LIMA; Cintia Rosa Pereira. **(Org.). Direito e Internet III: Marco Civil da Internet**. 1ed. São Paulo: Quartier Latin, v. 2, p. 100-127, 2015.

BAUMAN, Zygmunt. Modernidade líquida. Rio de Janeiro: Jorge Zahar Ed., 2001.

BECK, Ulrich. Risk society: Towards a new modernity. Sage, 1992.

BIONI, Bruno Ricardo. Proteção de dados pessoais: a função e os limites do consentimento. 2. ed. Rio de Janeiro: Forense, 2020.

BRASIL. LEI FEDERAL Nº 12.965/2014, de 23 de abril de 2014. **Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil**. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 11 de out. de 2022. BRASIL.

BRASIL. **LEI FEDERAL Nº 14.155/2021**, de 27 de maio de 2021. Altera o Decreto Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), para tornar mais graves os crimes de violação de dispositivo informático, furto e estelionato cometidos de forma eletrônica ou pela internet; e o Decreto-Lei nº 3.689, de 3 de outubro de 1941 (Código de Processo Penal), para definir a competência em modalidades de estelionato. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/lei/L14155.htm. Acesso em: 11 de out. de 2022.

BRASIL. **DECRETO 11.856/2023**, de 26 de dezembro de 2023. Institui a Política Nacional de Cibersegurança e o Comitê Nacional de Cibersegurança. CRIAÇÃO, POLITICA NACIONAL, SEGURANÇA DIGITAL, OBJETIVO, INSTRUMENTO, COMITE, COMPETENCIA, COMPOSIÇÃO, FUNCIONAMENTO. Disponível em:

https://www.in.gov.br/en/web/dou/-/decreto-n-11.856-de-26-de-dezembro-de-2023-533845289. Acesso em: 02 abr. 2024.

BRUSTOLIN, Vitelio; NUNES, Israel Aono; DE ASSUNÇÃO, Juliana Zaniboni. Análise estrutural das estratégias de segurança cibernética do Brasil e dos Estados Unidos. **Revista Brasileira de Estudos de Defesa**, v. 9, n. 2, 2022.

CASTELLS, Manuel. **A sociedade em rede**. 9. ed. rev. ampl. São Paulo: Paz e Terra, 2006.

CLARK, Mark; ESPINOSA, J.; DELONE, William. **Defending organizational assets: a preliminary framework for cybersecurity success and knowledge alignment**. 2020.

CORRÊA FILHO, Ivan de Sousa. A Segurança cibernética no Brasil: uma análise da situação atual. Rio de Janeiro: ESG, 2016.

DE ARAÚJO NETO, R. J.; AGUIAR, J. J. B. The impacts of the General Data Protection Law (LGPD) on information security: a literature review. **Revista de Gestão e Secretariado,** [S. l.], v. 15, n. 2, p. e3442, 2024. DOI: 10.7769/gesec.v15i2.3442. Disponível em: https://ojs.revistagesec.org.br/secretariado/article/view/3442. Acesso em: 8 abr. 2024.

DONEDA, D., SARLET, I. W., MENDES, L. S., JUNIOR, O. L. R., e BIONI, B. R. **Tratado de proteção de dados pessoais.** Rio de Janeiro: Forense, 2021.

FLORIDI, Luciano; TADDEO, Mariarosaria (Ed.). The ethics of information warfare. **Springer Science e Business Media**, 2014.

GOTTSCHALK NOLASCO, Loreci; MACIEL SILVA, Bruno Dutra. CRIMES CIBERNÉTICOS, PRIVACIDADE E CIBERSEGURANÇA. **Quaestio Iuris (QI)**, v. 15, n. 4, 2022.

GUIMARAES-FILHO, Pedro Andrade; FERNEDA, Arie Scherreier; FERRAZ, Miriam Olivia Knopik. A Proteção de Dados ea Defesa do Consumidor: Diálogos entre o CDC, O Marco Civil da Internet ea LGPD. **Meritum (Belo Horizonte)**, v. 15, n. 2, 2020.

HARRIS, Mark A.; MARTIN, Ronald. Promoting cybersecurity compliance. In: Cybersecurity education for awareness and compliance. **IGI Global**, 2019. p. 54-71.

JAGADISH, Aishwarya; SHANBHOG, Anusha Paniraj. Enhancing Data Protection and Compliance Through Cloud Security Solutions. **International Journal for Multidisciplinary Research**, 2023.

KESAN, Jay P.; HAYES, Carol M. Mitigative counterstriking: Self-defense and deterrence in cyberspace. **Harv. JL e Tech.**, v. 25, p. 429, 2011.

