REDE
DE PESQUISA
EM GOVERNANÇA
DA INTERNET

Anais do Encontro Anual da Rede de Pesquisa em Governança da Internet

Maio de 2023

VI ENCONTRO DA REDE DE PESQUISA EM GOVERNANÇA DA INTERNET - REDE 2023

FICHA TÉCNICA

ANAIS DA REDE DE PESQUISA EM GOVERNANÇA DA INTERNET-VOL. 6, ISSN 2675-1690

Editores
Maria Vitoria Pereira de Jesus
Rodolfo Avelino

Autores
Christiana Soares de Freitas
Isabelle Brito Bezerra Mendes
Jaqueline Trevisan Pigatto
João Araújo Monteiro Neto
Luis Henrique de Mendes Acioly
Luize Pereira Ribeiro
Maria Fernanda Amorim Fossaluza
Matheus Fernandes da Silva
Renata de Oliveira Miranda Gomes
Rhaiana Caminha Valois

COMITÊ ORGANIZADOR

O VI Encontro da Rede de Pesquisa em Governança da Internet e a publicação dos Anais resultantes deste encontro receberam apoio de: Comitê Gestor da Internet no Brasil - CGI.br, Internet Society - Capítulo Brasil e Programa de Pós-graduação em Ciências Sociais, da Universidade Estadual de Campinas (Unicamp), através de recursos da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior (CAPES)

Internet Society Capítulo Brasil

CAPES

cgi.br

ESTABILIDADE DO CIBERESPAÇO COMO VETOR DE GARANTIA DA CRIPTOGRAFIA NO CENÁRIO SOCIO-LEGAL CHILENO E A GOVERNANÇA DA INTERNET

Luis Henrique de Menezes Acioly, Isabelle Brito Bezerra Mendes, Matheus Fernandes da Silva, João Araújo Monteiro Neto

SUMÁRIO

INTRODUÇÃO....5

CONTEXTO SOCIOPOLÍTICO E PRINCIPAIS ELEMENTOS DO PROJETO DE LEI-QUADRO DE CIBERSEGURANÇA CHILENO....7

O LOCUS TOPOGRÁFICO DA DISCUSSÃO SOBRE CRIPTOGRAFIA NA GOVERNANÇA DA INTERNET....11

"PROMOVENDO A ESTABILIDADE DO CIBERESPAÇO" E A CRIPTOGRAFIA COMO NÚCLEO POLÍTICO DA INTERNET....15

CONCLUSÕES....18

DECLARAÇÃO DE DIVERSIDADE NAS CITAÇÕES....20

REFERÊNCIAS....20

ESTABILIDADE DO CIBERESPAÇO COMO VETOR DE GARANTIA DA CRIPTOGRAFIA NO CENÁRIO SOCIO-LEGAL CHILENO E A GOVERNANÇA DA INTERNET

Luis Henrique de Menezes Acioly[1]
Isabelle Brito Bezerra Mendes[2]
Matheus Fernandes da Silva[3]
João Araújo Monteiro Neto[4]

RESUMO

O presente trabalho tem como foco a regulação do ambiente digital chileno, que se deflagra por ocasião do *Proyecto de Ley-Marco de la Ciberseguridad e Infraestructura Crítica de la Información* e a consequente discussão acerca da Governança em Segurança Cibernética e garantia da criptografia em seu texto. Esta pesquisa tem o fito de analisar a interconexão entre o conteúdo da propositura legislativa e as disposições constantes em mecanismos de Governança da Internet que digam respeito à gestão de cibersegurança e preservação da criptografia. Objetiva-se, ainda, nesse contexto, compreender o sentido e alcance da estrutura delineada no Relatório Final da Comissão Global pela Estabilidade do Ciberespaço e sua relação com soberania digital. Para tanto, optou-se pela metodologia de revisão de literatura, a partir de artigos científicos e acadêmicos e de textos oficiais de entidades públicas e privadas conexas à temática. Tem-se também por referencial teórico o Relatório Sobre Avanços no Campo da Informação e Telecomunicações no Contexto da Segurança Internacional e o Relatório Final da Comissão Global de Estabilidade do Ciberespaço. Considerou-se, ao final, que a regulação da cibersegurança no contexto chileno não é contraposta à criptogra-

[1] Graduando em Direito pelo Centro Universitário Ruy Barbosa (UniRuy). Pesquisador junto ao Grupo de Estudos em Tecnologia, Informação e Sociedade da UNIFOR – GETIS. Pesquisador em Grupo de Pesquisa "Conversas Civilísticas" - UFBA/CNPq. Vice-Presidente do Laboratório de Inovação e Direitos Digitais (LABID²) - UFBA. Contato: acioly10@gmail.com

[2] Advogada. Tax Consultant na EY. Pós- Graduanda em Proteção de Dados e Governança Digital pela UNIFOR. Mestranda em Direito Constitucional pela UFC. Pesquisadora no Grupo de Estudos em Tecnologia, Informação e Sociedade (GETIS). Contato: isabellemendes06@gmail.com

[3] Mestrando em Direito (UFERSA). Pesquisador no Grupo de Estudos em Tecnologia, Informação e Sociedade (GETIS). Advogado OAB/RN. Contato: matheusfernandes@asba.adv.br.

[4] PhD em Direito pela Universidade de Kent no Reino Unido. Mestre em Direito Constitucional pela Universidade de Fortaleza. Professor do Centro de Ciências Jurídicas da Universidade de Fortaleza. Advogado especializado em Proteção de Dados e Privacidade, Presidente da Comissão de Direito Digital da OAB/CE. Contato: joaoneto@unifor.br.

fia, mas que estas se complementam, de forma que ambas têm por objetivo a garantia da estabilidade da rede, tanto quanto à confiabilidade e resiliência, especialmente em cenários de combate a *hacking* governamental. O caráter supranacional condizente às estruturas internacionais, com mandatos para gestar normas não vinculantes, soma o mecanismos político-diplomático ao rol de abordagens que instrumentalizam a preservação da criptografia como meio de garantia de direitos fundamentais no âmbito digital, inclusive o direito de proteção das infraestruturas críticas da internet.

PALAVRAS-CHAVE
Soberania Digital; Mecanismos Criptográficos; Chile; Ciberestabilidade; Governança Multissetorial.

ABSTRACT
The present work focuses on the regulation of the Chilean digital environment that was triggered by the *Proyecto de Ley-Marco de la Ciberseguridad e Infraestructura Crítica de la Información* and the consequent discussion about Governance in Cybersecurity and the guarantee of encryption in its text. This research aims to analyze the interconnection between the content of the legislative proposal and the provisions contained in Internet Governance mechanisms that concern the management of cybersecurity and preservation of cryptography. In this context, the objective is also to understand the meaning and scope of the structure outlined in the Final Report of the Global Commission for the Stability of Cyberspace and its relationship with digital sovereignty. For that, we opted for the literature review methodology, based on scientific and academic articles and official texts from public and private entities related to the theme. Another theoretical reference is the Report on Advances in the Field of Information and Telecommunications in the Context of International Security and the Final Report of the Global Commission on the Stability of Cyberspace. In the end, it was considered that the regulation of cybersecurity in the Chilean context is not opposed to cryptography, but that these complement each other, so that both aim to guarantee the stability of the network, as far as reliability and resilience, especially in government *hacking* scenarios. The supranational nature consistent with international structures, with mandates to generate non-binding norms, adds political-diplomatic mechanisms to the list of approaches that instrumentalize the preservation of cryptography as a means of guaranteeing fundamental rights in the digital sphere, including the right to protect infrastructures internet reviews.

