



UFRJ

UNIVERSIDADE FEDERAL DO RIO DE JANEIRO
CENTRO DE CIÊNCIAS JURÍDICAS E ECONÔMICAS
FACULDADE DE DIREITO

**GOVERNANÇA DA INTERNET: UMA VISÃO SOBRE A ATUAÇÃO DO BRASIL
NA GESTÃO DA INTERNET**

JESSIKA CARDOSO DE MEDEIROS

RIO DE JANEIRO

2023

JESSIKA CARDOSO DE MEDEIROS

**GOVERNANÇA DA INTERNET: UMA VISÃO SOBRE A ATUAÇÃO DO BRASIL
NA GESTÃO DA INTERNET**

Monografia de final de curso elaborada no âmbito da graduação em Direito da Universidade Federal do Rio de Janeiro como requisito para obtenção do grau de bacharel em Direito, sob a orientação da Professora Dra. Carolina Pizoeiro.

RIO DE JANEIRO

2023

FICHA CATALOGRÁFICA

CIP - Catalogação na Publicação

M488g Medeiros, Jessika Cardoso de
Governança da Internet: Uma visão sobre a atuação do Brasil na gestão da Internet / Jessika Cardoso de Medeiros. -- Rio de Janeiro, 2023.
49 f.

Orientadora: Carolina Azevedo Pizoeiro Gerolimich.
Trabalho de conclusão de curso (graduação) - Universidade Federal do Rio de Janeiro, Faculdade Nacional de Direito, Bacharel em Direito, 2023.

1. Governança da Internet. 2. internet. 3. Brasil. 4. Marco Civil da Internet. 5. privacidade.
I. Gerolimich, Carolina Azevedo Pizoeiro, orient.
II. Título.

Elaborado pelo Sistema de Geração Automática da UFRJ com os dados fornecidos pelo(a) autor(a), sob a responsabilidade de Miguel Romeu Amorim Neto - CRB-7/6283.

JESSIKA CARDOSO DE MEDEIROS

**GOVERNANÇA DA INTERNET: UMA VISÃO SOBRE A ATUAÇÃO DO BRASIL
NA GESTÃO DA INTERNET**

Monografia de final de curso elaborada no âmbito da graduação em Direito da Universidade Federal do Rio de Janeiro como requisito para obtenção do grau de bacharel em Direito, sob a orientação da Professora Dra. Carolina Pizoeiro.

Data da Aprovação: __/__/____.

Banca Examinadora:

Orientador

Membro da Banca

Membro da Banca

Membro da Banca

À família e amigos por todo o suporte.

AGRADECIMENTOS

Em primeiro lugar, agradeço aos meus pais –Solange e Luiz Carlos- pelo apoio durante esses anos de graduações e pós-graduação. Entre idas e vindas para a UFF, UFRJ e estágios, sempre soube que teria em casa um local tranquilo e com afeto. Agradeço a minha namorada, Alinne, seu carinho, apoio, incentivo, me fizeram seguir firme em todas as etapas desse final de faculdade. A confiança em mim é algo que me encanta diariamente e me faz seguir.

À Carolina Pizoeiro que tornou possível a execução deste trabalho de pesquisa, agradeço o apoio nesse tempo e pelas conversas. Aos professores que cruzei ao longo da minha trajetória acadêmica, agradeço a dedicação. Aos amigos que cruzei na FND, vocês tiveram um lugar especial nessa longa jornada de crescimento pessoal e profissional. Em especial, tenho muito o que agradecer a Júlia e a Camila, sem dúvidas, sem elas eu não teria passado por todos esses anos de graduação. Tenham certeza de que cheguei até o final, pois tive vocês como suporte.

Não posso deixar de agradecer imensamente à Marina, Charles e Larissa, por todo esse tempo de incentivo nas graduações, na pós e em todo o caminho! Todo o suporte moral e amizade foram essenciais durante esses anos. Ao Felipe Simoni, amigo que há anos temos discussões enriquecedoras sobre as nossas pesquisas e que sempre me auxilia quando preciso elaborar alguma temática. Por fim, agradeço pelas amizades que fiz no estágio, tanto no CEPRI quanto na Beaumont. Marina Burck, Carol, Renata e Andressa, vocês foram muito importantes para o meu crescimento profissional.

RESUMO

Esta pesquisa busca elaborar um levantamento bibliográfico sobre a temática da governança da internet. Tomando está como norte, parte-se para o esforço de compreender o que é a governança da internet e como o Brasil está atuando para a implantação da mesma e regulamentação da internet. As fontes usadas foram artigos e livros sobre o tema, além de legislação nacional e internacional que tem como objetivo a regulamentação da atividade na internet. Para a análise a monografia foi dividida em três capítulos: o primeiro abordando o entendimento sobre a governança da internet; o segundo sobre a atuação do Brasil; o terceiro, e último capítulo, são levantados desafios acerca do tema.

Palavras-chave: Governança da internet; internet; Brasil; Marco Civil da Internet; privacidade.

ABSTRACT

This research seeks to elaborate a bibliographic survey about internet governance. We consider this theme as guide, the effort is made to understand what internet governance is and how Brazil is working towards its implementation and internet regulation. The sources used were articles and books on the subject, as well as national and international legislation that aims to regulate activity on the internet. For the analysis, this research work was divided into three chapters: the first addressing the understanding of internet governance; the second on Brazil's performance regarding internet governance; the third, and last chapter, challenges on the subject are raised.

Keywords: Internet Governance; internet; Brazil; Brazilian Civil Rights Framework for the Internet; privacy.

SUMÁRIO

INTRODUÇÃO	10
CAPÍTULO 1: A GOVERNANÇA DA INTERNET	12
1.1 A INTERNET	13
1.2 A GOVERNANÇA GLOBAL DA INTERNET	14
CAPÍTULO 2: A GOVERNANÇA DA INTERNET NO BRASIL	19
2.1 O COMITÊ GESTOR DA INTERNET NO BRASIL (CGI.br)	19
2.2 O PAPEL DO BRASIL INTERNACIONALMENTE	22
2.3 COMO O BRASIL ATUA INTERNAMENTE	24
2.3.1 MARCO CIVIL DA INTERNET – LEI Nº 12.965, DE 23 DE ABRIL DE 2014	24
2.3.2 LEI DOS CRIMES CIBERNÉTICOS – LEI Nº 12.737, DE 30 DE NOVEMBRO DE 2012	26
2.3.3 LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS (LGPD) – LEI Nº 13.709, DE 14 DE AGOSTO DE 2018	27
2.3.4 LEI Nº 14.132, DE 31 DE MARÇO DE 2021 E LEI Nº 14.155, DE 17 DE MAIO DE 2021	30
2.3.5 PROJETO DE LEI Nº 2630/2020 (LEI BRASILEIRA DE LIBERDADE, RESPONSABILIDADE E TRANSPARÊNCIA NA INTERNET)	31
CAPÍTULO 3: DESAFIOS DA GOVERNANÇA GLOBAL DA INTERNET	33
DEMOCRACIA	34
JURISDIÇÃO E CRIME	36
PRIVACIDADE	37
CONSIDERAÇÕES FINAIS	42
REFERÊNCIAS BIBLIOGRÁFICAS	44

INTRODUÇÃO

A origem da internet remonta da Segunda Guerra Mundial, onde o embrião do que conhecemos hoje foi criado no seio do complexo militar estadunidense. À época, a conexão entre computadores era primária e apenas conectava algumas máquinas localizadas em grandes universidades. Este foi o primeiro passo para o que anos depois viria a ser o mundo interconectado e transfronteiriço que temos hoje.

Assim, conforme a tecnologia avançou e a conectividade passou a ser global, nos encontramos imersos em uma Revolução Digital que se encontra em pleno fluxo. A sociedade está criando, vendo os frutos e consequências de maneira veloz, da mesma maneira, os impactos positivos e negativos também são sentidos tão rápido quanto. Desta forma, os Estados e demais entes interessados precisam criar mecanismos para que haja uma regulação, a governança da Internet. Esta deve caminhar junto ao Direito para que haja legislações e, conseqüentemente, sanções adequadas para a melhor ingerência e funcionamento deste exagerado número de conexões e indivíduos se relacionando concomitantemente.

A abordagem feita neste trabalho de monografia tem como objetivo abordar a governança da internet de maneira abrangente. O objeto de pesquisa é a própria governança da internet e seus desdobramentos globais, mas também colocando um destaque maior a atuação do Brasil neste contexto. Para atingir este objetivo, alguns pontos específicos foram divididos em capítulos para abranger a pesquisa.

O primeiro capítulo está dividido em duas partes, na primeira tratamos sobre a internet, entretanto, não cabe nesta pesquisa a descrição de como a mesma surgiu e todo o histórico detalhado. O que é abordado é no que tange ao seu significado além da tecnicidade que a envolve, entender como a internet é um território que está em constante expansão e que há uma infinidade de formas de explorá-la. A partir desse entendimento, na segunda parte trataremos sobre a governança global da internet, portanto, trazendo à luz o que se compreende sobre o tema, sua construção global com o passar dos anos e órgão/instituições que fazem parte desse contexto de tomada de decisão e formação de políticas.

No segundo capítulo se coloca o foco sobre o Brasil, desta forma, dividiremos a seção em três partes que completam o quadro de entendimento sobre a atuação nacional. O Comitê

Gestor da Internet no Brasil (CGI.br) é o ponto chave para o início da inserção do Brasil nesse contexto, ainda na década de 90. Em seguida veremos o papel do Brasil internacionalmente, no qual possui importante relevância devido a sua política ativa de regulamentação da internet. E, finalmente, a prática jurídica doméstica, com algumas leis que regulam o espaço cibernético e afins.

