Ordem e progresso?
Analisando as respostas brasileiras aos cibercrimes

Mariana Grilli Belinotte | *Luiz Rogério Franco Goldoni* | *Joe Devanny* | *Carlos Frederico Coelho*

INTRODUÇÃO

O presente artigo analisa a reação do Estado brasileiro em relação a dois casos emblemáticos de violação de sistemas e dados: o vazamento das fotos íntimas da atriz Carolina Dieckmann, em 2012, e a revelação, por Edward Snowden e pelo grupo Wikileaks, que as comunicações de cidadãos brasileiros, incluindo as da então Presidente da República, Dilma Rousseff, eram monitoradas pelo Governo estadunidense. Assim, investiga-se a influência desses acontecimentos na aprovação de dois diplomas legais sobre crimes cibernéticos e proteção de dados: no primeiro caso, a Lei N.º 12.737/2012 – Lei Carolina Dieckmann –, e, no segundo, a Lei Geral de Proteção de Dados (Lei N.º 13.709/2018).

O objetivo geral do artigo é averiguar como Estados reagem legalmente a violações de sistemas e dados com ampla repercussão na sociedade. Os objetivos específicos são: *a*) analisar as reações legislativas ao incidente Carolina Dieckmann e *b*) ao caso Snowden, e *c*) contrastá-las para compreender as diferenças e semelhanças entre os casos. A hipótese apresentada é a de que casos de alta repercussão aceleram ou intensificam as ações governamentais voltadas à cibersegurança. Neste artigo, a investigação foi restrita às respostas legislativas aos incidentes, reconhecendo-se que há uma série de outras respostas possíveis, como reorganizações orçamentárias ou institucionais, pronunciamentos ou decisões judiciais. Justifica-se a escolha do tema pois o estudo de processos

RESUMO

A ameaça cibernética tornou-se questão cada vez mais proeminente nos últimos anos. Embora global, o problema afeta alguns países mais do que outros. Este é o caso do Brasil, que se tornou um ponto focal para ataques cibernéticos. O principal objetivo do artigo é analisar as reações do Estado brasileiro a cibercrimes de alto perfil. O artigo fornece uma visão contextual de como incidentes significativos moldaram a resposta legislativa do Brasil ao cibercrime, principalmente na Lei Geral de Proteção de Dados e na Lei Carolina Dieckmann. Contribui para uma agenda de pesquisa focada em analisar como e por que algumas atividades são criminalizadas, enquanto outras não o são, ajudando também a compreender as prioridades e percepções de diferentes Estados.

Palavras-chave: cibersegurança, cibercrime, Lei Geral de Proteção de Dados, Lei Carolina Dieckmann, Brasil.

ABSTRACT

Order and progress? An analysis of Brazilian responses to cybercrime

The cyber threat has become an increasingly important issue in →

 https://doi.org/10.23906/ri2024.82a07

recent years. Although the problem is global, it affects some countries more than others. This is the case in Brazil, which has become a focal point for cyber attacks. The main goal of this article is to analyze the Brazilian state's responses to high-profile cybercrimes. The article provides a contextual overview of how significant incidents have shaped Brazil's legislative response to cybercrime, particularly in the General Data Protection Law and the Carolina Dieckmann Law. It contributes to a research agenda focused on analyzing how and why some activities are criminalized while others are not, and also helps to understand the priorities and perceptions of different states.

Keywords: cybersecurity, cybercrime, General Data Protection Law, Carolina Dieckmann Law, Brazil.

específicos de criminalização (ou de não criminalização, como no incidente Snowden) demonstra as prioridades e o entendimento dos atores sobre aspectos como a importância do valor afetado, as sanções consideradas adequadas, os procedimentos a serem realizados, etc.

Os casos foram escolhidos por suas diferenças: o incidente Dieckmann foi de natureza privada. Seus valores protegidos foram a privacidade e a intimidade, e culminou na aprovação de uma lei penal, que criminalizou a invasão e a manipulação de sistemas e o acesso a dados pessoais. Já o monitoramento de empresas brasileiras e autoridades nacionais e internacionais por outros Estados tem caráter eminentemente público – envolveu, também, a privacidade, mas, devido ao perfil das vítimas, ganhou conotações mais amplas, por ter aspectos relacionados à soberania e à segurança nacional. Nesse caso, a resposta igualmente envolveu a promulgação de uma lei, mas não de natureza penal, ou seja, não criou ou alterou um tipo penal (ou crime, como entende o público em geral). Ademais, a resposta ao caso Snowden também foi acompanhada de ações diplomáticas voltadas às discussões sobre a governança global do ciberespaço.

Nas seções seguintes, serão tratados a criminalização em geral, o fenômeno dos cibercrimes e o contexto do Brasil na questão. Após, analisa-se os casos Dieckmann e Snowden. A discussão sobre os casos é realizada à luz de questões internas inerentes ao Brasil e sua posição nas discussões globais sobre a governança da internet.

CRIMINALIZAÇÃO

Nesta seção, será explicado o que é e como ocorre a criminalização, ou seja, de que maneira uma ação se torna proibida e penalmente punível. Também se discutirá, brevemente, os direitos e garantias e sua importância para o direito penal, as causas e motores da criminalização, a efetividade do direito penal, e a criminalização nos casos em tela – incidentes Dieckmann e Snowden.

Criminalização é o processo que torna uma conduta penalmente sancionável dentro de um ordenamento jurídico. Na criminalização, uma atividade é identificada[1] como proscrita, e uma pena é imposta para as pessoas que a praticam – privação de liberdade, pagamento de multas, suspensão de direitos, práticas reeducativas, ou mesmo a pena capital. Nos Estados contemporâneos, os atores responsáveis pela definição das condutas proibidas são, em geral, os legisladores, e o meio competente é a lei[2].

Os legisladores e demais agentes implicados na coibição das práticas criminalizadas (juízes, promotores, policiais, advogados, agentes penitenciários) devem respeitar garantias e direitos típicos do Estado democrático de direito. Não é, e não pode ser, um vale-tudo, como

desde o século XVIII foi observado por Rousseau. As garantias processuais, os limites da criminalização, os benefícios da execução penal, o direito à ampla defesa, ao contraditório e ao tratamento digno, mesmo após a condenação, são conquistas civilizatórias e estão, no Brasil, consagradas na Constituição Federal e na legislação infraconstitucional.

Esse arcabouço básico de direitos humanos também aparece na forma de tratados internacionais, que definem limites ao poder interno dos países de legislar e definir crimes, como o Pacto de San Jose da Costa Rica. No entanto, cada Estado ainda define o que é crime em seu território. Logo, o crime é uma construção coletiva de uma determinada sociedade, em uma determinada época, e varia de acordo com o local e o tempo[3].

Em teoria, a criminalização teria como objetivo diminuir a frequência de uma atividade considerada indesejável pela sociedade. Na realidade, esse processo pode ocorrer devido a outros fatores: pressão da população ou da mídia, desejo das autoridades de demonstrar ação, atos discriminatórios e repressão contra minorias, ou busca por um aumento do prestígio e/ou do orçamento de forças policiais, por exemplo.