KEY WORDS
Technological Sovereignty; Cryptographic Mechanisms; Chile; Cyberstability; Multistakeholder Governance.

INTRODUÇÃO

A relação crescentemente indissociável entre ser humano e internet tem gerado o recrudescimento da infraestrutura tecnológica associada às redes. A transposição da interação social para o ambiente digital tem condicionado a formação de um ciberespa-

ço que potencializa as ações humanas, até mesmo as maliciosas. Há uma crescente de ataques cibernéticos e ameaças, inclusive a órgãos e entidades governamentais. Observa-se que, desde 2019, órgãos estatais foram o terceiro maior alvo de ataques cibernéticos ao redor do globo (MOYA, 2021). Assim, agentes estatais e não estatais têm aportado esforços no sentido de garantir a estabilidade da internet, especialmente quanto à infraestrutura crítica da informação. Para os Estados, contudo, a segurança cibernética é questão imanente à defesa da segurança nacional e soberania.

No cenário da América-Latina, o Chile consta no rol de países que mais registraram ataques cibernéticos (MOYA, 2021), inclusive em face de estruturas governamentais. Nesse contexto, o ex-presidente chileno, Sebastián Piñera, propôs a elaboração de uma Lei, denominada *Ley-Marco de la Ciberseguridad e Infraestructura Crítica de la Información*, que dispõe sobre mecanismos de prevenção e investigação de ataques cibernéticos, a partir de estruturas de vigilância contínua, cuja proposta se encontra em debate. No entanto, as regulações em sede de vigilância digital se tensionam, potencialmente, com os direitos digitais de privacidade, proteção de dados e sigilo das comunicações.

A criptografia, enquanto medida técnica de garantia de segurança e confidencialidade das interações digitais, têm demonstrado certo conflito com pretensões de autoridades investigativas no contexto cibernético. As *cripto-wars* apontam para episódios de clara atuação estatal em sentido contrário à adoção comercial de criptografia na internet por entes não militares (LIGUORI FILHO; SALVADOR, 2018).

Noutro lado, a crescente difusão de mecanismos criptográficos em aplicações da rede tem contribuído para a efetivação de direitos digitais fundamentais, como a privacidade, confiabilidade e a própria estabilidade da internet. Atores estatais e não estatais da governança da internet têm levantado questões sobre a necessidade de manutenção de mecanismos criptográficos, ainda que em face de questões sensíveis como a persecução a cibercrimes e defesa da segurança da infraestrutura crítica da informação.

Não sem razão, entidades da sociedade civil chilena e latino-americana têm se manifestado no sentido da necessidade de previsão expressa da garantia da criptografia no mencionado projeto de lei (MONTEIRO NETO *et. al.*, 2023), como forma de ponderação da ação estatal e preservação da privacidade digital e segurança da *internet*. Seguindo-se a perspectiva da necessária estabilidade da internet, a ponderação

da ação do Estado Chileno em seu contexto de cibersegurança, alcança novos ares quando reconhecido o caráter global da rede e a possibilidade de influxos na dinâmica regional e global de acesso. Eventual viabilidade jurídica para a quebra da criptografia das comunicações por legislação chilena pode afetar os usuários da internet na América Latina e do mundo como um todo.

Garantir a estabilidade do ciberespaço perpassa por mecanismos multissetoriais e supranacionais, de modo que a discussão sobre a adoção de criptografia ultrapassa a esfera da atuação de uma dada jurisdição. É imprescindível, assim, a compreensão das principais esferas de deliberação multissetorial da governança da internet acerca da importância da criptografia para a internet, essencialmente, no que diz respeito à resiliência de sua infraestrutura crítica e confiabilidade dos seus usuários.

Pretende-se analisar a interconexão entre o conteúdo do *Proyecto de Ley-Marco de la Ciberseguridad e Infraestructura Crítica de la Información* e as disposições constantes em mecanismos de governança da internet. Visa-se, assim, verificar a existência de normas ou orientações de ordem supranacional no escopo de governança da internet sobre criptografia. Busca-se, ainda, compreender o sentido e alcance da estrutura delineada no Relatório Final da Comissão Global pela Estabilidade do Ciberespaço e sua relação com soberania digital.

Para tanto, pretende-se utilizar a metodologia de investigação, privilegiando a interdisciplinaridade da ciência jurídica interseccionada a outras áreas das ciências sociais. Empreendeu-se uma revisão de literatura de abordagem narrativa, materializada por meio de pesquisa bibliográfica de cunho descritivo e natureza qualitativa, coletando-se dados em artigos científicos e acadêmicos, bem como da análise documental de textos oficiais de entidades públicas e privadas.

CONTEXTO SOCIOPOLÍTICO E PRINCIPAIS ELEMENTOS DO PROJETO DE LEI-QUADRO DE CIBERSEGURANÇA CHILENO

A análise do contexto que antecede as discussões acerca da cibersegurança no Chile perpassa, eminentemente, pela exploração das tensões sociais e políticas visualizadas no país. É certo que as bases para pensar um panorama regulatório que trate do tema há muito tempo vêm sendo desenvolvidas, mas a sua expansão está relacionada com movimentos constitucionais e legislativos mais profundos.

A crescente ocorrência de ataques e incidentes cibernéticos despertaram no país a urgência na busca por adoção de estratégias para alcançar, minimamente, níveis de cibersegurança. Rapidamente, se incorpora então, o discurso da segurança nacional e da soberania, que, transportados às agendas políticas, vão impulsionar movimentos para pensar estruturas de respostas aos problemas visualizados. Há, nesse sentido, específica distinção entre segurança cibernética e defesa cibernética, sendo essa mais voltada à soberania e aquela, com escopo na persecução criminal de crimes digitais (RIBAS; PORTELA, 2021) influenciando esferas distintas de atuação estatal no ciberespaço.

Isso pode ser exemplificado pela criação, no ano de 2009, da *Comissión de trabajo interministerial conducente a la adhesión de Chile a la convención sobre ciber delitos del consejo de Europa,* por meio do Decreto 3265. Em nível internacional, a participação do Chile na União Internacional de Telecomunicações (UIT) também remete à busca pelo amadurecimento no tema (LISBOA, 2022). A inclusão da temática na agenda política do Chile corresponde, então, à relevância que isto ganha no cenário internacional, sobretudo pela expansão da virtualidade. A partir disso, novos desafios ganham espaço e problemáticas sobre segurança nacional rearranjam-se no centro do debate político.

Moya (2021) destaca um quadro evolutivo no desenvolvimento de uma institucionalização de políticas e iniciativas relacionadas à cibersegurança. O referido autor, didaticamente, estabelece cinco marcos temporais que representam diferentes visões sociopolíticas: (i) construção de uma infraestrutura de informação; (ii) solidificar a estrutura por meio da educação, acesso e da capacitação; (iii) estratégia digital 2007-2012, que desenha a utilização intensiva das TICs; (iv) inclusão digital e desenvolvimento de serviços e; (v) desenvolvimento digital vinculado aos setores de produção.