LANZ, Zachary. Cybersecurity risk in US critical infrastructure: An analysis of publicly available US government alerts and advisories. **International Journal of Cybersecurity Intelligence e Cybercrime**, v. 5, n. 1, p. 43-70, 2022.

LESSIG, Lawrence. Code and Other Laws of Cyberspace. New York: Basic Books, 1999.

LÉVY, Pierre. Cibercultura na rede. **Por uma Outra Comunicação: mídia, mundialização, cultura e poder.** Rio de Janeiro: Record, 2003.

LOCASCIO, Dana. Measuring the Effectiveness of the Cybersecurity and Infrastructure Security Act (CISA) of 2015 against the Russian-Ukraine Conflict. 2022. Tese de Doutorado. Utica University.

LOMAS, Elizabeth. Information governance and cybersecurity: Framework for securing and managing information effectively and ethically. In: Cybersecurity for Information Professionals. **Auerbach Publications**, 2020. p. 109-130.

LUCAS, Ropek. **Will CISA be the Savior of State and Local Cybersecurity**?. NASWA Workforce Technology, 2020.

LUHMANN, Niklas. **Social Systems**. Stanford CA: Stanford University Press, 1995.

MADALENA, Juliano. Regulação das fronteiras da internet: Um primeiro passo para uma teoria geral do direito digital. **Revista dos Tribunais**, v. 974, p. 81-110, 2016.

MARTÍNEZ, Jeferson; DURÁN, Javier M. Software supply chain attacks, a threat to global cybersecurity: SolarWinds' case study. I**nternational Journal of Safety and Security Engineering,** v. 11, n. 5, p. 537-545, 2021.

MCMURROUGH, Micaela; FEIN, Ashden; SKEATH, Caleb. CISA Issues Joint Cybersecurity Advisory on Ransomware Trends and Recommendations. **Bank. Law J**, v. 139, n. 5, 2022.

MELAKU, Henock Mulugeta. A dynamic and adaptive cybersecurity governance framework. **Journal of Cybersecurity and Privacy**, v. 3, n. 3, p. 327-350, 2023.

MITTERLEHNER, Birgit. Cyber-Democracy and cybercrime: Two sides of the same coin. **Cyber-Development, Cyber-Democracy and Cyber-Defense: Challenges, Opportunities and Implications for Theory, Policy and Practice**, p. 207-230, 2014.

MORIN, Edgar. **A cabeça bem-feita: repensar a reforma, reformar o pensamento**. Tradução de Eloá Jacobina, 3. ed., Rio de Janeiro, Bertrand Brasil, 2001.

OLMEDO, Jorge Izaguirre; GAVILÁNEZ, Fernando León. Análisis de los ciberataques realizados en América Latina. **INNOVA Research Journal**, v. 3, n. 9, p. 172-181, 2018.

RICH, Samuel. **Enhancing cybersecurity to protect america's data**. Public Policy Center, University of Iowa. ppc. uiowa. edu/publications/enhancing-cybersecurity-protect-americas-data, 2022.

ROBERTSON, Roland. Glocalization: Time-space and homogeneity-heterogeneity. **Global modernities**, v. 2, n. 1, p. 25-44, 1995.

SOLOVE, Daniel J.; HARTZOG, Woodrow. The FTC and the new common law of privacy. **Colum. L. Rev.**, v. 114, p. 583, 2014.

SONI, T.; KAUR, R.; GUPTA, D.; SHARMA, A.; GUPTA, G. **The Cybersecurity Ecosystem: Challenges, Risk and Emerging Technologies**. In: 2023 7th International Conference on Trends in Electronics and Informatics (ICOEI). IEEE, 2023. p. 699-703.

STERNS, Richard Q. **Complementary Approaches or Conflicting Strategies**? Examining CISA and New York's DFS Cybersecurity Regulations as a Harmonizing Framework for a Bilateral Approach to Cybersecurity. Rich. **JL e Tech.**, v. 26, p. 1, 2019.

SZINVELSKI, Mártin Marks; ARCENO, Taynara Silva. A cibersegurança no tratamento de dados pessoais: a chave de ouro para efetividade da lei geral de proteção de dados (lei nº 13.709/2018). **REVISTA DA AGU**, 2022.

WICKI-BIRCHLER, David. The Budapest Convention and the General Data Protection Regulation: acting in concert to curb cybercrime? **International Cybersecurity Law Review**, v. 1, n. 1, p. 63-72, 2020.

YUSIF, Salifu; HAFEEZ-BAIG, Abdul. A conceptual model for cybersecurity governance. **Journal of applied security research**, v. 16, n. 4, p. 490-513, 2021.