Por fim, no terceiro capítulo, temos como objeto os desafios que a governança global da internet enfrenta ao se colocar como realidade de atuação dos Estados. A democracia frente ao enxame de informação disponível ao alcance de um clique; as questões jurídicas de jurisdição e crime, uma vez que o caráter global da internet permite que um indivíduo em uma localidade possa praticar um delito em outra e; a privacidade, assunto que é sempre muito questionado quando tratamos de dados online disponíveis.

CAPÍTULO 1: A GOVERNANÇA DA INTERNET

A *internet*¹ está presente na nossa rotina de maneira quase que intrínseca, uma vez que muitas vezes nem ao menos notamos a sua presença. Além disso, a sociedade depende da *internet* para muitas operações burocráticas, judiciária, doméstica, educacionais e muitos outros exemplos do seu uso, seja profissional ou recreativo.

A *internet* é um dos elementos que estão presentes na revolução tecnológica em curso na sociedade contemporânea. Se no século XVIII o mundo viveu a primeira Revolução Industrial (máquina à vapor), no século XIX a segunda Revolução Industrial (eletricidade e produção em massa) e no século XX a terceira Revolução Industrial (eletrônicos e produção automatizada), agora estamos presenciando uma transição entre a terceira e quarta Revolução Industrial, também chamada de Revolução Digital. Essa última vem ocorrendo a passos largos e baseada na evolução/melhoramento de mecanismos e técnicas da anterior (SCHWAB, 2016).

Para Schwab (2016) “ela é caracterizada pela fusão de tecnologias que está borrando as linhas entre as esferas físicas, digitais e biológicas” (tradução nossa)². O autor destaca que a velocidade exponencial, fluidez e impactos que os sistemas causam na sociedade demonstra que estamos, de fato, em um novo momento e inteiramente imersos na Revolução Digital.

A inteligência artificial já está a nossa volta, desde carros com direção autônoma e drones com assistentes virtuais e softwares que traduzem ou investem. Progressos impressionantes em IA tem sido feito nos últimos anos, direcionados pelo exponencial crescimento do poder da capacidade computacional e pela disposição de vasta quantidade de dados, desde software usado para descobrir novas drogas até algoritmos usados para prever nossos interesses culturais. Tecnologias de fabricação digital, enquanto, estão interagindo com o mundo biológico diariamente. Engenheiros, designers e arquitetos estão combinando design computacional, aditivos de fabricação, engenharia de materiais e biologia sintética para explorar uma simbiose entre microrganismos, nossos corpos, os produtos que consumimos e, até os prédios que habitamos (tradução nossa) (SCHWAB, 2016).³

¹ Nesse trabalho optou-se por seguir a grafia de “internet/Internet” conforme Lucero (2011) e WSIS (2003 & 2005), no qual em minúsculo faz-se referência genérica e em maiúsculo é em referência a rede global, no qual o regime de governança é aplicado.

² *It is characterized by a fusion of technologies that is blurring the lines between the physical, digital, and biological spheres* (SCHWAB, 2016).

³ *Already, artificial intelligence is all around us, from self-driving cars and drones to virtual assistants and software that translate or invest. Impressive progress has been made in AI in recent years, driven by exponential*

Essa presença ostensiva no dia a dia quando atravessada por um olhar questionador pode levantar discussões acerca dos limites e impactos desse meio. Com base nessas possíveis discussões, serão abordados adiante no capítulo a questão da governança da *Internet*, perpassando pela privacidade e a governança corporativa para completar o quadro de análise deste capítulo.

1.1 A INTERNET

Outrossim, nesta pesquisa não convém abordar a história da *internet*, pois não faz parte do escopo escolhido para discussão⁴. Entretanto, não se pode ignorar que se deve entender qual o seu significado além dos conhecimentos técnicos que envolve a sua dinâmica, tal qual seus protocolos que permitem a conexão das redes à *Internet*, as programações em códigos e os cálculos de dados que fluem diariamente.

A *internet* permite que a sociedade interaja entre si e com outros, portanto esse movimento desperta o interesse de outras ciências, tais como a políticas, sociais e as relações internacionais. Esse meio cria um lugar onde inúmeras vozes falam, são ouvidas e entram, conseqüentemente em conflito, portanto como destaca Lucero (2011)

Do ponto de vista das ciências políticas e sociais e, em particular, da perspectiva das relações internacionais, faz sentido estudar a Internet como meio de interação e comunicação social. Cabe estudar a Internet como fenômeno que visa conectar pessoas, e não apenas máquinas, em redes de informação e comunicação. Defini-las pelo critério técnico do protocolo usado para conectar computadores seria insuficiente para justificar o apelo que sua governança global costuma suscitar em diversos grupos e setores da sociedade e dos governos (LUCERO, 2011, p. 35).

Tomando a definição acima, principalmente no trecho “...conectar pessoas, e não apenas máquinas, em redes de informação e comunicação.”, observa-se que há sujeitos que interagem entre si nesse lugar (ou não lugar, se lugar for entendido somente como algo físico). Para visão

increases in computing power and by the availability of vast amounts of data, from software used to discover new drugs to algorithms used to predict our cultural interests. Digital fabrication technologies, meanwhile, are interacting with the biological world on a daily basis. Engineers, designers, and architects are combining computational design, additive manufacturing, materials engineering, and synthetic biology to pioneer a symbiosis between microorganisms, our bodies, the products we consume, and even the buildings we inhabit (SCHWAB, 2016).

⁴ Para leitura sobre a história da Arpanet até o que conhecemos hoje como internert, ver Rocha (2017).

do que se pretende auferir ao mencionar *lugar*, faz-se necessário apresentar o conceito de território.

O território carrega no seu significado o entendimento que ultrapassa a dominação política concreta, no qual ele é visto como uma proteção do indivíduo que se encontra dentro dos seus limites, mas compreende o poder simbólico também. Essa visão simbólica do território gera no sujeito que interage uma identificação com o mesmo, apropriação de sentimentos e valores (HAESBAERT, 2004; MEDEIROS, 2009). Complementando, Haesbaert (2011), apresenta o território rede ou aglomerado que admite o que é chamado de sobreposição territorial, que consiste na partilha de múltiplos territórios em um mesmo espaço.

Portanto, a Internet com o seu constante e volumoso fluxo de pessoas, informações, dados e territórios sobrepostos apresenta aos Estados um desafio de controlar ou regulamentar esses movimentos. Assim, o próprio aparato Estatal, mais para frente da pesquisa veremos que não é somente este, tenta territorializar-se, ou seja, “construir e/ou controlar fluxos/redes e criar referenciais simbólicos num espaço em movimento, no e pelo movimento” (HAESBAERT, 2011, p.280).

Desta forma, pode-se entender a Internet como territórios dentro de um território mais abrangente, o qual nos referimos como espaço cibernético. Este *cyberspace* seria um meio de interação e comunicação através da *internet*, portanto os indivíduos trocando informações, transações econômicas, relações sociais e simbólicas. (LUCERO, 2011)

Portanto, a compreensão dos conceitos e relações abordadas acima auxilia no entendimento de que a governança da Internet é a busca por uma regulação de um lugar que (co)existe em territórios físicos dos Estados Nação. Entretanto, exatamente por ser fluido e não ter um aporte físico, vamos ver na próxima sessão que a governança da Internet enfrenta alguns desafios compartilhado pelos Estados para se consolidar.

1.2 A GOVERNANÇA GLOBAL DA INTERNET

Nesta seção vamos abordar diretamente o que se compreende como governança da Internet, qual o seu caminho ao longo do tempo, as suas formas, tomada de decisão e órgãos que fazem parte desta. Essa é uma temática que vai além da estrutura da *internet* em si, mas engloba os usuários, o ciberespaço e a sociedade que convive com a *internet* e tem que administrar seus desdobramentos (privacidade, segurança, acessibilidade etc.).

O sentido da governança nesse cenário é de gestão da Internet, mas não por um Estado nação unicamente, mas de maneira global, o que também abarcaria os mecanismos empregados pelos Estados para com o seu território. Essa gestão inclui também a tomada de decisão por atores⁵ governamentais ou não (LUCERO, 2011).

O processo de globalização⁶ foi catalisado com a *internet*, tomando como referência a presente pesquisa, portanto fez-se necessário para definição de normas sobre determinadas temáticas, no qual abrangeria o sistema internacional⁷, mas que não seria dominado pela hierarquia tradicional da estrutura de poder dos Estado, o surgimento de um campo onde “participariam atores interessados e capacitados, governamentais ou não, dar-se-ia o nome de governança” (LUCERO, 2011, p. 77).

Portanto, concatenando os conceitos abordados acima, seja *internet* e governança, vemos que no início do século XXI houve a tentativa das Nações Unidas em abordar o tema e trazer à luz o desafio global durante a construção de uma sociedade cada vez mais informatizada. O primeiro encontro⁸ do *World Summit on the Information Society - WSIS* (Cúpula Mundial sobre a Sociedade da Informação - CMSI) aconteceu em Genebra no ano de 2003 e definiu uma declaração de princípios chaves⁹ para a construção de uma Sociedade da

⁵ São atores cujas ações, interações definem as mudanças no cenário do Sistema Internacional. Podem ser de dois tipos: Atores Estatais ou não-Estatais (PECEQUILO, 2004).

⁶ Nessa pesquisa compreende-se globalização como “...a intensificação das relações sociais em escala mundial, que ligam localidades distantes de tal maneira que acontecimentos locais são modelados por eventos ocorrendo a muitas milhas de distância e vice-versa” (GIDDENS, 1991, p. 60).

⁷ O sistema internacional abrange, globalmente, todas as relações e fluxos entre os atores e seus intercâmbios, os fenômenos que ocorrem a partir desses intercâmbios ou mesmo independem deles, cobrindo todas as atividades além das fronteiras do cenário. Hoje, toda ação política no cenário internacional envolve forças do próprio sistema” (PECEQUILO, 2004, p. 39).