Percebe-se que o país vem se aparelhando em uma perspectiva estrutural há muito tempo, no desenvolvimento de medidas que visem o debate e a incorporação de temáticas sobre segurança cibernética. Desde o ano de 1999, a agenda de cibersegurança ganha robustez no cenário nacional, o que ensejou a criação de cinco instrumentos de planejamento: "*Chile: Hacia la sociedad de la informacion*"; "*Agenda Digital: Te acerca al futuro*"; "*Estratégia Digital*"; *"Agenda Digital: Imagina Chile*"; e *"Agenda Digital"* (MONTEIRO NETO *et. al.*, 2023).

No ano de 2017, o país estabeleceu a Política Nacional de Cibersegurança (PNC), com vistas ao desenho de políticas sobre o tema a curto e médio prazo, precisamente para o período compreendido entre os anos de 2017-2022 (CHILE, 2017). A PNC representou um primeiro movimento interno sistemático de Estado para a concretização de medidas que efetivamente discutam a segurança, a gestão de riscos e a cooperação institucional sobre o tema (LISBOA, 2022). Insta acentuar que a PNC reconhece expressamente a criptografia como tecnologia que fornece um alto nível de confidencialidade e integridade para a informação, sendo uma estratégia relevante para a segurança cibernética chilena, ao passo que estabelece medidas que promovam a adoção da criptografia *end-to-end* pelos usuários (MONTEIRO NETO *et. al.*, 2023).

A discussão sobre cibersegurança ganhou novos contornos a partir da apresentação do *Projeto de Ley-Marco sobre Ciberseguridad e Infraestructura Crítica de la Información* perante o legislativo chileno (*Boletín nº 14.847-06*), por iniciativa do ex-Presidente da República chilena, *Sebástian Piñera* (CHILE, 2022). À luz dessa propositura legislativa, cibersegurança[5] seria:

> O conjunto de ações voltadas ao estudo e gerenciamento das ameaças e riscos de incidentes de cibersegurança; à sua prevenção, mitigação e resposta, bem como à redução dos seus efeitos e dos danos causados, antes, durante e após a sua ocorrência, no que diz respeito aos bens e serviços informáticos[6] (CHILE, 2022).

No bojo do *Boletín nº 14.847-06*, a mensagem que acompanhou o texto normativo trouxe parâmetros de interpretação da proposta. Segundo o escopo da proposta legislativa, a preponderância da própria consolidação da segurança da informação no âmbito do aparato estatal, bem como a regulação do tema junto aos particulares é notória. Nesse contexto, o referido Projeto de Lei busca viabilizar a supervigilância, estabelecendo meios para o exercício do Poder de Polícia no âmbito digital (MONTEIRO *et. al.*, 2023).

Para tanto, o texto normativo defere à Agência Nacional de Cibersegurança a prerrogativa de enfrentar ameaças à infraestrutura crítica da informação e implementar

[5] Nesse sentido, a União Internacional das Telecomunicações (UIT) define cibersegurança como o conjunto de ferramentas, políticas, conceitos de segurança, salvaguardas de segurança, diretrizes, métodos de gestão de risco, ações, treinamento, melhores práticas, seguros e tecnologias que podem ser usadas para proteger ativos da organização e usuários no ambiente cibernético (UIT, 2018).

[6] Tradução Livre de “el conjunto de acciones destinadas al estudio y manejo de las amenazas y riesgos de incidentes de ciberseguridad; a la prevención, mitigación y respuesta frente a estos, así como para reducir sus efectos y el daño causado, antes, durante y después de su ocurrencia, respecto de los activos informáticos y de servicios”.

ações preventivas, sem, contudo, especificar garantias mínimas aos cidadãos nesse contexto (MONTEIRO NETO *et. al.*, 2023). Nesse cenário, a opacidade do processo investigativo, bem como a ausência de parâmetros para o estabelecimento de ações preventivas têm o condão de viabilizar uma quebra permanente da privacidade digital (MONTEIRO NETO *et. al.*, 2023).

Contudo, tratar de cibersegurança somente no escopo estatal carrega uma série de riscos que mitigam a legitimidade do Estado em dispor sobre o âmbito privado, ainda que se trate de segurança cibernética. Nesse sentido, Hurel e Lobato (2018) sintetizam em quatro os desafios da atuação estatal na cibersegurança: (i) risco de militarização da cibersegurança; (ii) risco de exclusão dos demais *stakeholders* da governança da internet do âmbito da discussão sobre as prioridades até a implementação de políticas públicas; (iii) preferência de soluções que se fundem no bloqueio de aplicativos e remoção judicial de conteúdo; (iv) risco de politização da coordenação e problemas de transferência de tecnologia.

Como se observa, a exclusão de agentes não estatais da discussão de cibersegurança contribui para a militarização da política de segurança cibernética (CEPIK *et. al.*, 2014), ao passo que o bloqueio judicial de aplicativos ou remoção de conteúdo eleva a tensão entre a abordagem com foco na criminalização de condutas e a abordagem de proteção de direitos fundamentais digitais (HUREL; LOBATO, 2018; RIBAS; PORTELA, 2021). A abordagem da segurança cibernética como soberania digital tem levado ao estabelecimento de um novo domínio militar no ciberespaço (DOUZET; GÉRY, 2021).

Assim, entidades da sociedade civil chilena e latino-americana têm se movimentado para garantir que a defesa da infraestrutura crítica da informação seja ponderada com a observância da Criptografia ponta-a-ponta nesse Projeto de Lei, dentre as quais a Aliança para a Criptografia na América Latina e Caribe – AC-LAC, que encaminhou carta aberta ao Senado Chileno com esse objetivo (AC-LAC, 2022).

Por conseguinte, a busca pela garantia da criptografia no texto legal tem recebido influxos a partir do contexto social de preservação e avanço dos direitos digitais no Chile, bem como apoia-se em um prisma supranacional de preservação da estabilidade do ciberespaço, oriundo de mecanismos de governança da internet.

O *LOCUS* TOPOGRÁFICO DA DISCUSSÃO SOBRE CRIPTOGRAFIA NA GOVERNANÇA DA INTERNET

Vigilância é instrumento de poder (ROGAWAY, 2021). Na sociedade em rede, como pensada por Castells (2002), não é somente *malwares*, *ransomwares* e *hackers* que apresentam riscos à privacidade dos usuários da rede. O Estado, no exercício do seu poder-dever fiscalizatório, também tangencia a vigilância dos seus cidadãos, especialmente no tocante à defesa e segurança nacional (CEBIK *et. al.*, 2014). Embora a vigilância seja algo já inerente à dinâmica da relação de poder do Estado, o advento da internet concedeu às agências estatais aparatos tecnológicos suficientes para uma larga capacidade para monitoramento das comunicações privadas (ROGAWAY, 2021).