Duas últimas áreas de análise discutem a efetividade da criminalização: uma busca entender o grau de sucesso na transformação de determinadas condutas em crime; a outra investiga a eficiência da criminalização – em outras palavras, averigua se a criminalização de uma atividade reduz sua prática. Isto é especialmente importante quando a dimensão «tempo» é considerada, em situações que envolvem o avanço tecnológico. O direito, enquanto processo socialmente construído, apresenta grande dificuldade em reagir aos avanços tecnológicos na mesma velocidade em que estes ocorrem. Tal qual sugerido por Gutwirth, De Hert e De Sutter[4], o direito busca, inicialmente, responder aos novos desafios utilizando regras já existentes. A criação de novas normas, assim, geralmente se dá num segundo momento, o que é o eixo de análise deste trabalho.

No caso Dieckmann, ocorreu um processo de criminalização movido, em parte, pela comoção causada na sociedade, na mídia e nos atores políticos após o incidente. Condutas relacionadas a invadir computadores ou manipular dados passaram a ser puníveis com até um ano de prisão, respeitadas as garantias e direitos. Já no caso Snowden, houve a promulgação da Lei Geral de Proteção de Dados (LGPD), que só prevê sanções administrativas. Ou seja, o legislador não se utilizou da LGPD para criminalizar as condutas ali descritas – embora elas possam ser crimes com base em outras leis.

Ressalta-se que as características acima descritas da criminalização – o processo social de designar uma sanção para uma conduta coletivamente entendida como indesejada, respeitando o devido processo legislativo e as garantias e direitos aplicáveis ao caso – permanecem válidas ao se falar de cibercrimes, como demonstrado acima. Mas os cibercrimes possuem peculiaridades e subdivisões próprias, como será analisado a seguir.

CIBERCRIMES

Esta seção aborda as características do ciberespaço que alteram as condições para o cometimento de ilícitos (ação à distância, anonimato, aumento do número de alvos em

potencial e ação transnacional) e o descompasso entre o surgimento das novas tecnologias – e por conseguinte, dos novos delitos – e os sistemas legais, especialmente, como no caso do Brasil, aqueles de orientação romano-germânica. Versa, ainda, sobre a amplitude das condutas denominadas «cibercrimes», ou «crimes cibernéticos», e apresenta uma possível classificação.

Em primeiro lugar, o ciberespaço altera as formas de relacionamento interpessoais possíveis. As peculiaridades inerentes a esse domínio possibilitam um distanciamento entre os criminosos e suas vítimas, o que aumenta potencialmente o número de alvos do transgressor[5]. Além disso, mediante o mesmo código malicioso ou ação de *phishing* um cibercriminoso pode causar danos a um número incalculável de alvos. A impessoalidade do ataque somada a técnicas relativas à ocultação de rastros dificulta a identificação dos perpetradores[6] e, consequentemente, na punição desses. Além disso, há empecilhos na investigação e na punição de crimes em que os suspeitos estão em outros países. A sensação de impunidade cria no coletivo a imagem do ciberespaço como uma «terra sem lei», fato que por um lado estimula as ações dos cibercriminosos e, por outro, causa insegurança nos demais cidadãos, principalmente naqueles não muito afeitos à tecnologia.

A SENSAÇÃO DE IMPUNIDADE CRIA NO COLETIVO A IMAGEM DO CIBERESPAÇO COMO UMA «TERRA SEM LEI», FATO QUE POR UM LADO ESTIMULA AS AÇÕES DOS CIBERCRIMINOSOS E, POR OUTRO, CAUSA INSEGURANÇA NOS DEMAIS CIDADÃOS.

Em segundo lugar, a tecnologia está sempre «um passo a frente» das normas. O surgimento de uma nova tecnologia acarreta, inevitavelmente, o surgimento de uma série de novas ameaças, riscos e ilícitos. Esses fenômenos não existiam e não eram conhecidos, até o momento em que novas técnicas e sistemas são implementados: «nenhum dispositivo técnico pode desenvolver-se sem, por sua vez, gerar o ‹seu› acidente específico»[7] e, acrescentamos, não podem ser desenvolvidos sem darem origem a tipos novos e específicos de delitos. Em outras palavras e exemplificando: os acidentes aéreos e as normas relativas à aviação apenas surgiram com a invenção do avião.

Esse descompasso é mais perceptível nos sistemas jurídicos de inspiração romano-germânica[8]. Nos sistemas anglo-saxões, de tradição consuetudinária, baseada em precedentes, é possível, observados os limites constitucionais, utilizar ferramentas como a analogia e a interpretação extensiva para resolver dilemas cujas soluções ainda não foram codificadas. É daí que surge, por exemplo, a abundante literatura acadêmica estadunidense dos anos 1990 que discutia a aplicabilidade de conceitos jurídicos como «propriedade» e «privacidade» no ciberespaço, e suas possíveis consequências legais[9]. Isso não é possível nos países que adotam os princípios romano-germânicos, em que, geralmente, apenas a lei pode criar deveres e sanções.

Por fim, o cibercrime é de difícil conceituação e classificação, principalmente devido à multiplicidade de finalidades e meios envolvidos. Cibercrime[10] pode envolver desde *malwares* sofisticados até ações de engenharia social, pode ter como finalidade obter recursos financeiros, disseminar mensagens de ódio ou perseguir e humilhar indivíduos; pode ser cometido

por um indivíduo, por grupos criminosos, ou por atores organizados por Estados. Nesse sentido, Gordon e Ford[11] propõem compreender o cibercrime de acordo com sua duração e sua dependência no uso de *crimewares*[12]. Em termos de duração, existiriam os incidentes discretos, que ocorreriam em um único episódio, como o uso de um *trojan* para acessar dados pessoais e transferir recursos financeiros, e os contínuos – *ciberstalking*, espionagem, cooptação de membros para redes terroristas, pornografia infantil, chantagem e extorsão, etc.