⁸ Os encontros continuam acontecendo anualmente, para mais informações ver: <https://www.itu.int/net4/wsis/forum/2023/en>

⁹ Os princípios são de acordo com a WSIS (2003 – Tradução nossa): 1- O papel dos governos e todas as partes interessadas para a promoção das Tecnologias da Informação e Comunicação para o desenvolvimento. (*The role of governments and stakeholders in the promotion of ICTs for development*); 2 – Infraestrutura de comunicação e informação: fundação essencial para uma sociedade da informação inclusiva (*Information and communication infrastructure: an essential foundation for an inclusive information society*); 3 – Acesso à informação e

Informação inclusiva. Esse encontro contou com a participação de 11.000 pessoas representando 175 países, de acordo com informações da ONU (UN, S.I).

O segundo encontro da Cúpula Mundial sobre a Sociedade da Informação aconteceu em 2005 em Túnis (Tunísia) e contou com a participação de mais de 19.000 pessoas representando 174 países (UN, S.I). Nesse encontro tivemos a Agenda de Túnis sobre a Sociedade da Informação, no qual há uma espécie de carta de intenções, mas sem caráter vinculante.

Nesse encontro de 2005, a CMSI apresentou uma definição de governança da Internet que consiste em como “o desenvolvimento e a aplicação pelos Governos, pelo setor privado e pela sociedade civil, em seus respectivos papéis, de princípios, normas, regras, procedimentos de tomadas de decisão e programas em comum que definem a evolução e o uso da Internet”¹⁰ (WSIS, 2005, p.6). Também houve a criação do Fórum de Governança da Internet (*Internet Governance Forum – IGF*)¹¹, no qual seria um local de articulação da sociedade civil (ROCHA, 2017).

Neste encontro, os princípios da reunião de 2003 foram reafirmados e, principalmente, que a governança da Internet não deve ser feita somente pelos Governos. A Agenda de Túnis deixa explícito que o setor privado, a sociedade civil e organizações internacionais e todas as partes interessadas devem se envolver junto aos Governos, cada um no papel que lhe cabe, para garantir “...uma distribuição de recursos equitativa, facilitar o acesso para todos e garantir um funcionamento estável e seguro da internet, levando em consideração o multilinguismo.”¹² (WSIS, 2005, p.6).

conhecimento (*Access to information and knowledge*); 4 – Construção de capacidade (*Capacity Building*); 5 – Construção de confiança e segurança no uso das Tecnologias da Informação e Comunicação (*Building confidence and security in the use of ICTs*); 6 – Ambiente capacitante (*Enabling environment*); 7 - Aplicações das Tecnologias da Informação e Comunicação: Benefícios em todos os aspectos da vida (*ICT applications: benefits in all aspects of life*); 8 – Diversidade cultural e identidade, diversidade linguística e conteúdo local (*Cultural diversity and identity, linguistic diversity and local content*); 9 – Mídia (*Media*); 10 – Dimensões éticas da Sociedade da Informação (*Ethical dimensions of the Information Society*) e; 11 – Cooperação internacional e regional (*International and regional cooperation*).

¹⁰ “A working definition of Internet governance is the development and application by governments, the private sector and civil society, in their respective roles, of shared principles, norms, rules, decision-making procedures, and programmes that shape the evolution and use of the Internet.” (WSIS, 2005, p.6).

¹¹ Os encontros continuam acontecendo, para mais informações ver:

<https://www.intgovforum.org/en>

¹² “...an equitable distribution of resources, facilitate access for all and ensure a stable and secure functioning of the Internet, taking into account multilingualism” (WSIS, 2005, p.6).

Esses papéis das instituições são, inclusive, abordados no documento. Assim, de acordo com o WSIS (2005), os Estados são responsáveis pelas políticas públicas¹³ relacionadas à *internet*; o setor privado é responsável pelo desenvolvimento técnico e econômico do campo; a sociedade civil desenvolve seu papel no nível da coletividade; as organizações intergovernamentais coordenam e são facilitadora das políticas públicas e; as organizações internacionais atuam no desenvolvimento de padrões técnicos e políticas importantes ao campo. Importante destacar que, embora, não caracterize com um dos principais, o documento não deixa de citar a contribuição acadêmica e técnica como relevante junto aos grupos citados em epígrafe.

Rocha (2017) tece uma importante observação ao destacar que o texto da Agenda de Túnis coloca o regime de governança internacional da Internet deva ser o multilateral, o que faria com que os Estados estivessem tentando trazer o poder decisório para si. Lucero (2011) também faz colocações onde implica que essa atuação em várias frentes e com partes que atuam em regime de igualdade, deixaria a tomada de decisões fragilizada. Isto porque, o autor critica que os atores internacionais (Estados e organizações intergovernamentais) se mostram incapazes de carregar a responsabilidade de coordenar políticas públicas que, também, sejam de interesse global acerca da governança da Internet.

Em outro ponto, Grossman (2014), já aborda que as discussões sobre a rede vão além dessa questão do multilateralismo, no qual cada país tem seu voto e, do multissetorialismo, no qual a participação dos outros interessados (sociedade civil e setor privado, p.ex.) tem peso igual à dos Estados. Um ponto que ele aponta é justamente o quanto interesses privados podem interferir na tomada de decisão sobre a regulação, portanto tendo essa dicotomia uma relevância limitada.

Na mesma toada, Rocha (2017) entende que a internet é, de fato, multissetorial e não intergovernamental, já que a rede é “controlada por um complexo amálgama de organizações que incluem representantes do poder público, setor privado, comunidade técnica, ativistas etc.” (ROCHA, 2017, p. 506). Essa configuração é consoante com o dinamismo que a própria rede

¹³ Nesse ponto o documento destaca que as políticas públicas devem incluir a segurança e proteção da internet, além de aspectos sociais, econômicos e técnicos. Por fim, aborda que o desenvolvimento de políticas públicas que aborem todos os temas já citados no texto, devem também contar com consulta a todas as partes interessadas (WSIS, 2005).

apresenta e permite que o debate seja mais livre da inércia em que se observa quando somente Estados Nações estão envolvidos.

Dando sequência ao que se compreende como governança da Internet¹⁴, deve-se considerar que há o olhar macro, mais voltado ao global e o olhar micro, no qual o regional tem mais peso. O primeiro é onde o fluxo de informações e transações acontecem utilizando a *internet* como meio, enquanto o segundo é a visão territorial, onde observamos os usuários da *internet* dentro do ciberespaço, provedores, as infraestruturas que mantêm relação com a *internet* (CANABARRO, 2018).

Portanto, entender a governança da Internet envolve a regulação da rede em si quanto dos elementos que coexistem em relação a ela. Os autores Wagner & Canabarro (2014) abordam que também deve-se atentar que a governança da Internet também é política e que envolve inúmeros atores, no qual cada um deles possui seus próprios interesses que se modificam ao longo do tempo.

Desta forma, ao abarcar essas visões, que já em si já envolve uma amalgama de temas, a governança da Internet enfrenta um desafio em coordenar políticas, inclusive, políticas públicas, na dinâmica coletiva. Canabarro (2018) nos apresenta alguns exemplos de temas que estão presente nesse desafio.

Entre muitos outros temas, são questões comuns dessa agenda ampliada: a privacidade e a proteção de dados pessoais no contexto da crescente coleta, armazenamento e processamento de informações como modelo de negócio na era digital; a tensão entre, de um lado, a possibilidade potencialmente infinita de livre acesso à informação e ao conhecimento e, de outro, os direitos de propriedade intelectual; o contencioso entre a liberdade de expressão e a remoção de conteúdos ofensivos aos direitos de atores sociais dos mais variados; as modalidades de regulação, fiscalização e tributação de serviços (tanto os tradicionais serviços de telecomunicações que servem de suporte à Internet, quanto aqueles serviços que são oferecidos através dela). (CANABARRO, 2018, p. 76)

Canabarro (2018) aponta uma crítica onde reconhece que a governança da Internet no que tange a área técnica é bem estruturada, no entanto, a coordenação de políticas públicas

¹⁴ Um mapa elaborado pela ICANN (*Internet Corporation for Assigned Names and Numbers*) que mostra a complexidade da governança da internet pode ser encontrado em: <https://www.icann.org/en/system/files/files/governance-06feb13-en.pdf>

institucionalizada em relação à *internet* ainda é dá passos lentos. Outrossim, cabe frisar que a evolução tecnológica galga espaço de maneira vertiginosa, desta maneira, uma governança da Internet eficiente deve(ria) acompanhar mais de perto.

Cada país também pode interpretar e definir governança da Internet a partir de seu ordenamento jurídico interno, com adoção de normas específicas para a temática, também por regulação de telecomunicações, uma vez que operadoras que proveem o acesso à *internet*, políticas públicas de acesso à *internet*, acessibilidade, pelo mercado e pelo contexto cultural da sociedade (CANABARRO, 2018).

Justamente a partir dessa visão que no próximo capítulo desta pesquisa, vamos abordar o papel do Brasil na governança global da Internet, inclusive o seu papel nas conferências e encontros internacionais. E as medidas internas que são tomadas para regulamentação, tais como o Marco Civil da Internet.

CAPÍTULO 2: A GOVERNANÇA DA INTERNET NO BRASIL

Vimos anteriormente a governança global da Internet, com suas definições e elementos. Neste capítulo, vamos ter como foco como o Brasil está inserido nessa dinâmica e, principalmente como o país atua internamente para regulamentar e estabelecer diretrizes para e da *internet*. Para tanto, são abordados nessa sessão o papel do Brasil nas conferências internacionais, o Comitê Gestor da Internet no Brasil (CGI.br) e, por fim, as normativas que tangem o território da *internet*.

2.1 O COMITÊ GESTOR DA INTERNET NO BRASIL (CGI.br)

O Brasil em meado da década de 90, mais precisamente em 1995, já colocava em prática um dos mais importantes organismos de governança da Internet no país. Dele que, por exemplo, deriva os princípios da normativa do Marco Civil da Internet. Em 1995 nascia o Comitê Gestor da Internet no Brasil (CGI.br) através de uma Portaria Interministerial nº 147 de maio de 1995

de iniciativa do Ministério das Comunicações e da Ciência e Tecnologia. No artigo primeiro do dispositivo são informadas as atribuições do CGI.br.