Em um contexto de desenvoltura temporal das tecnologias, a interceptação das comunicações deixou de ser um relevante instrumento de vigilância, dada a transferência das comunicações para o cenário da mensageria por aplicações (RAMIRO *et. al.*, 2022). A busca por mecanismos efetivos de vigilância estatal conduziu o mercado da tecnologia à exploração de pesquisa comercial no desenvolvimento de instrumentos de exploração de vulnerabilidades na integridade de dispositivos, tendo em vista a extração de informações em massa (RAMIRO *et. al.*, 2022).

A criptografia, nesse contexto, tem o papel de proteção da privacidade de informações através da codificação de dados de forma que apenas os interlocutores tenham condições técnicas para acessar o conteúdo da mensagem ou das informações de navegação na rede (LANZA, 2019; COSTA, 2021). No âmbito das comunicações privadas, tem-se a criptografia de dados em trânsito, que se refere ao mecanismo de proteção de informações transportadas de um computador para outro, seja no de tráfego na rede ou formulário na web, seja no envio de mensagens de texto por e-mail ou aplicativo (LIGUORI, 2022). Essa criptografia pode ser aplicada à camada de transporte, atuando no protocolo *HTTP - HyperText Transfer Protocol Secure*, através do protocolo *TLS – Transporty Layer Securty* ou *SSL – Secure Sockets Layer*, impedindo que terceiros tenham acesso à atividade do usuário em determinado site (LIGUORI, 2022). Ou, pode ser aposta em aplicações de comunicações, denominando-se criptografia ponta-a-ponta:

> A ideia desse mecanismo é, de forma simplificada, cifrar o conteúdo da mensagem no dispositivo do emissor a partir da chave pública do receptor e ela só poder ser decifrada no dispositivo do receptor a partir de sua chave privada. Nessa lógica, mesmo se houver um servidor central que encaminhe a mensagem a um usuário do sistema, ele não

> conseguirá acessar o conteúdo da mensagem, uma vez que não possui a chave para tanto (LIGUORI, 2022, p. 17).

A adoção de mecanismos criptográficos, justamente por impedir o acesso de terceiros, também estabelece certos limites à atuação estatal (COSTA, 2019). Por essa razão, autoridades investigativas têm denominado essas tecnologias como "*Going Dark*" (LIGUORI FILHO; SALVADOR, 2018), pois sustentam que, à medida em que se acresce a distância entre a autoridade estatal e a sua viabilidade técnica, o Poder Público se torna cada vez mais ineficaz, impedido de realizar a colheita de provas de crimes, que vão desde a pedofilia e pornografia infantil à tráfico de drogas e terrorismo (CAPRONI, 2011). No ponto de vista político, é possível observar coalizões contra a criptografia, simbolizadas pelo que se convencionou denominar "*Five Eyes*", grupo político formado pelos Estados de Austrália, Canadá, Estados Unidos, Nova Zelândia e Reino Unido (COSTA, 2021), sob o enfoque da guerra ao terrorismo e proteção de suas vítimas.

O panorama de restrição de mecanismos criptográficos por regulação estatal pode ser sintetizado a partir do trabalho de Liguori Filho *et. al.* (2018), que elencaram cinco categorias de ações: (i) criminalização ou proibição da criptografia; (ii) limitação do tamanho de chaves criptográficas; (iii) obrigação genérica de assistência; (iv) obrigação específica de assistência; (v) necessidade de autorização governamental para criptografia.

Contudo, o "*caso Snowden*", de 2013, a partir das revelações acerca de um sofisticado esquema de vigilância estatal americano, inclusive contra autoridades de diversos Estado-Nações, teve o condão de trazer à tona a discussão sobre segurança cibernética e privacidade digital (LIGUORI, 2022; ROGAWAY, 2021). Nesse cenário, a agência norte-americana contava com sofisticados mecanismos de exploração de vulnerabilidade de sistemas e raspagem de dados pessoais, especialmente, de provedores de aplicações da rede (LIGUORI, 2022; COSTA, 2021), atuação atribuída com espécie de *hacking governamental*. O "*efeito Snowden*" modificou substancialmente a dinâmica das relações na internet, de forma que diversos provedores de aplicações passaram a implementar sistemas de criptografia por padrão (LIGUORI FILHO; SALVADOR, 2018), seja em camada de transporte, ou ponta-a-ponta.

A compreensão de *hacking* governamental se traduz como um meio superação de mecanismos de segurança por autoridades públicas, mediante exploração de vul-

nerabilidades de sistemas informáticos, para acesso a determinadas informações sem necessidade de comunicação com o provedor, habilitando novas formas de produção digital de provas e vigilância (RAMIRO *et. al.*, 2021). Para se configurar um *hacking* são necessários dois fatores: (i) um de ordem técnica, concernente à exploração da vulnerabilidade que resulte no acesso não autorizado de uma informação e; (ii) outro de ordem comportamental, concernente à intencionalidade do agente em violar um sistema de segurança da informação (RAMIRO *et. al.*, 2022).

À guisa de exemplo, a utilização do sistema *Galileo* da *Hacking Team* (DE ACHA, 2016) pelo Estado chileno – cujo nome foi modificado para *Phantom* no país – teve por notória a elevada instabilidade e risco à privacidade dos usuários da internet, que estariam ou manteriam conexões com residentes do Chile (PARTARRIEU; JARA, 2015). Ramiro *et. al.* (2022) explicam que o *hacking* governamental pode ocorrer a partir do controle físico do aparelho, em que há a extração em massa de dados, inclusive com quebra da criptografia ou superação de sistemas de autenticação digital. Também pode ocorrer a partir do acesso remoto ao dispositivo por meio da exploração de vulnerabilidade não conhecida pelo fabricante, o que concede acesso total ou parcial ao aparelho (RAMIRO *et. al.*, 2022).

Nesse cenário, a criptografia se impõe como conceito necessário à pauta da governança da internet, com consequências na própria estabilidade da rede. Com o avanço das tecnologias e ante os efeitos sociais decorrentes da internet (CORDEIRO, 2021; GEORGE, 2011), a estabilidade do ciberespaço é objeto de esforços globais, por Estado-Nações e *stakeholders* não estatais. Essa noção é visualizada tanto no que diz respeito à dispersão geográfica dos atores, oriundos de diversos *backgrounds*, que agem para o desenvolvimento da internet (ANASTÁCIO, 2015), demonstrando o caráter global e aberto da rede, quanto em função do multissetorialismo.

A governança da internet perpassa por um modelo multissetorial. O multissetorialismo, enquanto princípio da governança das redes, pressupõe a definição de papéis dos atores, isoladamente considerados, e a forma como eles se interconectam (KURBALIJA, 2016). Como apontam Canabarro e Wagner (2014, p. 13), a governança da internet tem como caminho a “harmonização e integração de uma série de regimes técnicos e político-jurídicos que organizam a ação coletiva nos níveis sistêmico, regional e nacional e abarcam múltiplas áreas da vida social”.