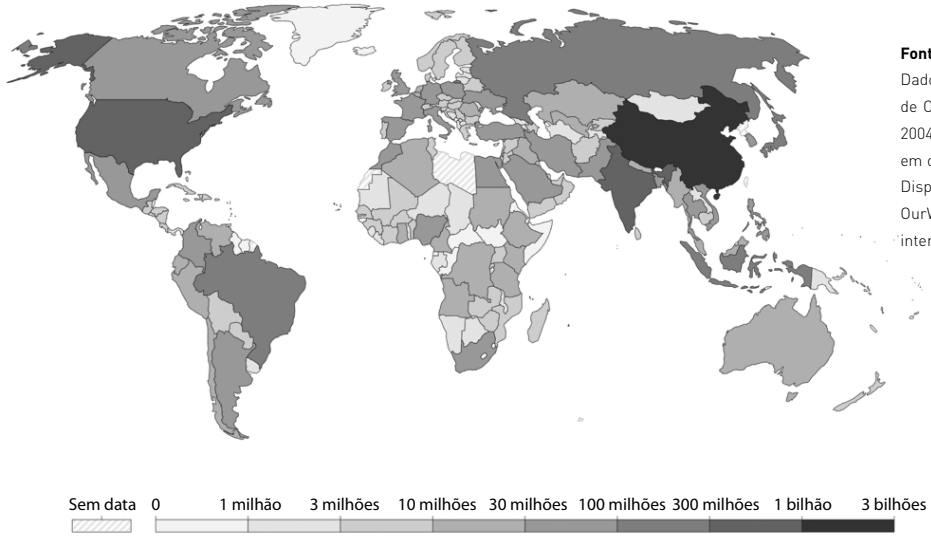
Em relação a dependência do uso de *crimeware* para o cometimento dos delitos, a classificação se daria em um *continuum*, com um dos extremos sendo o das fraudes inteiramente dependentes dessas ferramentas, como transferências de dinheiro de bancos centrais a partir da captura do controle do sistema por meio de um vírus, e, do outro, ações que se utilizam do ciberespaço e de ferramentas de uso comum como apps de mensagens, redes sociais, *websites*, jogos virtuais, para a prática de fraudes, estelionato, *bullying*, etc.[13].

O cibercrime é difícil de ser medido, devido à diversidade de formatos e à subnotificação. Por isso, as informações sobre o contexto de um país ou região em relação a essa ameaça são, por vezes, pouco precisas. No entanto, alguns dados podem ser obtidos em documentos oficiais de organismos internacionais, na imprensa e nos relatórios de companhias de segurança cibernética. Na seção seguinte, será apresentado o panorama do Brasil nesse contexto, relacionando-o a seu entorno e à situação geopolítica global.

CONTEXTO BRASILEIRO

O Brasil é um dos países mais populosos do mundo e, como tal, natural que seja também um dos países com maior número de usuários de internet do planeta, conforme se depreende da figura 1.

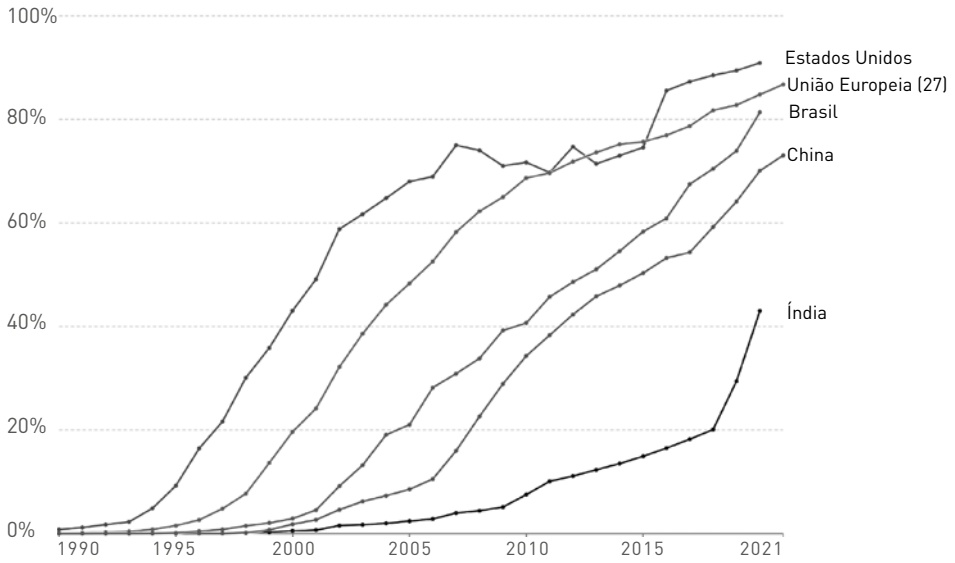
Figura 1 > Número total de usuários de internet do planeta



Fonte: Dados extraídos de Our World Data, 2004. Consultado em dezembro de 2023. Disponível em: OurWorldInData.org/internet.

Seus números relativos de usuários de internet são igualmente expressivos e maiores que aqueles encontrados em países em desenvolvimento como a China e a Índia, sendo apenas um pouco aquém dos números encontrados na Europa e nos Estados Unidos, conforme pode ser observado na figura 2.

Figura 2 > Número relativo de usuários de internet: Brasil, China, Índia, Estados Unidos e União Europeia



Fonte: Dados extraídos de Our World Data, 2004. Consultado em dezembro de 2023. Disponível em: OurWorldInData.org/internet.

Portanto, é natural que, em razão dos números acima mostrados, o Brasil apresente um arcabouço legislativo substantivo quanto à legislação atinente ao ciberespaço. Em seu relatório de cibersegurança global (RCG), de 2020, a União Internacional das Telecomunicações (em inglês, International Telecommunication Union) dá a nota máxima possível ao Brasil, quanto às medidas legais existentes no país na temática de cibersegurança[14]. A tabela a seguir apresenta as notas obtidas por alguns países da América Latina; dentre os países em desenvolvimento da região, o Brasil apresenta a melhor pontuação.

Tabela 1 > Pontuação do RCG 2020 da União Internacional das Telecomunicações – países da América Latina

Pontuação: Medidas Legais (0-20)	
Brasil, Canadá, Estados Unidos	20,0
Costa Rica	17,62

[Cont.]

Chile	17,20
México	15,61
Uruguai	13,90
Colômbia	9,14

Fonte: Elaboração própria, com dados do RCG (União Internacional das Telecomunicações, 2021).

Na temática de cibercrimes, a estrutura legislativa brasileira é relativamente enxuta, baseando-se primordialmente na Constituição do país, que comparativamente a outros, é relativamente jovem (1988), e em legislação infraconstitucional específica trazida em anos posteriores, entre as quais se destacam o Marco Civil da Internet (Lei N.º 12.965/2014), LGPD (Lei N.º 13.709/2018) e, mais recentemente, a Lei N.º 14.155/2021. De maneira intencional, a Lei N.º 12.737/2012 será objeto de análise específica em seção posterior, por configurar objeto do presente artigo.

O Marco Civil da Internet estabelece princípios, garantias, direitos e deveres relativos ao uso da internet no Brasil. Foi nesse momento que foram introduzidas definições de dados pessoais e tratamento de dados pessoais aplicáveis ao ambiente *online*, bem como normas de segurança a serem adotadas pelos provedores de conexões e fabricantes de aplicativos no armazenamento de dados pessoais e comunicações privadas.

Por sua vez, a LGPD tornou-se a principal fonte legislativa do ciberespaço brasileiro, apesar de não estabelecer especificamente a regulamentação de segurança cibernética. A LGPD estabeleceu a Agência Nacional de Proteção de Dados como ator central na imposição de sanções administrativas e na regulação de parâmetros sobre a temática.