Art. 1º. Criar o Comitê Gestor Internet do Brasil, que terá como atribuições:

- I - acompanhar a disponibilização de serviços Internet no país;
- II - estabelecer recomendações relativas a: estratégia de implantação e interconexão de redes, análise e seleção de opções tecnológicas, e papéis funcionais de empresas, instituições de educação, pesquisa e desenvolvimento (IEPD);
- III - emitir parecer sobre a aplicabilidade de tarifa especial de telecomunicações nos circuitos por linha dedicada, solicitados por IEPDs qualificados;
- IV - recomendar padrões, procedimentos técnicos e operacionais e código de ética de uso, para todos os serviços Internet no Brasil;
- V - coordenar a atribuição de endereços IP (Internet Protocol) e o registro de nomes de domínios;
- VI - recomendar procedimentos operacionais de gerência de redes;
- VII - coletar, organizar e disseminar informações sobre o serviço Internet no Brasil; e
- VIII - deliberar sobre quaisquer questões a ele encaminhadas. (BRASIL, 1995).

Importante destacar que o CGI.br não é uma agência governamental, como o próprio nome diz, ele gere e coordena os setores que atuam com e na *internet* no Brasil. No início dos anos 2000 o CGI.br firma compromissos com a intenção de trabalhar em conjunto com a sociedade civil, com entidades que atuam na área e, inclusive, com provedores de acesso (iniciativa privada) em prol de uma internet segura¹⁵. Ainda nos anos 2000 é criado o Núcleo de Informação e Coordenação do Ponto BR (NIC.br), que é uma entidade civil sem fins lucrativos e braço executivo do CGI.br. O NIC.br¹⁶ possui importante papel, uma vez que detém as funções administrativas e operações do domínio “.br”, também com alocação de endereços de IP (*Internet Protocol*) e auxilia na execução de projetos e implementação de decisões do CGI.br.

O CGI.br teve a sua composição estabelecida pelo Decreto nº 4.829 de setembro de 2003, no qual fariam parte 9 representantes do setor governamental, 4 do empresarial, 4 do terceiro setor, 3 da comunidade científica e tecnológica e 1 representante de notório saber em assuntos de internet (BRASIL, 2003). Assim, nota-se que o CGI.br é um modelo de governança

¹⁵ Em 2000 foi lançada a Cartilha de Segurança para Internet, no qual consiste em um conjunto de documentos que reúne dicas e recomendações para que usuários da internet possam utilizar a mesma de maneira segura e se proteger de ameaças. A Cartilha já teve várias versões e a última atualização foi em 2021 com mudança na identidade visual e, atualmente, o documento consta com vários fascículos de temáticas diferentes. Os fascículos, história e demais informações podem ser encontradas em: <https://cartilha.cert.br/>

¹⁶ Para mais informações sobre as suas frentes de atuação, ver: <https://www.nic.br/atividades/>

que permite a participação de diversos setores, inclusive, governamental, mas ao mesmo tempo evita a burocracia inerente as engrenagens da máquina do Estado (LUCERO, 2011).

Lucero (2011), o autor sendo, inclusive, diplomata, destaca que o Ministério das Relações Exteriores (MRE) colabora com o CGI.br e apresenta alguns aspectos importantes. O primeiro é a legitimidade às posições brasileiras elaboradas dentro do Comitê, o que se deve, justamente, pela composição de diversos setores citados em epígrafe. Segundo é que esse modelo de gestão multissetorial vai ao encontro do que foi estabelecido pela Cúpula Mundial sobre a Sociedade da Informação. Terceiro, e último, o CGI.br atua junto às delegações brasileiras no exterior com fundamentação técnica, dados e estáticas sobre as pautas.

O ano de 2009 representa também um importante passo tanto para o CGI.br quanto para o ordenamento jurídico brasileiro, pois nesse ano foi aprovado o decálogo com os princípios para a governança e uso da Internet no Brasil, tais vão se tornar também base para o Marco Civil da Internet que será abordado mais à frente. O Decálogo aprovado pela Resolução CGI.br/RES/2009/003/P possui os seguintes princípios:

1. Liberdade, privacidade e direitos humanos

O uso da Internet deve guiar-se pelos princípios de liberdade de expressão, de privacidade do indivíduo e de respeito aos direitos humanos, reconhecendo-os como fundamentais para a preservação de uma sociedade justa e democrática.

2. Governança democrática e colaborativa

A governança da Internet deve ser exercida de forma transparente, multilateral e democrática, com a participação dos vários setores da sociedade, preservando e estimulando o seu caráter de criação coletiva.

3. Universalidade

O acesso à Internet deve ser universal para que ela seja um meio para o desenvolvimento social e humano, contribuindo para a construção de uma sociedade inclusiva e não discriminatória em benefício de todos.

4. Diversidade

A diversidade cultural deve ser respeitada e preservada e sua expressão deve ser estimulada, sem a imposição de crenças, costumes ou valores.

5. Inovação

A governança da Internet deve promover a contínua evolução e ampla difusão de novas tecnologias e modelos de uso e acesso.

6. Neutralidade da rede

Filtragem ou privilégios de tráfego devem respeitar apenas critérios técnicos e éticos, não sendo admissíveis motivos políticos, comerciais, religiosos, culturais, ou qualquer outra forma de discriminação ou favorecimento.

7. Inimputabilidade da rede

O combate a ilícitos na rede deve atingir os responsáveis finais e não os meios de acesso e transporte, sempre preservando os princípios maiores de defesa da liberdade, da privacidade e do respeito aos direitos humanos.

8. Funcionalidade, segurança e estabilidade

A estabilidade, a segurança e a funcionalidade globais da rede devem ser preservadas de forma ativa através de medidas técnicas compatíveis com os padrões internacionais e estímulo ao uso das boas práticas.

9. Padronização e interoperabilidade

A Internet deve basear-se em padrões abertos que permitam a interoperabilidade e a participação de todos em seu desenvolvimento.

10. Ambiente legal e regulatório

O ambiente legal e regulatório deve preservar a dinâmica da Internet como espaço de colaboração. (CGI.BR, 2009).

Como dito em epígrafe, 2009 foi um ano marcante porque também fora dado o primeiro passo para o Marco Civil da Internet, já que houve a primeira fase das consultas públicas do Marco Civil. A segunda fase ocorreu no ano seguinte e em 2011, o Marco Civil começa a tramitar na Câmara dos Deputados como projeto de lei (CGI.BRr, 2023b).

2.2 O PAPEL DO BRASIL INTERNACIONALMENTE

Em 2013 o mundo teve revelado por Edward Snowden¹⁷, ex-funcionário da *National Security Agency – NSA* (Agência de Segurança Nacional) que o órgão governamental estadunidense realizava espionagem e coleta de dados dos seus cidadãos e de diversos chefes de Estado, inclusive da ex-Presidenta Dilma. A agência monitorava as comunicações da embaixada, ligações telefônicas da chefe de Estado e da Petrobrás, o que foi chamado por Dilma Rousseff de violação do direito internacional (MACASKILL & DANCE, 2013).

¹⁷ Para a matéria completa sobre o escândalo de espionagem revelado por Snowden, ver: <https://www.theguardian.com/world/interactive/2013/nov/01/snowden-nsa-files-surveillance-revelations-decoded#section/1>

Como mostrado acima, o Marco Civil da Internet já tinha começado a ser discutido anos antes, entretanto o estouro desse caso de espionagem fez com que a relevância de um ordenamento interno específico fosse catalisada. No mesmo ano, na reunião da Assembleia Geral da ONU, a Presidenta Dilma enfatizou que alguns princípios deveriam ser garantidos mundialmente, tais como a governança democrática, respeito aos direitos humanos, liberdade de expressão, privacidade, neutralidade da rede, entre outros. Tais princípios defendidos vão ao encontro aos princípios para a governança e uso da Internet no Brasil aprovados pelo CGI.br em 2009 (KEMER, 2018).

Canabarro (2018) aponta que ao ter esse complexo esquema de espionagem descoberto, a credibilidade dos Estados Unidos como “guardião da rede aberta e livre foi posto em xeque” (p. 93), além de escancarar que o país possui um arcabouço tecnológico militar que permite essa exploração informacional sobre outros países. Tanto que ainda em 2013, Dilma Rousseff se reúne com o CGI.br para discussão do projeto de Lei do Marco Civil da Internet, este que nos primeiros meses de 2014 seria aprovado na Câmara dos Deputados e no Senado, respectivamente (GGI.BR, 2023b).

Comprometido com a promoção da governança da Internet e em parceria com a ICANN, o Brasil foi sede do NETMundial – Encontro Multissetorial Sobre o Futuro da Governança da Internet em 2014 ocorrido em São Paulo. Neste evento foi adotada uma declaração que, além dos princípios já citados anteriormente, o processo de governança da Internet deve ser transparente, inclusivo, colaborativo e passível de que ocorra uma “prestação de contas” para, entre outros, a proteção dos direitos humanos (NETMUNDIAL, 2014).

Durante a abertura da conferência, o Marco Civil da Internet aprovado por meio da Lei nº 12.965 de 23 de abril de 2014 foi sancionado pela presidenta (CGI.BR, 2023b). Rocha (2017) aponta exatamente essa relação entre política internacional e doméstica, uma vez que as denúncias de espionagem apontadas por Snowden foram o estopim para a aprovação mais célere do Marco Civil da Internet nas casas legislativas, pois como vimos as discussões foram iniciadas anos antes.

Esse ato representou o quanto o Brasil estava preocupado em estabelecer parâmetros que permitissem a regulamentação da Internet. Não podemos esquecer que a normatização da

Internet envolve inúmeros desafios, mas foi um passo importante para a política externa brasileira ter um papel de liderança.