A Estabilidade da Internet é um conceito aberto, cuja definição decorre de um exercício de validação da perspectiva social e histórica da rede. Ao mesmo tempo, realizar esta delimitação conceitual tem uma função estratégica no futuro da governança da internet. Em busca de exprimir esforços, a Comissão Global sobre Estabilidade do Ciberespaço propõe que esse conceito seja apreendido a partir do binômio “confiança do usuário” e “resiliência ante o avanço tecnológico” (GCSC, 2022). Tem-se a dimensão de confiança do usuário, pois as decisões humanas estão baseadas em suas percepções, de forma que a sensação de segurança no uso da internet tem o condão de direcionar os seus usos. Por outro lado, a resiliência é tida como elemento da estabilidade, pois com o avanço da tecnologia da informação, é necessário que a rede se mantenha, ainda sim, disponível e íntegra em suas funcionalidades. Indo-se além, Kurbalija (2016) propõe para a estabilidade da rede, uma abordagem de introdução gradual de mudanças extensivamente testadas na infraestrutura técnica.

Um importante exemplo do esforço de agentes não estatais na estabilidade da rede a partir de mecanismos criptográficos é o *Request For Comments* (RFC) n. 7696 da *Internet Engineering Task Force – IETF*, que estabelece diretrizes de Criptografia para melhor prática na internet (IETF, 2015). O RFC n. 7696 tem a primazia em estabelecer protocolos de migração e adaptação de algoritmos de implementação obrigatória (*mandatory-to-implement algorithm*), de forma que crie viabilidade para manutenção da criptografia ao longo do tempo, e em face de mudanças de paradigmas tecnológicos.

No escopo dos agentes estatais, em esforço supranacional, a Assembleia Geral das Nações Unidas estabeleceu um Grupo de Especialistas Governamentais sobre Desenvolvimentos no Domínio da Informação e Telecomunicações no Contexto da Segurança Internacional (GGE – ONU) (ASSEMBLEIA GERAL DAS NAÇÕES UNIDAS, 2013). A atuação desses especialistas resultou em um documento intitulado “Relatório Sobre Avanços no Campo da Informação e Telecomunicações no Contexto da Segurança Internacional”, que, além de reforçar o benefício de mecanismos de participação de diversos setores privados, trouxe normas sobre a relação de Estados com as TICs (ASSEMBLEIA GERAL DAS NAÇÕES UNIDAS, 2015).

Entre essas normas, há expressa menção à necessidade de os Estados tomarem medidas razoáveis para garantir a integridade da cadeia de suprimentos, de modo a que os usuários finais possam ter confiança na segurança dos produtos e serviços de Tecnologia da Informação (ASSEMBLEIA GERAL DAS NAÇÕES UNIDAS, 2015).

Essa normatização se correlaciona diretamente à necessidade manutenção da dimensão subjetiva da estabilidade, a confiança dos usuários.

"PROMOVENDO A ESTABILIDADE DO CIBERESPAÇO" E A CRIPTOGRAFIA COMO NÚCLEO POLÍTICO DA INTERNET

Para além da compreensão isolada dos atores que compõem o ecossistema de governança da internet, há frutos de seus trabalhos em conjunto. Nesse sentido, a Comissão Global pela Estabilidade do Ciberespaço (GCSC – *Global Commission on the Stability of Cyberespace*) representou espaço de discussão multissetorial, culminando na formulação do Relatório Final "Promovendo a Ciberestabilidade" (GCSC, 2022).

Apesar da existência de diversas formas de estabelecimento de um modelo multissetorial de governança muito ínsito às diversas conformações de estruturas de poder (SOLAGNA, 2020), a importância da GCSC se descortina, na medida em que se constitui como espaço destinado para que os diversos *stakeholders* aportem conhecimentos e perspectivas para ciberestabilidade.

> Nomeadamente, a própria Comissão é multissetorial e global, uma vez que é composta por indivíduos com conhecimentos e históricos diversos. Alguns Comissários atuaram no governo e participaram em negociações bilaterais e multilaterais sobre questões cibernéticas, enquanto outros têm experiência na construção, manutenção e proteção da própria Internet. Outros representaram a sociedade civil (GCSC, 2022, pp. 31-32).

A Comissão Global pela Estabilidade do Ciberespaço foi estabelecida com o mandato de "desenvolver propostas de normas e políticas para melhorar a segurança e a estabilidade internacionais", agindo de forma suplementar às diretrizes já elencadas no Relatório Sobre Avanços no Campo da Informação e Telecomunicações no Contexto da Segurança Internacional, do GGE-ONU (GCSC, 2022). O Relatório "Promovendo a Ciberestabilidade" teve sua estrutura delineada no estabelecimento de Princípios, Normas e Recomendações (GCSC, 2022). Os princípios buscam empreender comportamentos dos *stakeholders* da Governança da Internet, a partir dos ditames de:

> Responsabilidade: Todos são responsáveis por garantir a estabilidade do ciberespaço. Restrição: Nenhum ator estatal ou não estatal deve tomar medidas que prejudiquem a estabilidade do ciberespaço. Obrigatoriedade de Ação: Os atores estatais ou não estatais devem tomar medidas razoáveis e apropriadas para assegurar a estabilidade do ciberespaço. Respeito aos Direitos Humanos: Os esforços para garantir a estabilidade do ciberespaço devem respeitar os direitos humanos e o Estado de Direito (GCSC, 2022, p. 25).

A seu turno, as normas materializam comandos a serem seguidos pelos *stakeholders* a partir da concretização dos princípios acima assinalados. Dentre as oito normas elencadas pela Comissão, encontra-se expressamente:

> Os atores estatais e não estatais não devem conduzir nem permitir conscientemente atividades que prejudiquem intencionalmente e substancialmente a disponibilidade geral ou a integridade do núcleo público da Internet e, por conseguinte, a estabilidade do ciberespaço; […] Todos os atores têm o dever de compartilhar informações sobre vulnerabilidades, a fim de ajudar a prevenir ou mitigar atividades cibernéticas maliciosas; […] Os atores não estatais não devem participar em operações cibernéticas ofensivas e os atores estatais devem prevenir essas atividades e responder caso elas ocorram (GCSC, 2022, pp. 25-26).

Tais normas guardam estreita correlação com o panorama chileno de regulação do cibersegurança pois, ao passo que o núcleo político da internet, em que se encontra a discussão sobre criptografia, é objeto de especial proteção, também há norma que impõe aos agentes estatais o dever de prevenção de operações cibernéticas ofensivas, ou de garantia da segurança cibernética. Nesse sentido, a regulação chilena aporta confluência com essas questões, ao adotar uma postura preventiva e reativa quanto à cibersegurança, de vigilância digital permanente, pondo em risco os mecanismos criptográficos (MONTEIRO NETO *et. al.*, 2023).

Os mecanismos criptográficos denotam especial relevância na cibersegurança, de forma que a inclusão de *backdoors* ou outros mecanismos que venham a desconstituir a criptografia para um usuário específico, enfraquece essa tecnologia para todos os usuários da rede (SVANTESSON, 2019; COSTA, 2021). O desenvolvimento e aplicação de mecanismos que mitiguem a criptografia ponta-a-ponta, *exempli gratia*, para cumprimento de decisão judicial em caso específico, representa risco a outras formas de criptografia, como a de camada de transporte, pondo em vulnerabilidade os demais usuários da rede, que poderão ter seus dados acessados por agentes maliciosos.