Em abril de 2023, o Brasil tornou-se signatário da Convenção de Budapeste. Trata-se de importante marco, formal e internacional, que une o país ao tratado assinado originalmente por países europeus no início do século[15], para a cooperação no combate e investigação de crimes cibernéticos. Tal qual será assinalado na próxima seção, chama a atenção que entre a assinatura e a posterior adoção da convenção no ordenamento jurídico interno, transcorreram mais de 20 anos.

CASOS DIECKMANN E SNOWDEN

O CASO DIECKMANN TRATA DA INTIMIDADE DE UM INDIVÍDUO, ENQUANTO O CASO SNOWDEN CAUSOU ALARME EM RELAÇÃO À SOBERANIA E À SEGURANÇA NACIONAL.

Como mencionado na Introdução, os casos Dieckmann e Snowden foram selecionados devido a suas diferenças. Pode-se dizer que são dois extremos de crimes cibernéticos, tanto quanto é possível ocorrer na realidade: o caso Dieckmann trata da intimidade de um indivíduo, enquanto o caso Snowden causou alarme em relação à soberania e à segurança nacional, após as revelações de que a então Presidente do Brasil, Dilma Rousseff, fora monitorada pelos Estados Unidos. Um deles – Dieckmann –, culminou na aprovação-relâmpago de uma lei penal, que prevê a prisão de quem acessar dados

e sistemas de terceiros sem autorização. O segundo levou ao estabelecimento de princípios e garantias gerais para o tratamento de dados pessoais. Nas subseções seguintes, serão analisados os incidentes em si, a repercussão de cada um, o processo de aprovação e o conteúdo dos dois diplomas legais em tela – a Lei Carolina Dieckmann e a LGPD.

CASO CAROLINA DIECKMANN

No dia 6 de maio de 2012, o jornal *O Estado de S. Paulo* noticiou que fotos íntimas da atriz Carolina Dieckmann haviam sido divulgadas, e estavam entre os assuntos mais comentados da rede social Twitter[16]. Nos dias e semanas seguintes, o tema foi continuamente abordado em matérias de jornal e televisão. Uma semana depois, em 14 de maio de 2012, os suspeitos foram encontrados, por meio do rastreamento de seus endereços IP. Foi provado que eles obtiveram as fotos a partir do *e-mail* da atriz, e, em seguida, passaram a chantageá-la, pedindo dinheiro em troca da não divulgação das imagens[17].

Os suspeitos foram acusados de difamação, furto e extorsão qualificada. No entanto, a conduta de invadir sistemas e acessar dados pessoais de terceiro ainda não era tipificada no ordenamento jurídico brasileiro: o Projeto de Lei N.º 84, de 1999 (Projeto Azeredo), por exemplo, buscava criminalizar a ação de *hackers* e *crackers*, e tramitava no Congresso Nacional, então por mais de doze anos, sem que fosse aprovado[18].

Essa demora não afligiu a Lei Carolina Dieckmann, cuja velocidade de tramitação surpreendeu até mesmo o Presidente da Câmara dos Deputados à época, Marco Maia (PT-RS)[19]. O projeto original, submetido à apreciação da Câmara Baixa em novembro de 2011, foi aprovado pelos deputados em 15 de maio de 2012 – menos de dez dias após a repercussão do vazamento das fotos[20]. Após envio ao Senado Federal, o projeto retornou à Câmara dos Deputados para a aprovação final no início de novembro do mesmo ano.

Em síntese, a lei acrescentou dois artigos ao Código Penal Brasileiro, além de marcar a primeira vez que a legislação penal pátria alcançaria, de maneira específica, crimes cibernéticos. A partir de então, quedou tipificada penalmente tanto a invasão de dispositivo informático quanto a interrupção de serviços informáticos. As penas estabelecidas pela Lei Carolina Dieckmann seriam alteradas quase dez anos depois, em 2021, através da Lei N.º 14.155/2021 de modo a punir com ainda maior rigor os crimes cibernéticos nela contidos. Hoje, é possível encontrar 77 projetos de lei em tramitação relacionados a crimes cibernéticos na Câmara dos Deputados[21].

CASO SNOWDEN

As revelações feitas por Edward Snowden em 2013, expondo o alcance global do monitoramento conduzido pela agência de segurança nacional dos Estados Unidos (NSA)[22], provocaram uma reavaliação significativa das práticas de segurança e privacidade de dados em todo o mundo. O ex-analista da NSA revelou que informações da alta cúpula

dos governos brasileiro[23], alemão[24] e francês[25] e da empresa Petrobrás[26] eram monitoradas pela agência estadunidense.

No contexto brasileiro, essas revelações tiveram impactos nas relações diplomáticas, manifestados no cancelamento da visita que a Presidente Dilma Rousseff faria aos Estados Unidos em setembro daquele ano[27] e no discurso de abertura da Assembleia Geral das Nações Unidas, proferido por Rousseff em 2013[28], classificado como um «ataque feroz à espionagem dos EUA»[29]. Internamente, as revelações impulsionariam a consolidação do Centro de Defesa Cibernético, estabelecido em 2012, e a criação do Comando de Defesa Cibernético, em 2016 (este, incorporando o Centro, criado em 2012)[30], e desencadeariam reflexões que influenciaram diretamente a criação e aprovação da LGPD em 2018.

O processo de elaboração da LGPD teve início com a apresentação do Projeto de Lei N.º 4060/2012, que visava criar uma legislação específica para a proteção de dados pessoais[31]. O debate sobre a necessidade de uma legislação abrangente para a proteção de dados ganhou força principalmente após as revelações de Snowden, que provocaram uma crescente conscientização sobre a vulnerabilidade dos dados pessoais em um mundo digital interconectado.

O DEBATE SOBRE A NECESSIDADE DE UMA LEGISLAÇÃO ABRANGENTE PARA A PROTEÇÃO DE DADOS GANHOU FORÇA PRINCIPALMENTE APÓS AS REVELAÇÕES DE SNOWDEN, QUE PROVOCARAM UMA CRESCENTE CONSCIENTIZAÇÃO SOBRE A VULNERABILIDADE DOS DADOS PESSOAIS.

A sociedade brasileira, em transição para uma economia digital, demandou medidas mais robustas para proteger sua privacidade em um ambiente virtual. A LGPD, nesse sentido, surgiu como uma resposta legislativa a essas preocupações crescentes. O Brasil reconheceu a necessidade de estabelecer uma legislação abrangente que regulamentasse o tratamento de dados pessoais, equilibrando a inovação tecnológica com a proteção dos direitos individuais. A lei não apenas reflete as demandas internas por maior segurança de dados, mas também incorpora uma resposta ao ambiente internacional pós-Snowden, no qual a privacidade se tornou uma questão central nas discussões sobre governança digital[32].