2.3 COMO O BRASIL ATUA INTERNAMENTE

Nesta sessão é abordado como o Brasil atua no ordenamento jurídico interno para regulamentação da Internet e de suas consequências, entretanto, não se busca nessa pesquisa esgotar a temática. Tais leis escolhidas servem para ilustrar o comprometimento do Brasil para governança da Internet, para tanto, vemos o Marco Civil da Internet - Lei nº 12.965/2014, a Lei dos crimes cibernéticos – Lei 12.737/2012, a Lei Geral de Proteção de Dados Pessoais (LGPD) – Lei 13.709/2018, Leis 14.155 e 14.132 de 2021, nas quais alteram o Código Penal e Código de Processo Penal e o Projeto de Lei 2630/2020 (Lei Brasileira de Liberdade, Responsabilidade e Transparência na Internet).

2.3.1 MARCO CIVIL DA INTERNET – LEI Nº 12.965, DE 23 DE ABRIL DE 2014

Conforme já abordamos anteriormente, o Marco Civil da internet começou a dar os seus primeiros passos em 2009 quando houve a primeira fase das consultas públicas. Além disso, tivemos o Decálogo aprovado pelo CGI.br, onde os seus princípios serviram de inspiração para o que viria a ser positivado na normativa jurídica.

Com a situação já narrada ocasionada pelo escândalo de espionagem denunciado por Snowden, a Lei 12.965/2014 tramitou com prioridade e conseguiu ser apresentada no evento NETMundial – Encontro Multissetorial Sobre o Futuro da Governança da Internet, fazendo com que o seu sancionamento na abertura fosse uma referência. O Marco Civil teve a sua vigência iniciada em junho de 2014 (CGI.BR, 2023b).

O Ministério da Justiça define essa normativa como a Constituição da Internet e que ele veio na legislação brasileira para:

Conhecido como a “**Constituição da Internet**”, o Marco Civil preencheu uma lacuna na legislação brasileira definindo de forma clara direitos e responsabilidades relativas

à utilização dos meios digitais, ao invés de apenas criminalizar condutas nesses espaços. Por esse motivo, tornou-se referência para outros países do mundo não somente por seu conteúdo, mas também pelo amplo processo participativo que lhe deu origem (MJ, [2015a])

Esse processo participativo consistiu em uma plataforma online lançada pelo Ministério da Justiça para que a sociedade debatesse acerca de quatro eixos da lei: neutralidade de rede, guarda de registros, privacidade na rede e outros temas e considerações. Esse processo foi dividido em duas fases, onde na segunda o foco estava no debate para minutar o decreto a partir das abordagens da primeira fase, portanto a discussão posterior focou no texto. Foi a primeira vez que um decreto foi colocado para consulta pública e o Decreto nº 8.771/2016 foi publicado em maio de 2016, por volta, de um ano depois do início da primeira fase do debate (MJ, [2015b]).

Para Canabarro & Wagner (2014) o projeto de lei originário pode ser entendido como uma reação das partes interessadas da Internet que atuavam internamente, uma vez “não deve haver criminalização sem que haja um rol de direitos e garantias fundamentais na Internet reconhecidos explicitamente no ordenamento jurídico brasileiro” (p. 203). Desta forma, em consonância com os princípios do Decálogo, a lei estabelece princípios, garantias, direitos e deveres para o uso da Internet.

O Marco Civil da Internet em diversos dispositivos aborda a responsabilidade civil dos envolvidos. Entre os artigos temos o Artigo 3º, inciso VI; Artigo 10, §1º, Artigo 12, a Seção III e o Artigo 31. Inclusive, importante destacar que o Artigo 12 em seu parágrafo único (“*Parágrafo único. Tratando-se de empresa estrangeira, responde solidariamente pelo pagamento da multa de que trata o caput sua filial, sucursal, escritório ou estabelecimento situado no País.*” (BRASIL, 2014) não exclui de responsabilização a empresa estrangeira que atua em território nacional, pelo contrário, dá destaque a sua responsabilidade solidaria.

Por fim, a normativa explicita que houve um regime jurídico buscando a segurança, uma vez que a proteção da privacidade e a liberdade de expressão, caracterizados pelo livre acesso aos dados e a remoção de conteúdos devem passar pelo poder judiciário. Em diversos momentos do texto legal há a prerrogativa de “ordem/autorização/determinação judicial”, demonstrando que a justiça está preocupada com a regulação do que acontece online, mas deve equilibrar com a liberdade e neutralidade da rede (CANABARRO & WAGNER, 2014; ROCHA, 2017).

2.3.2 LEI DOS CRIMES CIBERNÉTICOS – LEI Nº 12.737, DE 30 DE NOVEMBRO DE 2012

Em 2011 a atriz Carolina Dieckmann teve seu computador invadido e fotos íntimas da atriz foram roubadas, além disso a atriz sofreu extorsão para que as imagens não fossem divulgadas. Como ela não pagou, as suas imagens íntimas foram amplamente divulgadas na internet e não lhe fora dado o devido amparo legal para a penalização aos perpetradores (ARAÚJO, 2023).

Assim, com o primeiro escândalo de crime virtual amplamente divulgado, o caso chegou ao judiciário brasileiro que se viu forçado a tipificar crimes cibernéticos. É válido destacar que o projeto de lei tramitou em regime de urgência e a lei foi sancionada em 2012, entrando em vigor em março de 2013 (FMP, 2021).

A Lei 12.737/2012 é apelidada de Lei Carolina Dieckmann justamente por ter se originado do caso da atriz. No dispositivo legal há alteração do Código Penal Brasileiro e, entre outros, incluiu-se dois artigos que tipificavam crimes virtuais e delitos informáticos (DPCE, 2022). Os artigos foram incluídos na seção IV do Código Penal que tratam dos crimes contra a inviolabilidade dos segredos.

Invasão de dispositivo informático

Art. 154-A. Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita: Pena - detenção, de 3 (três) meses a 1 (um) ano, e multa.

§ 1º Na mesma pena incorre quem produz, oferece, distribui, vende ou difunde dispositivo ou programa de computador com o intuito de permitir a prática da conduta definida no **caput**.

§ 2º Aumenta-se a pena de um sexto a um terço se da invasão resulta prejuízo econômico.

§ 3º Se da invasão resultar a obtenção de conteúdo de comunicações eletrônicas privadas, segredos comerciais ou industriais, informações sigilosas, assim definidas em lei, ou o controle remoto não autorizado do dispositivo invadido:

Pena - reclusão, de 6 (seis) meses a 2 (dois) anos, e multa, se a conduta não constitui crime mais grave.

§ 4º Na hipótese do § 3º, aumenta-se a pena de um a dois terços se houver divulgação, comercialização ou transmissão a terceiro, a qualquer título, dos dados ou informações obtidos.

§ 5º Aumenta-se a pena de um terço à metade se o crime for praticado contra:

I - Presidente da República, governadores e prefeitos;

II - Presidente do Supremo Tribunal Federal;

III - Presidente da Câmara dos Deputados, do Senado Federal, de Assembleia Legislativa de Estado, da Câmara Legislativa do Distrito Federal ou de Câmara Municipal; ou

IV - dirigente máximo da administração direta e indireta federal, estadual, municipal ou do Distrito Federal.”

“Ação penal

Art. 154-B. Nos crimes definidos no art. 154-A, somente se procede mediante representação, salvo se o crime é cometido contra a administração pública direta ou indireta de qualquer dos Poderes da União, Estados, Distrito Federal ou Municípios ou contra empresas concessionárias de serviços públicos.” (BRASIL, 2012).

A lei completou 10 anos em que foi sancionada e que está em vigor, entretanto ainda enfrenta críticas uma vez que deixa margem para interpretação sobre quais tipos de dispositivos podem ser alvo de invasão e, conseqüentemente, se enquadrar no tipo penal. Rocha (2022) também destaca que as leis devem acompanhar o ritmo das tecnologias e que os conteúdos devem ser mais bem debatidos do que o tempo recorde com qual foi discutido.

Apesar das críticas válidas e importantes para o debate e evolução do ordenamento jurídico, a Lei Carolina Dieckmann é um importante marco legal brasileiro. Esta lei foi a primeira a punir crimes cibernéticos e foi anterior ao Marco Civil da Internet, portanto, a “Constituição da Internet”, conforme chamado pelo Ministério da Justiça, ainda estava em discussão e formação do seu arcabouço legal.

2.3.3 LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS (LGPD) – LEI Nº 13.709, DE 14 DE AGOSTO DE 2018

Anteriormente a essa Lei, o tema de privacidade e proteção de dados eram abordados e forneciam proteção ao usuário por meio de leis espaciais, tais como o Código de Defesa do

Consumidos e o Marco Civil da Internet. O sancionamento em 2018 da Lei Geral de Proteção de Dados tem por objetivo o tratamento de dados pessoais, a proteção dos direitos fundamentais de liberdade de privacidade e o livre desenvolvimento da pessoa natural, conforme descrito em seu primeiro artigo. Portanto, fazendo com que o cuidado ao usuário e a privacidade fossem mais concentrados em uma única normativa (VERÍSSIMO JÚNIOR, 2023).

Em razão do *vacatio legis* de 18 meses, a LGPD entrou em vigor somente em 2020 e as multas (sanções) puderam começar a ser aplicadas em 2021. A LGPD teve como inspiração a *General Data Protection Regulation (GDPR)*¹⁸, lei europeia que também buscava a proteção de dados e privacidade. Veríssimo Junior (2023) aborda que ambas as legislações guardam suas semelhanças, mas que a lei nacional é mais minuciosa no que tange a transparência, com exigência que as empresas que tenham acesso as informações de maneira precisa e acessível sobre o processamento de dados. Outro ponto é que a LGPD “ênfatiza o princípio da prevenção, que exige medidas para prevenir a ocorrência de danos devido ao processamento de dados pessoais.” (NASCIMENTO, SBAITE E SOARES, 2020; VERÍSSIMO JÚNIOR, 2023).