De outro lado, a exploração de vulnerabilidades desconhecidas pelos fabricantes - o que pode ser vista como uma forma de *hacking governamental* - cria uma série de riscos técnicos e sociais para a internet, tendo em vista a superação do intermediário na obtenção de dados (RAMIRO *et. al.*, 2022). O rompimento da cadeia de confiança entre usuário e provedor da aplicação, além de esvaziar o conteúdo dos negócios privados pelos quais os usuários confiam seus dados (RAMIRO *et. al.*, 2022), mitigam

a confiabilidade na própria internet, restringindo um dos requisitos para a estabilidade do ciberespaço.

Destaca-se que questões que envolvem a segurança cibernética, por se confundirem com a própria segurança e soberania nacional, têm se desenvolvido de forma a endereçar medidas estatais como a localização forçada de empresas e de dados e vigilância digital estatal (SVANTESSON, 2019). Ressalta Cerf (2019), que, a defesa da rede contra-ataques externos, contudo, demanda de uma pesquisa exaustiva e esforços diplomáticos entre Estado-Nações, para que de forma criativa se realize a inibição ou mitigação de seus efeitos e a consequente indicação dos responsáveis.

O estabelecimento de normas pela Comissão Global representa um avanço em relação ao Grupo de Especialistas Governamentais da ONU, pois elucida questões por eles não abordadas. Nesse sentido, a Comissão Global ressalta que embora o GGE-ONU tenha elaborado norma de proteção da infraestrutura crítica da rede, não restou esclarecido se o Núcleo Político da Internet estaria coberto por esse termo (GCSC, 2022).

O Núcleo Político da Internet é, assim como ciberestabilidade, um conceito abstrato, porém estratégico (LOVELUCK, 2018). A Comissão Global define o Núcleo Político da Internet como sendo os “elementos críticos da infraestrutura da Internet, tais como roteamento e encaminhamento de pacotes, sistemas de nomes e números, mecanismos criptográficos de segurança e identidade” (GCSC, 2022, p. 78). A abrangência da proteção aos mecanismos criptográficos nesta norma direciona para elementos como (i) chaves criptográficas usadas para autenticar usuários e dispositivos e transações seguras na Internet; (ii) equipamentos, instalações, informações, protocolos e sistemas que permitem a produção, comunicação, uso e descontinuação dessas chaves; (iii) servidores de chaves PGP, Autoridades Certificadoras e sua Infraestrutura de Chaves Públicas; o (iv) design, produção e cadeia de abastecimento de equipamentos usados para implementar processos criptográficos, entre outras faces tecnológicas (GCSC, 2022).

Nesse mesmo sentido, como reforço argumentativo em favor da indissociabilidade da criptografia da proteção de direitos digitais, o Comitê Gestor da Internet do Brasil apresentou Nota Pública contra a adoção de “*backdoors*” ou “chaves-mestras” em sistemas criptográficos, ressaltando que “mecanismos criptográficos sólidos são fundamentais à integridade e segurança de sistemas digitais, ao sigilo empresarial,

bem como à garantia da inimputabilidade da rede e da funcionalidade, segurança e estabilidade da Internet" (COMITÊ GESTOR DA INTERNET, 2019, p. 2).

Por conseguinte, em face de uma propositura legislativa que tem em seu cerne a permissão à supervigilância estatal como meio de exercício de Poder de Polícia no âmbito digital, com parâmetros opacos do sistema investigatório conduzido por uma Agência Nacional de Cibersegurança (MONTEIRO NETO *et. al.*, 2023), a criptografia teria o condão de ponderar os direitos de privacidade digital e confiança do usuário. Dessa forma, depreende-se que, com a garantia legal da criptografia ter-se-á um contexto de segurança cibernética mais robusto, proporcional e estável, em que se demonstra a proteção do cidadão frente ao próprio Estado.

Para além disso, sob a ótica macro-estrutural da formulação de políticas públicas de segurança cibernética, é necessário ter como escopo a estruturação de uma Governança em Segurança Cibernética (HUREL; LOBATO, 2018; HUREL, 2021), que ponha em foco a atuação multissetorial na construção de normas com essa temática. A Governança em Segurança Cibernética se refere a uma visão holística e integrada da segurança das redes, dos sistemas e serviços e das infraestruturas em uma sociedade, incluindo, por conseguinte, "instituições, iniciativas, políticas, programas e entre outros mecanismos (formais e informais) que integram um ecossistema de competências e responsabilidades distribuídas para a segurança cibernética" (HUREL, 2021, p. 7).

Como componente temático da Governança em Segurança Cibernética, a adoção de meios de proteção à criptografia se coaduna a um conjunto de esforços na implementação de uma cultura de cibersegurança, tendo por alvo a proteção da pessoa, usuário da internet, e as instituições que fundam sua atuação na rede, protegendo a própria cidadania.

CONCLUSÕES

A partir do empreendimento da pesquisa, tem-se como conclusão a necessidade de inserção da discussão sobre a criptografia nos mecanismos supranacionais e multissetoriais de Governança da Internet, para além da compreensão da atividade jurisdicional de determinado Estado-Nação. A compreensão da internet como uma rede aberta global pressupõe que suas características essenciais não sejam substancialmente alteradas em determinados espaços jurisdicionais, mas que seus elementos

sejam garantidos como fundamento para o desenvolvimento cooperativo de Estados--Nações e indivíduos.

Nesse cenário, a tecnologia criptográfica, em toda a sua extensão, pode ser compreendida como estrutura lógica e técnica da segurança da rede e, por conseguinte, da sua estabilidade, seja através do prisma subjetivo de confiabilidade, seja no enfoque objetivo de resiliência, ganhando especial relevo na Governança da Internet em nível global. É necessário, assim, consignar a não rivalidade entre a preservação da criptografia e a segurança cibernética nacional, pois ambos decorrem do dever inerente aos *stakeholders* estatais e não estatais em defesa do Núcleo Político da Internet e suas infraestruturas.

Os mandatos do Grupo de Especialistas da ONU e da Comissão Global pela estabilidade do Ciberespaço representam a materialização dessa não rivalidade, na medida em que representantes estatais e não estatais reconhecem o dever de os Estados não interferirem na cadeia de suprimentos da internet, nem em seu núcleo político. Conclui-se, assim, que a expressa menção à criptografia como núcleo político da internet enseja um grau de reconhecimento supranacional da necessidade de sua proteção, denotando força político-diplomática como reforço argumentativo em seu favor. A criptografia, como medida de preservação da privacidade digital e segurança da informação, tem seu reconhecimento político-diplomático como elemento técnico indispensável à moderação da atuação estatal em sua vigilância e investigação criminal.

Portanto, conclui-se que a regulação da cibersegurança no contexto chileno, a partir do projeto de lei objeto deste estudo, para que forneça viabilidade político-social no contexto de uma internet livre, aberta, universal e inclusiva, depende da observância da preservação da criptografia. A Estabilidade da Rede garantida através de mecanismos criptográficos, diante do histórico político chileno e latino-americano de manejo de instrumentos de *hacking* governamental, tem o potencial de legitimar as ações estatais de preservação da infraestrutura crítica da informação por meio da ponderação entre o dever estatal de segurança nacional e direitos digitais dos usuários. Em âmbito macro-estrutural, a formulação de políticas de segurança cibernética a partir da preponderância do Estado tem o condão de gerar insuficiências protetivas que, além de enfraquecer a proteção a direitos fundamentais, atua em violar-lhes.