A tramitação do projeto de lei no Congresso Nacional envolveu debates como a definição de dados sensíveis, os princípios para o tratamento de dados, as responsabilidades das empresas e as penalidades por descumprimento[33]. A adequação da legislação à realidade das pequenas e médias empresas foi um ponto sensível, buscando-se equilibrar a proteção dos direitos dos cidadãos com a viabilidade econômica[34].

A necessidade de compatibilidade com padrões internacionais também foi outro ponto relevante nos debates. A sociedade brasileira estava atenta às discussões globais sobre privacidade e proteção de dados, influenciada, em parte, pelas revelações de Snowden sobre a vigilância em massa. Isso impulsionou a busca por uma legislação alinhada com padrões internacionais, reforçando a posição do Brasil como um ator global comprometido com a proteção da privacidade[35].

No âmbito legislativo brasileiro, as revelações de Snowden influenciaram os debates em torno da LGPD, moldando as discussões e ampliando a conscientização sobre a importância de proteger a privacidade em um cenário de crescente digitalização. A legislação, por sua vez, incorporou princípios fundamentais que refletem as preocupações suscitadas por Snowden, tais como a transparência no tratamento de dados, o respeito à privacidade e a necessidade de consentimento para coleta e processamento de informações pessoais[36].

A trajetória da LGPD no Congresso Nacional reflete a complexidade inerente à elaboração de uma legislação que busca equilibrar interesses diversos. Audiências públicas, debates e convites a especialistas foram realizados na Comissão de Ciência e Tecnologia, Comunicação e Informática e na Comissão Especial para Tratamento e Proteção de Dados Pessoais, criada especialmente para debater o projeto, bem como nos plenários da Câmara dos Deputados e do Senado Federal[37]. A participação ativa da sociedade civil nas audiências públicas desempenhou um papel crucial na identificação de preocupações e na sugestão de aprimoramentos no texto da lei[38].

Durante os debates, foram consideradas as experiências de outros países que já haviam implementado legislações semelhantes, como o Regulamento Geral de Proteção de Dados União Europeia[39]. A análise comparativa contribuiu para moldar a LGPD de maneira a atender às necessidades específicas do Brasil, levando em consideração suas características culturais, sociais e econômicas[40].

A aprovação da LGPD não marcou o fim do processo, mas sim o início de uma nova fase: a implementação efetiva da legislação. Órgãos reguladores foram criados, como a já citada Agência Nacional de Proteção de Dados, e as empresas tiveram prazos para se adequar às novas regras[41]. O processo de implementação envolveu não apenas a adaptação de políticas internas, mas também a conscientização dos cidadãos sobre seus direitos e das empresas sobre suas responsabilidades.

Apesar dos avanços proporcionados pela LGPD, alguns desafios persistem. A implementação efetiva da legislação demanda conscientização e capacitação contínuas de organizações e cidadãos. A garantia de conformidade com os princípios da lei requer monitoramento constante e uma abordagem proativa para lidar com as evoluções tecnológicas e os desafios emergentes relacionados à segurança de dados.

CONSIDERAÇÕES FINAIS: O BRASIL E SUAS OSCILAÇÕES INTERNAS E EXTERNAS NO COMBATE AO CIBERCRIME

As respostas aos incidentes cibernéticos aqui analisadas demonstram, de certa forma, uma oscilação do Brasil entre um constante binômio presente quando se pensa na governança e securitização do ciberespaço: liberdade x controle. Quando o tema em questão foi fácil e diretamente associado a crime passível de ser sofrido por um «cidadão comum» (no caso, o vazamento de fotos íntimas), houve um rápido apelo por um maior controle do ciberespaço pelo Estado.

Por outro lado, a proteção de dados pessoais é, de certa forma, tema mais amplo e nebuloso e, por conseguinte, menos impactante e preocupante para a população em geral. A LGPD estipula, por exemplo, como empresas devem gerir os dados pessoais de consumidores, se estes são ou não sigilosos, se podem ou não ser comercializados, como devem ser tratados, etc. Seu escopo, se por um lado abrangente, por outro traz questionamentos relativos a excessos de controle por parte do Estado e a possíveis ameaças às liberdades individuais e coletivas.

Ademais, a LGPD por refletir e ser impactada por caso de espionagem internacional, do qual o Brasil não foi a única vítima, não pode ser analisada fora do debate global sobre a governança do ciberespaço. Ou seja, há uma perspectiva internacional mais ampla na qual a política e a resposta legislativa do Brasil ao cibercrime devem ser situadas. O ciberespaço é, afinal, global, e as ameaças relacionadas à cibersegurança, portanto, afetam todos os Estados. Entretanto, as capacidades dos Estados para lidar com essas ameaças variam consideravelmente. Da mesma forma, existem inúmeras possíveis respostas de política doméstica e externa às ameaças cibernéticas. O Brasil é frequentemente considerado um «Estado-pêndulo» na diplomacia cibernética global[42]. Essa descrição define a diplomacia brasileira em relação a dois campos: uma posição ocidental, com opiniões semelhantes, a favor de uma internet livre e aberta e de uma governança multissetorial; e uma outra constelação, associada de forma proeminente à China e à Rússia, que favorece um modelo mais intergovernamental de governança global da internet, bem como uma maior assertividade da soberania estatal sobre a política cibernética.

Dessa maneira, as respostas dos Estados às ameaças cibernéticas podem apresentar diferenças normativas claras, não obstante o consenso normativo aparente sobre o comportamento estatal responsável no ciberespaço, que surge sob os auspícios da diplomacia cibernética da Organização das Nações Unidas (ONU) nos últimos quinze anos. A diplomacia cibernética do Brasil, bem como a resposta legislativa a ciberincidentes, em diferentes momentos, reflete oscilações no posicionamento brasileiro, inserindo-o ora mais em um campo, ora no outro. O Brasil é, em geral, fortemente favorável à abordagem multissetorial para a governança da internet, um dos pilares da iniciativa NETmundial (2014-2016). Mas também é um apoiador consistente da necessidade de reequilibrar a ordem internacional e representar melhor o Sul Global, o que pode ser visto como uma razão para apoiar um maior papel da ONU na governança global da internet.

O ponto-chave nesta análise, no entanto, é que o Brasil faz suas próprias escolhas na política cibernética. Não se pode definir a política cibernética brasileira em referência às políticas dos grupos ocidentais ou da China/Rússia na diplomacia cibernética global. Isso é claramente o caso no engajamento de longo prazo do Brasil com as dimensões internacionais do combate ao cibercrime. O Brasil foi, por exemplo, por muito tempo cético em relação aos méritos de aderir à Convenção de Budapeste, acabando por ade-

rir a ela por razões pragmáticas. Da mesma forma, o Brasil apoia o comitê *ad hoc* da ONU negociando um novo tratado global de cibercrime. A estratégia cibernética do Brasil nos assuntos internacionais é tanto normativa – promovendo o multissetorialismo e processos intergovernamentais mais globalmente representativos – quanto pragmática, visando acordos que aumentem a capacidade do país de alcançar seu objetivo estratégico nacional de combater o cibercrime.