A Lei se aplica a operações de tratamento de dados pessoais e pode ser realizada por pessoa natural, pessoa jurídica de direito público ou privado. Um ponto importante da Lei é que a sua aplicação não se restringe somente ao Brasil, mas deve seguir as orientações do Artigo 3º:

Art. 3º Esta Lei aplica-se a qualquer operação de tratamento realizada por pessoa natural ou por pessoa jurídica de direito público ou privado, independentemente do meio, do país de sua sede ou do país onde estejam localizados os dados, desde que:

I - a operação de tratamento seja realizada no território nacional;

II - a atividade de tratamento tenha por objetivo a oferta ou o fornecimento de bens ou serviços ou o tratamento de dados de indivíduos localizados no território nacional; ou

III - os dados pessoais objeto do tratamento tenham sido coletados no território nacional.

§ 1º Consideram-se coletados no território nacional os dados pessoais cujo titular nele se encontre no momento da coleta. (BRASIL, 2018).

A lei é bem descritiva sobre o seu alcance e princípios, em seu Artigo 5º trás as definições dos termos que aborda durante todo o texto legal. Além do mais, no Capítulo III da

¹⁸ Para mais informações, ver: <https://gdpr-info.eu/>

lei observamos os direitos do titular dos dados pessoais, que estão dispostos no Artigo 18: confirmação da existência de tratamento, acesso aos dados, correção deles, anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade, portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa, portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa, informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados, informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa e revogação do consentimento.

Uma disposição importante da lei que avança e se junta ao CGI.br, para a regulação do ambiente virtual, é a criação da Autoridade Nacional de Proteção de Dados (ANPD). A ANPD foi criada posteriormente pela Lei 13.853/2019 e é órgão da administração pública (ao contrário do CGI.br) que tem por objetivo a implementação, zelar pela proteção dos dados pessoais e a fiscalização da implementação da lei. É, inclusive, a ANPD que aplica as sanções administrativas previstas nos Artigos 53 e 54 da lei (BRASIL, 2018; NASCIMENTO, SBAITE E SOARES, 2020).

Por fim, se faz importante abordamos a Emenda Constitucional 115 de 2022 que inseriu no rol do Artigo 5º da Constituição o inciso LXXIX que possui a seguinte redação “LXXIX - é assegurado, nos termos da lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais.” (BRASIL, 1988). Dessarte, temos que a proteção dos dados pessoais é direito fundamental devidamente positivado na Constituição.

Sarlet (2022) destaca que a inclusão da proteção de dados ao rol dos direitos fundamentais cobre algumas lacunas que a LGPD havia deixado, tais como segurança nacional, segurança pública, investigação criminal e execução penal. Assim, para o autor, com essa cobertura constitucional, o ornamento jurídico brasileiro passa a abranger todas as nuances da proteção dos dados pessoais.

A LGPD é uma importante lei do nosso ordenamento no que tange a governança da Internet, em seu pouco tempo de vigência já surte efeitos e coloca em voga a cultura da proteção e privacidade de dados (RIVELLI, 2021). Não somente as empresas estão se conscientizando sobre o tratamento dos dados dos usuários, mas também os próprios consumidores estão se

questionam sobre o que é feito com os seus dados. Diariamente fornecemos dados pessoais e devemos ter consciência sobre qual conteúdo que disponibilizamos.

2.3.4 LEI N° 14.132, DE 31 DE MARÇO DE 2021 E LEI N° 14.155, DE 17 DE MAIO DE 2021

Em 2021 o ordenamento jurídico brasileiro teve duas leis sancionadas que alteravam o Código Penal para incluir e agravar crimes de cunho cibernético. A primeira de março, que insere dispositivo e passa a tipificar o crime de perseguição e, a segunda, de maio no qual altera o Art. 154-A e o torna mais gravoso, ambos do Código Penal.

No que tange a Lei 14.132/2021 ela inclui no Código Penal o Artigo 147-A que tipifica o crime de perseguição, no qual, de acordo com Cunha (2021) tem por finalidade “...a tutela da liberdade individual, abalada por condutas que constroem alguém a ponto de invadir severamente sua privacidade e de impedir sua livre determinação e o exercício de liberdades básicas.”.

Perseguição

[Art. 147-A.](#) Perseguir alguém, reiteradamente e por qualquer meio, ameaçando-lhe a integridade física ou psicológica, restringindo-lhe a capacidade de locomoção ou, de qualquer forma, invadindo ou perturbando sua esfera de liberdade ou privacidade.

Pena – reclusão, de 6 (seis) meses a 2 (dois) anos, e multa.

§ 1º A pena é aumentada de metade se o crime é cometido:

I – contra criança, adolescente ou idoso;

II – contra mulher por razões da condição de sexo feminino, nos termos do § 2º-A do art. 121 deste Código;

III – mediante concurso de 2 (duas) ou mais pessoas ou com o emprego de arma.

§ 2º As penas deste artigo são aplicáveis sem prejuízo das correspondentes à violência.

§ 3º Somente se procede mediante representação. (BRASIL, 2021a).

Essa lei revoga o dispositivo da Lei das contravenções penais no qual a perseguição era tratada, portanto, inferindo-se que tal conduta era de menor potencial lesivo e a insere no rol de crimes tipificados. O crime, conforme o artigo acima, consiste na ação de “perseguição”, destacando que não somente no sentido físico de ir atrás de algum indivíduo, mas de importunação e incômodo, além da utilização de violência ou ameaça (CUNHA, 2021).

Essa tipificação penal se enquadra no escopo desta pesquisa, pois a perseguição pode ser feita por “qualquer meio” e de “qualquer forma” invadindo a liberdade e privacidade. Portanto, a perseguição feita por meio virtual também pode ser uma conduta cabível de ser

criminalmente punida. Assim, podemos citar como exemplo, a perseguição por mensagens de texto (aplicativo de mensagens variados, tais como: *WhatsApp*, *Telegram*, *Messenger*, *Instagram*), e-mails, comentários, os quais podem acometer como ameaças psicológicas.

Essa perseguição virtual também pode desencadear uma perseguição física, uma vez que as pessoas postam suas rotinas online, muitas vezes, de maneira impensada. Cunha (2021) destaca que esse crime só admite a modalidade dolosa e de forma habitual, portanto, havendo vontade consciente e que haja mais de um ato de perseguição.

Sobre a Lei 14.155/2021 temos inclusão e alteração de dispositivos já existente. Essa Lei torna o crime de violação de dispositivo informático, furto e estelionato cometido de forma eletrônica ou pela internet mais gravoso, ou seja, a tipificação contida no Art. 154-A, o qual vimos anteriormente que fora inserido pela Lei Carolina Dieckmann.

Quanto a alteração, a Lei inclui a agravante de furto qualificado (Art. 155, § 4º-B, Código Penal) quando cometido por meio de dispositivo eletrônico ou informático, conectado ou não à internet e mesmo que não haja a violação de mecanismo de segurança. De acordo com o apontado por Baptista (2021), esse projeto de lei de iniciativa do Senador Izalci Lucas, seria devido a falta de punição adequada para os crimes de fraude eletrônica.

§ 4º-B. A pena é de reclusão, de 4 (quatro) a 8 (oito) anos, e multa, se o furto mediante fraude é cometido por meio de dispositivo eletrônico ou informático, conectado ou não à rede de computadores, com ou sem a violação de mecanismo de segurança ou a utilização de programa malicioso, ou por qualquer outro meio fraudulento análogo (BRASIL, 2021b).

Desta forma, podemos observar que o sancionamento de ambas as Lei mostram novamente que o direito brasileiro está tentando acompanhar a evolução virtual que acontece nos meios cibernéticos. Embora, seja natural que a atualização da normativa ocorra com atraso, uma vez que tal evolução ocorra de maneira exponencial e o ordenamento jurídico requer tempo e observação da sociedade para ir se modernizando.

2.3.5 PROJETO DE LEI Nº 2630/2020 (LEI BRASILEIRA DE LIBERDADE, RESPONSABILIDADE E TRANSPARÊNCIA NA INTERNET)

O Projeto de Lei 2630/2020 institui a Lei Brasileira de Liberdade, Responsabilidade e Transparência na Internet foi apresentado pelo senador Alessandro Vieira e já foi aprovado pelo Senado em junho de 2020. Em julho de 2020, o projeto foi recebido pela Câmara dos Deputados e, no momento, de acordo com informações do andamento do site da Câmara¹⁹, a votação da PL aguarda a criação da comissão especial pela Mesa Diretora.

Essa lei ganhou o apelido de Lei das Fake News, uma vez que tem como propósito criar medidas de transparência para combater conteúdo falso nas redes sociais e serviços de mensagens privadas, conseqüentemente, a sua disseminação através desses meios. A lei também seria aplicada não somente aos provedores de redes sociais e serviços de mensagem no Brasil, mas também aos que possuem sede no exterior, mas que ofertem serviço ao público brasileiro.

O Projeto de Lei também prevê que os provedores de redes sociais e mensagens privada devem adotar medidas para vedar contas falsas ou automatizadas (as que são geridas por robôs e não tem input orgânico) e identificar conteúdos publicitários (tal como já vemos no Instagram com publicidades). Além disso, esses provedores devem ser capazes de identificar movimentações que sejam incompatíveis com a capacidade humana²⁰(HAJE, 2020).