DECLARAÇÃO DE DIVERSIDADE NAS CITAÇÕES

Por meio desta declaração, nos juntamos a um esforço coletivo para desfazer o apagamento epistemológico estrutural na academia contra mulheres, pessoas não binárias, negres, do Sul global, e de outros grupos sociais, cujas vozes são menos ouvidas devido ao viés encontrado em citações. Acreditamos que a transparência em relação às nossas bibliografias é fundamental para compreender o presente, e alterar esse quadro estrutural de maneira conjunta e consistente. Compartilhamos que neste artigo, as citações se distribuem da seguinte forma: nomes femininos (15%), masculinos (50%), feminino-masculino (12,5%), e fontes institucionais (22,5%).

REFERÊNCIAS

A AC-LAC pede para incluir criptografia no projeto de Lei-Quadro de Segurança Cibernética e Infraestrutura Crítica da Informação do Chile. **AC-LAC**. 2022. Disponível em: <https://ac-lac.org/pt/a-ac-lac-pede-para-incluir-criptografia-no-projeto-de-leiquadro--de-seguranca-cibernetica-e-infraestrutura-critica-da-informacao-do-chile/>. Acesso em: 17 nov. 2022.

ANASTÁCIO, Kimberly. **Participação na governança da Internet**: o multissetorialismo do Comitê Gestor da Internet no Brasil (CGI.br). 2015. 59 f., il. Monografia (Bacharelado em Ciência Política). Universidade de Brasília, Brasília, 2015. Disponível em: <https://bdm.unb.br/handle/10483/12753>. Acesso em: 03 mai. 2023.

ASSEMBLEIA GERAL DAS NAÇÕES UNIDAS. Relatório do Grupo de Especialistas Governamentais sobre Desenvolvimentos no Domínio da Informação e Telecomunicações no Contexto da Segurança Internacional, A/68/98 (24 de junho de 2013). Disponível em: <https://undocs.org/A/68/98>. Acesso em: 03 abr. 2023.

ASSEMBLEIA GERAL DAS NAÇÕES UNIDAS. Relatório do Grupo de Especialistas Governamentais sobre Desenvolvimentos no Domínio da Informação e Telecomunicações no Contexto da Segurança Internacional, A/70/174 (22 de julho de 2015). Disponível em: <https://undocs.org/A/70/174>. Acesso em: 03 mai. 2023

CANABARRO, Diego Rafael; WAGNER, Flávio Rech. A Governança da Internet: Definição, Desafios e Perspectivas. In: 9º Encontro da Associação Brasileira de Ciência Política, 2014, Brasília - DF. **Anais Eletrônicos da ABCP**, 2014

CAPRONI, Valerie. Going Dark: Lawful electronic surveillance in the face of new technologies. In: **Hearing before the subcommittee on crime, terrorism and homeland security of the House Committee on the Judiciary**, 2011. Disponível em: <https://archives.fbi.gov/archives/news/testimony/going-dark-lawful-electronic-surveillance-in--the-face-of-new-technologies>. Acesso em: 05 mai. 2023.

CASTELLS, Manuel. **A sociedade em rede**. Trad. Roneide Venâncio Majer. 6. ed. São Paulo: Paz e Terra, 2002.

CERF, Vint. G. Questões e desafios da governança da Internet nas Américas. In: BELLI, Luca; CAVALLI, Olga (org). **Governança e regulações da Internet na América Latina**: análise sobre infraestrutura, privacidade, cibersegurança e evoluções tecnológicas em homenagem aos dez anos da South School on Internet Governance. Rio de Janeiro: Escola de Direito do Rio de Janeiro da Fundação Getulio Vargas, 2019, p. 7-11.

CEPIK, Marco; CANABARRO, Diego Rafael; BORNE, Tiago. A securitização do ciberespaço e o terrorismo: uma abordagem crítica. In: SOUZA, André de Melo; NASSER, Reginaldo Mattar; MORAES, Rodrigo Fracalossi (orgs.). **Do 11 de setembro de 2001 à guerra ao terror**: reflexões sobre o terrorismo no século XXI. Brasília: IPEA, 2014, p. 161-186.

CHILE. Ministerio del Interior y Seguridad Pública. **Política Nacional de Ciberseguridad (PNCS)**. 2017. Disponível em: <https://biblioteca.digital.gob.cl/handle/123456789/738>. Acesso em 08 abr. 2023.

CHILE. Senado. **Proyecto de Ley Marco sobre Ciberseguridad e Infraestructura Crítica de la Información**. Disponível em: <https://www.senado.cl/appsenado/templates/tramitacion/index.php?boletin_ini=1484>7-06. Acesso em: 09 jan. 2023.

COMITÊ GESTOR DA INTERNET. **Nota Pública sobre o uso de criptografia em sistemas e dispositivos conectados à Internet**. 2019. Disponível em <https://www.cgi.br/esclarecimentos/ver/nota-publica-sobre-o-uso-de-criptografia-em-sistemas-e-dispositivos-conectados-a-internet.pdf>. Acesso em: 07 mai. 2023.

CORDEIRO, Luís; LOURENÇÃO, Humberto; SOL, Eduardo. Perspectivas do Estado Brasileiro para o Ciberespaço. In: **Revista Hoplos**, v. 4, n. 6, p. 11-25, 6 mar. 2021. Disponível em: <https://doi.org/10.0000/hoplos.v4i6.36360>. Acesso em 03 mai. 2023.

COSTA, André Barbosa Ramiro. **Políticas de encriptação**: entre a codificação de direito, regulação política e o cipher-ativismo. 2021, 165 f. Dissertação (Mestrado) – Universidade Federal de Pernambuco. CIn, Ciência da Computação, Recife, 2021. Disponível em: <https://repositorio.ufpe.br/handle/123456789/42872>. Acesso em: 07 mai. 2023.

COSTA, Diogo Erthal Alves da. Nemo tenetur se detegere e dados criptografados: restabelecendo o equilíbrio. In: SALGADO, Daniel Resende; QUEIROZ, Ronaldo Pinheiro de (Orgs.). **A prova no enfrentamento à macrocriminalidade**. Salvador: JusPodivm, 2019, p. 209-252.

DOUZET; Frédérick; GÉRY, Aude. Cyberspace is used,first and foremost, to wage wars: proliferation, security and stability in cyberspace. In: **Journal of Cyber Policy**, v. 6, n. 1, 2021, p. 96-113. Disponível em: <https://doi.org/10.1080/23738871.2021.1937253>. Acesso em: 26 jun. 2023.

DE ACHA, Gisela Pérez. Hacking Team: malware para la vigilancia en América Latina. **Derechos Digitales**, 25 abr. 2016. Disponível em: <https://www.apc.org/fr/node/21624>. Acesso em: 10 nov. 2022.

GEORGE, Eric. Da “sociedade da informação” à “sociedade 2.0”: o retorno dos discursos “míticos” sobre o papel das TICs nas sociedades. In: **Líbero**, São Paulo, v. 14, n. 27, p. 45-54, jun. de 2011. Disponível em: <https://seer.casperlibero.edu.br/index.php/libero/article/view/362>. Acesso em: 04 mai. 2023.