Como outros Estados, para proteger seus cidadãos, empresas e instituições no ciberespaço, o Brasil precisa de uma combinação de capacidade doméstica aprimorada e parcerias internacionais eficazes. A agenda legislativa e a política doméstica do Brasil, incluindo reformas recentes do ecossistema de governança da cibersegurança por meio da nova Política Nacional de Cibersegurança, é um exemplo de iniciativas destinadas a aumentar a capacidade doméstica. Essa é uma agenda de longo prazo, na qual o governo nacional não é o único ator: empresas e sociedade civil são partes interessadas. Mas há também uma dimensão internacional significativa no combate ao cibercrime. Esta dimensão requer uma diplomacia assídua e paciente, não apenas do Ministério das Relações Exteriores, mas também da diplomacia funcional horizontal envolvendo cooperação judicial e policial, tanto regional quanto globalmente, por meio de organizações como a Interpol. Há uma clara oportunidade para o Brasil seguir tanto as dimensões domésticas quanto as internacionais de sua estratégia nacional de maneira integrada. Isso também se alinharia de perto com uma agenda para o Brasil exercer liderança regional, por exemplo, através da Organização dos Estados Americanos ou de outros órgãos regionais, para promover uma cooperação mais eficaz em segurança cibernética e combate ao cibercrime. O futuro de uma estratégia eficaz para combater o cibercrime deve residir na integração das agendas domésticas e internacionais. RI

Data de receção: 5 de janeiro de 2024 | Data de aprovação: 5 de abril de 2024

Mariana Grilli Belinotte Bolsista da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior (CAPES). Doutoranda do Programa de Pós-Graduação em Ciências Militares da Escola de Comando e Estado-Maior do Exército. Mestre em Direito (Universidade Federal de Minas Gerais).

> Instituto Meira Mattos (PPGCM-IMM), Praça General Tibúrcio, 125, Sala: 313, Urca, Praia Vermelha, Rio de Janeiro 22290-270, Brasil | marianabelinotte@gmail.com

Luiz Rogério Franco Goldoni Professor do Programa de Pós-Graduação em Ciências Militares da Escola de Comando e Estado-Maior do Exército e coordenador do Laboratório de Poder Cibernético (LPCiber). Doutor em Ciência Política (Universidade Federal Fluminense).

> Escola de Comando e Estado-Maior do Exército (ECEME), Praça General Tibúrcio, 125, Praia Vermelha, Rio de Janeiro 22290-270, Brasil | luizrfgoldoni@gmail.com

Joe Devanny Professor do Departamento de War Studies do King's College London. Doutor em Teoria Política pela Universidade de Cambridge.

> King's College London, Strand Campus, Strand, Londres, WC2R 2LS, Reino Unido | Joseph.devanny@kcl.ac.uk

Carlos Frederico Coelho Professor do Programa de Pós-Graduação em Ciências Militares da Escola de Comando e Estado-Maior do Exército. Doutor em Ciência Política pela Universidade do Estado do Rio de Janeiro.

> Escola de Comando e Estado-Maior do Exército (ECEME), Praça General Tibúrcio, 125, Praia Vermelha, Rio de Janeiro 22290-270, Brasil | cafrecoelho@gmail.com

NOTAS

1 Só será abordada a criminalização «substantiva», aquela que envolve a criação ou modificação de tipos penais, e não o conceito mais amplo, que envolveria, por exemplo, a análise do aparato repressivo do Estado e a administração da justiça.

2 LANCY, Nicola – «Historicising criminalisation». In *The Modern Law Review*. Londres. Vol. 72, N.º 6, 2009, pp. 936-960. DOI: 10.1111/j.1468-2230.2009.00775.x.

3 BERGER, Peter; LUCKMANN, Thomas – *The Social Construction of Reality*. 1.ª edição. Nova Iorque: Open Road, 1966.

4 GUTWIRTH, Serge; DE HERT, Paul; DE SUTTER, Laurent – «The trouble with technology regulation from a legal perspective». In *Regulating Technologies*. Oxford: Hart Publishers, 2008, pp. 193-218.

5 MEDEIROS, Breno; GOLDONI, Luiz – «The fundamental conceptual trinity of cyberspace». In *Contexto Internacional*. Rio de Janeiro. Vol. 42, N.º 1, 2020, pp. 31-54.

6 DEVANNY, Joe; GOLDONI, Luiz; MEDEIROS, Breno – «Strategy in an uncertain domain: threat and response in cyberspace». In *Journal of Strategic Security*. Rapid City. Vol. 12, N.º 2, 2022, pp. 34-47.

7 VIRILIO, Paul – *El Cibermundo, la política de lo peor*. Madrid: Cultura Libre, 1997.

8 DAVID, René – *Major Legal Systems in the World Today*. Milwaukee: Stevens, 1985.

9 JOHNSON, David; POST, David – «Law and borders». In *Stanford Law Review*. Stanford. Vol. 48, N.º 5, 1996, pp. 1367--1402; RONFELDT, David – «Cyberocracy is coming». In *The Information Society*. Nova Iorque. Vol. 8, N.º 4, 1992, pp. 243-296; SMITH, Stephen – «Communication and the Constitution in cyberspace». In *Communication Education*. Londres. Vol. 43, N.º 2, 1994, pp. 87-101.

10 O cibercrime, de acordo com a minuta da Política Nacional de Cibersegurança, em seu artigo 4, inciso III, é crime praticado contra, ou por meio de, ciberativos («MINUTA DA PNCiber». Gabinete de Segurança Institucional da Presidência da República. Consultado em: janeiro de 2024. Disponível em: https://www.gov.br/gsi/pt-br/ssic/audiencia-publica/PNCiberAudienciaPublicaProjetoBase.pdf).

11 GORDON, Sarah; FORD, Richard – «On the definition and classification of cybercrime». In *Journal of Computer Virology*. Berlim. Vol. 13, 2006, pp. 13-20.

12 *Crimeware* são programas desenvolvidos para fazer com que os sistemas de terceiros funcionem de maneira diversa da que seu legítimo usuário espera, como *keyloggers*, *trojans*, *worms*, *bots*, entre outros (GORDON, Sarah; FORD, Richard – «On the definition and classification of cybercrime»).

13 *Ibidem*.

14 INTERNATIONAL TELECOMMUNICATION UNION – *Global Cybersecurity Index 2020*. Consultado em: fevereiro de 2024. Disponível em: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2021-PDF-E.pdf.

15 «ASSINATURAS E ratificações da Convenção de Cibercrimes». Conselho da Europa. Consultado em: fevereiro de 2024. Disponível em: https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=185.

16 «ATRIZ CAROLINA Dieckmann é chantageada». In *O Estado de S. Paulo*. São Paulo, 6 de maio de 2012, p. C7.

17 VALLE, Sabrina – «Carolina Dieckmann teve as fotos roubadas por hackers». In *O Estado de S. Paulo*. São Paulo, 14 de maio de 2012, p. C7.