O projeto também coloca que o Congresso Nacional instituirá o Conselho de Transparência e Responsabilidade na Internet que será responsável por estudos, pareceres e recomendações sobre liberdade, responsabilidade e transparência, além de acompanhar as medidas que a lei trata. Esse Conselho teria um representante do CGI.br em seu quadro de 21 conselheiros. Além disso, as sanções previstas no projeto são de aplicação de multa e advertência, inclusive, destacando que os valores das multas serão revertidos ao Fundeb (Fundo de Manutenção e Desenvolvimento da Educação Básica e de Valorização dos Profissionais da Educação) e voltado para educação e alfabetização digital (DEPUTADOS, 2023).

¹⁹ Para informações sobre a tramitação, ver: <https://www.camara.leg.br/propostas-legislativas/2256735>

²⁰ Um exemplo dessa incompatibilidade com a capacidade humana que observamos recentemente é que IMDB (*Internet Movie Database*) alterou o seu mecanismo de votação nos cálculos da classificação do *live action* da “A Pequena Sereia” que estreou em maio de 2023. O filme já vinha recebendo comentários racistas e desde a estreia houve um boom de notas de negativas, o qual foi considerado uma atividade inumana. A mesma alteração foi feita pelo IMDB com relação ao filme “Marighella”. Ver: <https://portalpopline.com.br/imdb-atividade-incomum-avaliacoes-a-pequena-sereia/> / <https://cinebuzz.uol.com.br/noticias/cinema/marighella-e-atacado-no-imdb-e-site-muda-forma-de-calculo-da-nota.phtml>

Ruediger (2022) aponta que a elaboração desse projeto de lei é uma tentativa do Brasil de avançar junto à países da Europa que já possuem legislações semelhantes. O autor inclusive cita que a União Europeia em 2022 aprovou duas legislações nesse sentido. A primeira é a Lei dos Serviços Digitais (*Digital Services Act*) que tem como um dos objetivos a responsabilização por conteúdos ilegais em locais como os *marketplaces*, redes sociais, lojas de aplicativos e plataformas de viagens e acomodação, por exemplo (EU, 2023). A segunda é o Ato de Mercados Digitais (*Digital Markets Act*) que estabelece regras para plataformas digitais com papel de mercado. Portanto, tem por objetivo regular as empresas que fornecem ao usuário opções de consumo, por exemplo, comércio eletrônico, anúncios online, lojas de aplicativos (RUEDIGER, 2022; EU, 2023).

O Projeto de Lei ainda se encontra em votação e enfrenta(rá) um caminho tortuoso, uma vez que algumas polêmicas foram levantadas acerca do conteúdo. A questão da censura na prática da aplicação e da possibilidade de sanção penal no texto, são algumas que estão em voga. Por ser uma questão contemporânea à pesquisa, somente no futuro veremos o resultado, mas é mais uma movimentação do legislativo brasileiro em busca de um ordenamento jurídico que abranja as nuances que novas tecnologias trazem para o cotidiano da sociedade.

Neste capítulo vimos a atuação do Brasil no campo da governança da Internet. O quanto o país está inovando internamente em busca de normativas que consigam abarcar as mudanças e nuances que surgem constantemente quando falamos sobre internet e mundo virtual. Mostrou-se o quanto o país está na vanguarda junto com potências, tais quais a Europa e, que busca avançar na regulamentação, vide a discussão contemporânea do projeto de lei. Assim, no próximo capítulo, fecharemos a pesquisa com os desafios que são colocados nessa seara, tais como a privacidade, democracia e direitos humanos.

CAPÍTULO 3: DESAFIOS DA GOVERNANÇA GLOBAL DA INTERNET

Para o encerramento desta pesquisa, nessa seção, são abordadas temáticas que emergem a partir de tudo o que abordamos em epígrafe. Esses temas são novos desafios que surgem conforme a tecnologia avança, tais como os direitos humanos, a privacidade e a democracia. Neste capítulo, se faz importante levar em consideração que estes assuntos não são apartados

entre si, pelo contrário, cada um deles guarda relação com os outros, seja ela de maior ou menor grau.

DEMOCRACIA

Tomaremos a democracia como o ponto de partida para o desenvolvimento desta seção, destacando que não cabe a este trabalho os pormenores da relação, pois busca-se apenas demonstrar que a democracia também é afetada e se torna um desafio concomitante a Revolução de Digital que presenciamos acontecer contemporaneamente.

Primeiro, o entendimento de democracia está baseado na definição trazida pelo Núcleo de Pesquisa de Políticas Públicas da Universidade de São Paulo (NUPPs):

Segundo a definição mínima, a decisão sobre quem está autorizado a exercer o poder está baseada na lei, que a submete ao voto dos cidadãos (em substituição à antiga prática do sorteio); o voto é considerado um direito democrático se todos os indivíduos afetados por decisões coletivas puderem influir na escolha em condições iguais, podendo votar e ser votado. Além disso, o voto é efetivo se as eleições são livres, regulares e monitoradas por uma instituição independente de outras instituições do Estado, envolvendo o direito de contestação de quem exerce o poder através da competição política ao menos entre dois contendores diferentes. Ou seja, o direito de escolher quem pode exercer o poder expressa o princípio de que na democracia o soberano é o cidadão em sua condição de eleitor; mas, para ser efetiva, essa soberania depende de que os eleitores tenham o direito de se expressar livremente, de se organizar em partidos e/ou associações voluntárias, de ter assegurado o direito de competir em condições de igualdade e, finalmente, de ter acesso a fontes de informação não subordinadas às estruturas de poder. Essas normas, consolidadas em constituições políticas, fazem da democracia um governo baseado em leis em contraposição ao governo dos homens; é um sistema de governança em que os governantes devem explicações de seus atos, o tempo todo, aos que os elegeram ou aos seus representantes. (NUPPs, [S.I]).

A expansão da internet e redes sociais geram o aumento do fluxo de informações e trocas de conteúdo entre usuários em si e interação entre usuários e conteúdos criados. Portanto, a

velocidade com que cidadãos possam externar a insatisfação, favorecimento, descontentamento etc., com relação à alguma política, governo ou governante é instantânea²¹.

Oliveira (2013) ratifica esta visão e acrescenta que esse avanço lança uma nova perspectiva sobre o debate democrático, uma vez que essas relações instantâneas e entre grupos que não estão fisicamente próximos, gera um maior poder de influência. Ademais, o autor também aborda que os meios de mídias tradicionais, ao contrário do que circula na internet, são dependentes de concessão governamental, portanto, suas posições políticas podem ser enviesadas de algum modo.

De acordo com Balkin (2004) a revolução digital mudou as práticas de liberdade de discurso de quatro maneiras diferentes. A primeira é a diminuição dos custos para a distribuição de informação, já que os indivíduos podem transmitir suas publicações e pensamentos de maneira rápida e sem custos, um exemplo que podemos ver são os blogs, postagens em redes sociais. Segundo é que o conteúdo não tem mais fronteiras culturais e geográficas, uma vez na rede, o conteúdo vai circular livremente. Muitas vezes nem o idioma é uma barreira, pois, por exemplo, o Google tem a ferramenta de tradução acoplada ao navegador, o que gera uma tradução do conteúdo mostrado na tela.

Em terceiro, os custos com inovação da informação existente são menores, ou seja, conectado à primeira mudança, nesta os usuários podem distribuir, copiar e, até alterar o que já chega pronto. Desse ponto, podemos citar a questão com a manipulação de imagens, vídeos, áudios que está em voga. Até que ponto podemos acreditar no que vemos online? Essa é uma pergunta que devemos ter em mente ao interagir com o mundo virtual. Por fim, em quarto, temos a democratização do discurso, justamente pela diminuição dos custos de transmissão, apropriação e distribuição das informações (BALKIN, 2004).

A questão da qualidade da informação também deve ser mencionada nesta seara. A quantidade de informação, o tanto que pode ser compartilhada e manipulada, conforme vimos acima, além do que, os algoritmos são treinados e personalizados pelo tipo de conteúdo que

²¹ Não cabe ao escopo deste trabalho de pesquisa pormenorizar as relações entre política e internet. Para um aprofundamento no tema, existem pesquisas de pós-graduação focadas no assunto, ver:
<https://museudememes.com.br/>
<https://ppgcom.uff.br/rangel-ramiro-ramos>
<https://ppgcom.uff.br/tsai-yi-jing/>

cada pessoa acessa individualmente, influenciam no que devidamente apresentado como disponível. Portanto, nem tudo o que se observa online é o todo, esses fatores levam a formação de uma “bolha” de conteúdo, somando-se a velocidade com o que estes são gerados, pode-se ter a uma superficialidade no que tange a qualidade da informação (OLIVEIRA, 2013).

Portanto, entre muitos desafios, Oliveira (2013) coloca que a internet não serve como um meio fiel e forte para a promoção da democracia, mas vai no sentido oposto de ser uma ferramenta para junção e diálogo de ideias divergentes. O meio virtual torna a discussão polarizada, com algoritmos que são treinados a se manterem no campo de conforto, portanto, ideais divergentes não conversam entre si. Além do que, há a possibilidade de criação de conteúdos falsos e automatizado, conforme vimos no capítulo anterior com a apelidada PL das *fake news*.

JURISDIÇÃO E CRIME

O seguinte desafio é o que tange a normatização jurídica das relações em ambiente virtual, ou seja, a própria regulamentação da internet é um desafio. Um ponto que podemos abordar, indo ao encontro do que foi levantado por Lucero (2011) é a questão da jurisdição frente à extraterritorialidade. A internet permite justamente a transposição de fronteiras, desta forma não é impossível pensar que alguma ação executada em um território esteja resultando em crime ou contravenção em outro local.

No que vimos no capítulo anterior, a LGPD em seu Artigo 3º revela um caráter extraterritorial, uma vez que estabelece que a lei será aplicada independentemente do país de sede ou onde estejam localizados os dados, desde que sigam as regras dos incisos e parágrafos. A regra é baseada, principalmente, na operação de tratamento²² dos dados seja realizada em território nacional ou os dados coletos internamente, mas a sua aplicação pode ser feita fora dele.

²² Art. 5º Para os fins desta Lei, considera-se: X - tratamento: toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração; (BRASIL, 2018).