GCSC - Comissão Global sobre a Estabilidade do Ciberespaço. **Promovendo a ciberestabilidade**. Trad. Ana Zuleika Pinheiro Machado. São Paulo: Comitê Gestor da Internet do Brasil, 2022.

HUREL, Louise Marie. **Cibersegurança no Brasil**: uma análise da estratégia nacional. São Paulo: Instituto Igarapé, 2021.

HUREL, Louise Marie; LOBATO, Luiza Cruz. **Uma Estratégia para a Governança da Segurança Cibernética no Brasil**. São Paulo: Instituto Igarapé. 2018.

IETF - Internet Engineering Task Force. Request for Comments n. 7696, Guidelines for Cryptographic Algorithm Agility and Selecting Mandatory-to-Implement Algorithms. November, 2015. Disponível em: <https://www.rfc-editor.org/rfc/rfc7696>. Acesso em 03 abr. 2023.

KURBALIJA, Jovan. **Uma introdução à governança da internet**. Trad. Carolina Carvalho. São Paulo: Comitê Gestor da Internet no Brasil, 2016.

LANZA, Edison. Os princípios que garantem uma Internet livre, aberta e inclusiva para todas as pessoas e grupos sociais. In: BELLI, Luca; CAVALLI, Olga (org). **Governança e regulações da Internet na América Latina**: análise sobre infraestrutura, privacidade, cibersegurança e evoluções tecnológicas em homenagem aos dez anos da South School on Internet Governance. Rio de Janeiro: Escola de Direito do Rio de Janeiro da Fundação Getulio Vargas, 2019, p. 539-556.

LIGUORI, Carlos. **Direito e criptografia**. São Paulo: Saraiva, 2022.

LIGUORI FILHO, Carlos Augusto; SALVADOR, João Pedro Favaretto. Crypto wars e bloqueio de aplicativos: o debate sobre regulação jurídica da criptografia nos Estados Unidos e no Brasil. In: **Revista da Faculdade de Direito UFPR**, Curitiba, PR, Brasil, v. 63, n. 3, p. 135-161, set./dez. 2018. ISSN 2236-7284. Disponível em: <https://revistas.ufpr.br/direito/article/view/59422>. Acesso em: 07 mai. 2023.

LIGUORI FILHO, Carlos Augusto; SANTOS, Guilherme Kenzo; SALVADOR, João Pedro Favaretto. Direito e Criptografia: tendências legislativas e debate público internacional. In: POLIDO, Fabrício. ANJOS, Lucas. BRANDÃO, Luíza. (Org.). Seminário Governança das Redes. Belo Horizonte. **Anais do III Seminário Governança das Redes: políticas, internet e sociedade**. Belo Horizonte: Iris, 2018, p. 266-271.

LISBOA, Cícero Araújo. **A securitização do combate ao cibercrime no século XXI**: um estudo sobre a América do Sul. 2022, 149 f. Dissertação (Mestrado). Universidade Federal do Rio Grande do Sul. Faculdade de Ciências Econômicas. Programa de Pós-Graduação em Estudos Estratégicos Internacionais, Porto Alegre, 2022. Disponível em: <https://www.lume.ufrgs.br/handle/10183/238889>. Acesso em 16 mai. 2023.

LOVELUCK, Benjamin. **Redes, liberdades e controle**: Uma genealogia política da internet. Petrópolis: Vozes, 2018.

MONTEIRO NETO, João Araújo; GALVÃO, Alex Renan; MENDES, Isabelle Brito Bezerra; SÁ, Iago Capistrano; ALVES, Letícia; ACIOLY, Luis Henrique de Menezes; SILVA, Matheus Fernandes da. O uso da criptografia como um mecanismo de combate à vigilância estatal e a proteção de garantias e direitos fundamentais – uma avaliação sócio-legal da proposta regulatória chilena. In: CANTO, Mariana; SARAIVA, Raquel; SOUZA, Michel (coord.). **Relatório regional sobre políticas e liberdades no uso de criptografia na América Latina e no Caribe**. Recife: IP.rec, 2023, p. 18-24.

MOYA, Santiago Aguayo. **A política nacional de cibersegurança do Chile**: análise a partir da abordagem dos múltiplos fluxos para as políticas públicas. 2021, 118 f. Dissertação (Mestrado em Ciências Militares). Escola de Comando e Estado Maior do Exército, Rio de Janeiro, 2021. Disponível em: <https://www.bdex.eb.mil.br/jspui/handle/123456789/9900>. Acesso em 07 mai. 2023.

PARTARRIEU, Barbara; JARA, Matías. Los Correos que Alertaron Sobre la Compra del Poderoso Programa Espía de la PDI. **CIPER Centro de Investigación Periodística**, 10 jul. 2015. Disponível em: <http://ciperchile.cl/2015/07/10/los-correos-que-alertaron-sobre-la-compra-del-poderoso-programa-espia-dela-pdi/>. Acesso em: 08 jan. 2023.

RAMIRO, André; AMARAL, Pedro; PEREIRA, Marcos Cesar M. Insegurança Distribuída: Economia e Regulação do Hacking Governamental. In: IV Encontro da Rede de Pesquisa em Governança da Internet. Online. **Anais da Rede de Pesquisa em Governança da Internet - Vol. 4**. [S.l], 2021, p. 1-29.

RAMIRO, André; AMARAL; Pedro; CANTO, Mariana; PEREIRA, Marcos Cesar. **Mercadores da insegurança:** conjuntura e riscos do hacking governamental no Brasil. Recife: Instituto de Pesquisa de Recife, 2022.

RIBAS, Georgia Maria Vasconcelos Pfeilsticker; PORTELA, Lucas Soares. Governança Internacional no mundo Cibernético: Desafios para a defesa e segurança cibernética. In: III Simpósio de Defesa e Ciência Política da Universidade Federal de Pernambuco, Recife, 2021. **Anais do III Simpósio de Defesa e Ciência Política da Universidade Federal de Pernambuco**. Recife, 2021, p. 7-15.

ROGAWAYA, Phillip. **O Caráter Moral do Trabalho Criptográfico**. Trad. André Ramiro. Recife: Ed. do Autor, 2021.

SOLAGNA, Fabricio. **30 anos de governança da Internet no Brasil**: Coalizões e ideias em disputa pela rede. 2020. 300 f. Tese (Doutorado) - Universidade Federal do Rio Grande do Sul, Instituto de Filosofia e Ciências Humanas, Programa de Pós-Graduação em Sociologia, Porto Alegre, BR-RS, 2020. Disponível em: <https://lume.ufrgs.br/handle/10183/212954>. Acesso em: 04 mai. 2023.

SVANTESSON, Dan Jerker B. **Internet & jurisdição**: relatório de status global 2019. Trad. Ana Zuleika Pinheiro Machado. São Paulo: Comitê Gestor da Internet no Brasil, 2020.

UNIÓN INTERNACIONAL DE TELECOMUNICACIONES (UIT). **Guía para la elaboración de una estrategia nacional de ciberseguridad - Participación estratégica en la ciberseguridad**. Genebra: UIT, 2018. Disponível em: <https://www.itu.int/dms_pub/itud/opb/str/D-STR-CYB_GUIDE.01-2018-PDF-S.pdf>. Acesso em: 03 jul. 2023.