18 TRAMITAÇÃO DA Lei 12.737/2012. Câmara dos Deputados. Consultado em: janeiro de 2024. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=529011.

19 MADUEÑO, Denise – «Caso Carolina faz Câmara aprovar lei do crime cibernético». In *O Estado de S. Paulo*. São Paulo. 16 de maio de 2012, p. C7.

20 TRAMITAÇÃO DA Lei 12.737/2012.

21 TRAMITAÇÃO DE Projetos de Lei – crimes cibernéticos. Câmara dos Deputados. Consultado em: fevereiro de 2024. Disponível em: https://www.camara.leg.br/buscaProposicoesWeb/?wicket:interface=:1:2.

22 DEVANNY, Joe; MARTIN, Ciaran; STEVENS, Tim – «On the strategic consequences of digital espionage». In *Journal of Cyber Policy*. Londres. Vol. 3, N.º 6, 2021, pp. 429-450.

23 WATTS, Jonathan – «Brazil demands explanation from US over NSA spying». In *The Guardian*. Consultado em: janeiro de 2024. Disponível em: https://www.theguardian.com/world/2013/jul/08/brazil-demands-explanation-nsa-spying.

24 EDDY, Melissa – «File is said to confirm NSA spied on Merkel». Nytimes.com. Consultado em: janeiro de 2024. Disponível em: https://www.nytimes.com/2015/07/02/world/europe/file-is-said-to-confirm-nsa-spied-on-merkel.html.

25 REGAN, James; JOHN, Mark – «NSA spied on French presidents». In *WikiLeaks*. 2015. Consultado em: janeiro de 2024. Disponível em: https://www.reuters.com/article/idUSKBN0P32EA/.

26 MANZANO, Gabriel – «Documentos indicam que Petrobrás é espionada por agência americana». In *Estadão*. Consultado em: janeiro de 2024. Disponível em: https://politica.estadao.com.br/noticias/geral,documentos-indicam-que-petrobras-e-espionada-por-agencia-americana,1072697.

27 «DILMA DECIDE cancelar visita de Estado aos EUA, diz jornal». In *G1*. Consultado em: janeiro de 2024. Disponível em: https://g1.globo.com/politica/noticia/2013/09/dilma-decide-cancelar-visita-de-estado-aos-eua-diz-jornal-1.html.

28 BORGER, Julian – «Brazilian president: US surveillance a "breach of international law"». In *The Guardian*. Consultado em: janeiro de 2024. Disponível em: https://www.theguardian.com/world/2013/sep/24/brazil-president-un-speech-nsa-surveillance.

29 «JORNAIS INTERNACIONAIS destacam ataque "feroz" de Dilma à espionagem dos EUA». BBC News Brasil. Consultado em: janeiro de 2024. Disponível em: https://www.bbc.com/portuguese/noticias/2013/09/130925_dilma_discurso_press_rw.

30 DEVANNY, Joe; GOLDONI, Luiz; MEDEIROS, Breno – «The rise of cyber power in Brazil». In *Revista Brasileira de Política Internacional*. Brasília. Vol. 65, N.º 1, 2022, pp. 1-21.

31 TRAMITAÇÃO DA Lei 13709/2018. Câmara dos Deputados. Consultado em: janeiro de 2024. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=548066.

32 BAUMAN, Zygmunt, et al. – «After Snowden». In *International Political* Sociology. Oxford. Vol. 8, N.º 2, 2014, pp. 121-144; LYON, David – «Surveillance, Snowden, and big data». In *Big Data & Society*. Thousand Oaks. Vol. 1, N.º 2, 2014.

33 BIONI, Bruno Ricardo; RIELLI, Mariana Marques – «A construção multissetorial da LGPD: história e aprendizado». In *Proteção de Dados: Contexto, Narrativas e Elementos Fundantes*. São Paulo: B. R. Bioni Sociedade Individual de Advocacia, 2021.

34 LEI GERAL de Proteção de Dados. Presidência da República. Brasil. Consultado em: janeiro de 2024. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm.

35 EBERT, Hannes; MAURER, Tim – «Contested cyberspace and rising powers». In *Third World Quarterly*. Oxford. Vol. 34, N.º 6, 2013, pp. 1054-1074; SEGAL, Adam – *The Hacked World Order*. Londres: Hachette, 2016.

36 LEI GERAL de Proteção de Dados.

37 TRAMITAÇÃO DA Lei 13709/2018.

38 BIONI, Bruno Ricardo; RIELLI, Mariana Marques – «A construção multissetorial da LGPD...».

39 LIMBERGER, Têmis – «Lei Geral de Proteção de Dados (LGPD) e a Lei de Acesso à Informação Pública (LAI)». In *Revista de Direito Administrativo*. São Paulo. Vol. 281, N.º 1, 2022, pp. 113-144.

40 IRAMINA, Aline – «RGPD v. LGPD: adoção estratégica da abordagem responsivo na elaboração da Lei Geral de Proteção de Dados no Brasil e do Regulamento Geral de Proteção de Dados da União Europeia». In *Revista de Direito, Estado e Telecomunicações*. Brasília. Vol. 12, N.º 2, 2020, pp. 91-117.

41 LEI GERAL de Proteção de Dados.

42 EBERT, Hannes; MAURER, Tim – «Contested cyberspace and rising powers». In *Third World Quarterly*. Oxford. Vol. 34, N.º 6, 2013, pp. 1054-1074.

BIBLIOGRAFIA

«ASSINATURAS E ratificações da Convenção de Cibercrimes». Conselho da Europa. Consultado em: fevereiro de 2024. Disponível em: https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=185.

«ATRIZ CAROLINA Dieckmann é chantageada». In *O Estado de S. Paulo*. São Paulo, 6 de maio de 2012, p. C7.

BAUMAN, Zygmunt; BIGO, Didier; ESTEVES, Paulo; GUILD, Elspeth; JABRI, Vivienne; LYON, David; WALKER, R. B. J. – «After Snowden». In *International Political* Sociology. Oxford. Vol. 8, N.º 2, 2014, pp. 121-144. DOI: 10.1111/ips.12048.

BERGER, Peter; LUCKMANN, Thomas – *The Social Construction of Reality*. 1.ª edição. Nova Iorque: Open Road, 1966.

BIONI, Bruno Ricardo; RIELLI, Mariana Marques – «A construção multissetorial da LGPD: história e aprendizado». In *Proteção de Dados: Contexto, Narrativas e Elementos Fundantes*. São Paulo: B. R. Bioni Sociedade Individual de Advocacia, 2021.

BORGER, Julian – «Brazilian president: US surveillance a "breach of international law"». In *The Guardian*. Consultado em: janeiro de 2024. Disponível em: https://www.theguardian.com/world/2013/sep/24/brazil-president-un-speech-nsa-surveillance.

DAVID, René – *Major Legal Systems in the World Today*. Milwaukee: Stevens, 1985.
DEVANNY, Joe; GOLDONI, Luiz; MEDEIROS, Breno – «Strategy in an uncertain domain: threat and response in cyberspace». In *Journal of Strategic Security*. Rapid City. Vol. 12, N.º 2, 2022, pp. 34-47. DOI: 10.5038/1944-0472.15.2.1954.

DEVANNY, Joe; GOLDONI, Luiz; MEDEIROS, Breno – «The rise of cyber power in Brazil». In *Revista Brasileira de Política Internacional*. Brasília. Vol. 65, N.º 1, 2022, pp. 1-21. DOI: 10.1590/0034-7329202200113.

DEVANNY, Joe; MARTIN, Ciaran; STEVENS, Tim – «On the strategic consequences of digital espionage». In *Journal of Cyber Policy*. Londres. Vol. 3, N.º 6, 2021, pp. 429-450. DOI: 10.1080/23738871.2021.2000628.

«DILMA DECIDE cancelar visita de Estado aos EUA, diz jornal». In *G1*. Consultado em: janeiro de 2024. Disponível em: https://g1.globo.com/politica/noticia/2013/09/dilma-decide-cancelar-visita-de-estado-aos-eua-diz-jornal-1.html.

EBERT, Hannes; MAURER, Tim – «Contested cyberspace and rising powers». In *Third World Quarterly*. Oxford. Vol. 34, N.º 6, 2013, pp. 1054-1074. DOI: 10.1080/01436597.2013.802502.

EDDY, Melissa – «File is said to confirm NSA spied on Merkel». Nytimes.com. Consultado em: janeiro de 2024. Disponível em: https://www.nytimes.com/2015/07/02/world/europe/file-is-said-to-confirm-nsa-spied-on-merkel.html.

GORDON, Sarah; FORD, Richard – «On the definition and classification of cybercrime». In *Journal of Computer Virology*. Berlim. Vol. 13, 2006, pp. 13-20. DOI: 10.1007/s11416-006-0015-z.

GUTWIRTH, Serge; DE HERT, Paul; DE SUTTER, Laurent – «The trouble with technology regulation from a legal perspective». In *Regulating Technologies*. Oxford: Hart Publishers, 2008, pp. 193-218.

IRAMINA, Aline – «RGPD v. LGPD: adoção estratégica da abordagem responsivo na elaboração da Lei Geral de Proteção de Dados no Brasil e do Regulamento Geral de Proteção de Dados da União Europeia». In *Revista de Direito, Estado e Telecomunicações*. Brasília. Vol. 12, N.º 2, 2020, pp. 91-117. DOI: 10.26512/lstr.v12i2.34692.

INTERNATIONAL TELECOMMUNICATION UNION – *Global Cybersecurity Index 2020*. Consultado em: fevereiro de 2024. Disponível em: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2021-PDF-E.pdf.

JOHNSON, David; POST, David – «Law and borders». In *Stanford Law Review*. Stanford. Vol. 48, N.º 5, 1996, pp. 1367-1402. DOI: 10.2307/1229390.

«JORNAIS INTERNACIONAIS destacam ataque "feroz" de Dilma à espionagem dos EUA». BBC News Brasil. Consultado em: janeiro de 2024. Disponível em: https://www.bbc.com/portuguese/noticias/2013/09/130925_dilma_discurso_press_rw.

LANCY, Nicola – «Historicising criminalisation». In *The Modern Law Review*. Lon-

dres. Vol. 72, N.º 6, 2009, pp. 936-960. DOI: 10.1111/j.1468-2230.2009.00775.x.

LEI GERAL de Proteção de Dados. Presidência da República. Brasil. Consultado em: janeiro de 2024]. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm.

LIMBERGER, Têmis – «Lei Geral de Proteção de Dados (LGPD) e a Lei de Acesso à Informação Pública (LAI)». In *Revista de Direito Administrativo*. São Paulo. Vol. 281, N.º 1, 2022, pp. 113-144. DOI: 10.12660/rda.v281.2022.85654.

LYON, David – «Surveillance, Snowden, and big data». In *Big Data & Society*. Thousand Oaks. Vol. 1, N.º 2, 2014. DOI: 10.1177/2053951714541861.

MADUEÑO, Denise – «Caso Carolina faz Câmara aprovar lei do crime cibernético». In *O Estado de S. Paulo*. São Paulo. 16 de maio de 2012, p. C7.

MANZANO, Gabriel – «Documentos indicam que Petrobrás é espionada por agência americana». In *Estadão*. Consultado em: janeiro de 2024. Disponível em: https://politica.estadao.com.br/noticias/geral,documentos-indicam-que-petrobras-e-espionada-por-agencia-americana,1072697.

MEDEIROS, Breno; GOLDONI, Luiz – «The fundamental conceptual trinity of cyberspace». In *Contexto Internacional*. Rio de Janeiro. Vol. 42, N.º 1, 2020, pp. 31-54. DOI: 10.1590/S0102-8529.2019420100002.

«MINUTA DA PNCiber». Gabinete de Segurança Institucional da Presidência da República. Consultado em: janeiro de 2024. Disponível em: https://www.gov.br/gsi/pt-br/ssic/audiencia-publica/PNCiberAudienciaPublicaProjetoBase.pdf.

REGAN, James; JOHN, Mark – «NSA spied on French presidents». In *WikiLeaks*. 2015. Consultado em: janeiro de 2024. Disponível em: https://www.reuters.com/article/idUSKBN0P32EA/.

RONFELDT, David – «Cyberocracy is coming». In *The Information Society*. Nova Iorque. Vol. 8, N.º 4, 1992, pp. 243-296. DOI: 10.1080/01972243.1992.9960123.

SEGAL, Adam – *The Hacked World Order*. Londres: Hachette, 2016.

SMITH, Stephen – «Communication and the Constitution in cyberspace». In *Communication Education*. Londres. Vol. 43, N.º 2, 1994, pp. 87-101.

TRAMITAÇÃO DA Lei 12.737/2012. Câmara dos Deputados. Consultado em: janeiro de 2024. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=529011.

TRAMITAÇÃO DA Lei 13709/2018. Câmara dos Deputados. Consultado em: janeiro de 2024. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=548066.

TRAMITAÇÃO DE Projetos de Lei – crimes cibernéticos. Câmara dos Deputados. Consultado em: fevereiro de 2024. Disponível em: https://www.camara.leg.br/buscaProposicoesWeb/?wicket:interface=:1:2.

VALLE, Sabrina – «Carolina Dieckmann teve as fotos roubadas por hackers». In *O Estado de S. Paulo*. São Paulo, 14 de maio de 2012, p. C7.

VIRILIO, Paul – *El Cibermundo, la política de lo peor*. Madrid: Cultura Libre, 1997.

WATTS, Jonathan – «Brazil demands explanation from US over NSA spying». In *The Guardian*. Consultado em: janeiro de 2024. Disponível em: https://www.theguardian.com/world/2013/jul/08/brazil-demands-explanation-nsa-spying.