Outrossim, como observamos, os crimes que acontecem no meio virtual, sem um território físico restrito a um Estado, ficam em um limbo jurisdicional, em algumas ocasiões. Existem os crimes previstos no rol do Estatuto do Tribunal Penal Internacional, ou seja, os crimes contra a humanidade, genocídio, crimes de guerra e crime de agressão²³. Esses crimes são julgados em um tribunal internacional, todavia, os crimes cibernéticos dependem da jurisdição doméstica (LUCERO, 2011).

A Agenda de Túnis não deixa este ponto dos crimes cibernéticos cometidos em uma jurisdição e com efeitos em outra de fora de suas recomendações.

Nós também sublinhamos a necessidade de ferramentas e ações efetivas e eficientes, à nível nacional e internacional, para promover cooperação internacional entre, *inter alia*, agências policiais de crimes cibernéticos. Nós chamamos os governos em cooperação com outros interessados para desenvolver legislação necessária para a investigação e processo do crime cibernético, observando as estruturas existentes [...] (WSIS, 2005) (tradução nossa).²⁴

Essa problemática, onde em seus polos podem estar mais de um Estado, leva a um conflito de jurisdições, legislações e entendimentos acerca do ato e da própria governança da internet. Assim, o Fórum de Governança da Internet e a Cúpula Mundial sobre a Sociedade da Informação são mecanismos interessantes de discussões para políticas públicas, mas, infelizmente, não é suficiente para suprir as demandas que surgem no cotidiano da sociedade. Para o tratamento e coordenação de ações internacionais a tarefa passa a ser de cunho mais diplomático do que legislativo (LUCERO, 2011).

PRIVACIDADE

O último desafio apontado é o da privacidade, tão cara para os indivíduos, mas como quase um paradoxo, frequentemente exposta nas redes sociais. A privacidade pode ser entendida como a vida do indivíduo no seu mais íntimo, com suas relações

²³ Ver: https://www.planalto.gov.br/ccivil_03/decreto/2002/d4388.htm

²⁴ 40. We underline the importance of the prosecution of cybercrime, including cybercrime committed in one jurisdiction, but having effects in another. We further underline the necessity of effective and efficient tools and actions, at national and international levels, to promote international cooperation among, *inter alia*, law-enforcement agencies on cybercrime. We call upon governments in cooperation with other stakeholders to develop necessary legislation for the investigation and prosecution of cybercrime, noting existing frameworks, for example, UNGA Resolutions 55/63 and 56/121 on "Combating the criminal misuse of information technologies" and regional initiatives including, but not limited to, the Council of Europe's Convention on Cybercrime. (WSIS, 2005).

peçoais/sociais/profissionais/familiares/patrimonial. Não há uma exaustão de entendimentos do que pode ser privado em relação à algum sujeito, entretanto com a relação digital temos os dados pessoais dispostos em um clique. Dessarte, a privacidade e manutenção desta é um desafio para a governança da internet, como proteger os dados pessoais, imagens, preferências captadas por algoritmos (GODOY, 2017).

Conforme as redes sociais foram avançando, tanto de sofisticação quanto de popularidade, o compartilhamento de informações foi fazendo parte da rotina do indivíduo. Há diversas maneiras com que a privacidade é desafiada e a perda do controle dos nossos próprios dados é notável, afinal, quem nunca recebeu e-mail de lugar que sequer acessou oferecendo algo? Esses limites, até algum ponto éticos, de quem possui os dados e de quem fornece é que vão sendo testados mais e mais ao longo do avanço das tecnologias da informação (SCHWAB, 2016).

Canabarro (2018) aborda que a governança da internet tem como a interconexão plena, que é projetada pela internet das coisas, por exemplo, a Alexa que pode controlar uma casa inteira. Assim, a proteção da privacidade, dados pessoais, “economia do compartilhamento e novas modalidades de transação online que desafiam o sistema financeiro global; governança dos algoritmos que estruturam as aplicações e serviços na Internet; etc.,” (p.84), são pontos enfrentados ao construir uma governança da internet que seja completa.

Na legislação brasileira a privacidade e sua proteção são bem marcantes, o Marco Civil já traz essa prerrogativa e para a LGPD, a proteção dos dados pessoais é o mote legal. O Marco Civil da Internet tem como princípio do uso da internet no Brasil a proteção da privacidade (Art. 3º, inciso II, L. 12.965/2014) e que o direito à privacidade é condição plena para o acesso à internet, além de que institui a nulidade de cláusulas contratuais que violem este direito, tal como vemos abaixo:

Art. 8º A garantia do direito à privacidade e à liberdade de expressão nas comunicações é condição para o pleno exercício do direito de acesso à internet.

Parágrafo único. São nulas de pleno direito as cláusulas contratuais que violem o disposto no **caput**, tais como aquelas que:

I - impliquem ofensa à inviolabilidade e ao sigilo das comunicações privadas, pela internet; ou

II - em contrato de adesão, não ofereçam como alternativa ao contratante a adoção do foro brasileiro para solução de controvérsias decorrentes de serviços prestados no Brasil. (BRASIL, 2014).

Na LGPD a privacidade e intimidade vem como direitos fundamentais (“Art. 17. Toda pessoa natural tem assegurada a titularidade de seus dados pessoais e garantidos os direitos fundamentais de liberdade, de intimidade e de privacidade, nos termos desta Lei.”). Posteriormente, em 2022, a Constituição Federal reforçou e garantiu que a proteção dos dados pessoais, integrante do escopo da privacidade, fosse reconhecida como direito fundamental, conforme visto no capítulo anterior.

Nesse sentido, os Direitos Humanos também abarcam questões de privacidade. Embora a Declaração Universal de Direitos Humanos (DUDH) da Organização das Nações Unidas (ONU) tenha sido proclamada em 1948, ela já trazia o respeito a privacidade em seu dispositivo: “Artigo XII - Ninguém será sujeito à interferência em sua vida privada, em sua família, em seu lar ou em sua correspondência, nem a ataque à sua honra e reputação. Todo ser humano tem direito à proteção da lei contra tais interferências ou ataques.” (ONU, 2009, p.8).

Em outra legislação internacional o direito à privacidade é recepcionado, citamos o Pacto de San José da Costa Rica que promulga a Convenção Americanas sobre Direitos Humanos, no âmbito da Organização dos Estados Americanos (OEA). A Convenção entrou em vigor internacional em 1978 e o Brasil deposita a carta de adesão e promulga a mesma em território nacional em 1992. No Artigo 11.2 e 11.3 do Pacto, vemos a proteção ao direito a privacidade sendo positivada, segue:

ARTIGO 11

Proteção da Honra e da Dignidade

1. Toda pessoa tem direito ao respeito de sua honra e ao reconhecimento de sua dignidade.
2. Ninguém pode ser objeto de ingerências arbitrárias ou abusivas em sua vida privada, na de sua família, em seu domicílio ou em sua correspondência, nem de ofensas ilegais à sua honra ou reputação.
3. Toda pessoa tem direito à proteção da lei contra tais ingerências ou tais ofensas. (BRASIL, 1992).

Na Constituição de 1988, o direito à privacidade foi recepcionado pela Carta Magna como direito fundamental positivado em alguns incisos do Artigo 5º. O primeiro é o inciso X, no qual carrega redação semelhante ao da DUDH, vemos, “X – são invioláveis a intimidade, a

vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação;” e, temos o inciso XII, no qual temos a redação: “XII - é inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal;” (BRASIL, 1988).

Conforme vimos no Capítulo anterior e já comentado nesta seção, a Constituição teve alteração com a EC 115/2022 que inseriu o inciso LXXIX no rol dos direitos fundamentais, para especificamente dar proteção aos dados pessoais nos meios digitais. Embora existam essas normativas internacionais sobre a proteção à privacidade, a implementação em território nacional depende da anuência do Estado em promover normas jurídicas que permitam o seu cumprimento (KEMER, 2018).

O Brasil sofreu com a violação de sua privacidade com o caso Snowden, a nível estatal a questão pode gerar incidentes diplomáticos. Assim, a presidenta Dilma em conjunto com a chanceler alemã Angela Merkel, que também sofreu com a espionagem de ligações telefônicas, foram protagonistas na Assembleia Geral da ONU copatrocinaram duas resoluções com o título “O Direito a privacidade na era digital” (The right to privacy in the digital age). (MACASKILL & DANCE, 2013; ROCHA, 2017).

Na resolução 68/167 de 2013 destaca que o desenvolvimento de tecnologias ao mesmo tempo que aumenta a capacidade dos indivíduos de utilizarem e terem acesso à novas informações, também aumenta a capacidade de governos, empresas e indivíduos para super vigilância e de recolherem dados. Inclusive a resolução cita o artigo 12 da Declaração Universal de Direitos Humanos (UN, 2013).

Esta resolução reforça o direito humano à privacidade e rechaça interferência ilegal e arbitrária a privacidade, inclusive, frisando que a lei deve proteger contra tais atos. Um ponto tocado e que faz referência direta ao caso Snowden é sobre a coleta de dados ilegal e interceptação telefônica as quais é explicitamente dito que contradiz os princípios de uma sociedade democrática e fere os direitos humanos (UN, 2013).

No ano seguinte veio a resolução 69/166 que recapitula a resolução 68/167 e reforça algumas das discussões feitas anteriormente. Entretanto, esta segunda resolução é mais abrangente e também colocar luz sobre a promoção da proteção de dados pessoais e metadados, os quais internamente nos Estado Nação, muitas das vezes, não possuem nenhum grau de proteção (UN, 2014; ROCHA, 2017).

O Brasil à época tinha uma política externa muito ativa e, com a questão da espionagem evidenciada por Snowden, o país passou a se posicionar mais ainda com relação a proteção da proteção da privacidade. Em 2017 o país foi novamente importante para outra resolução da ONU (resolução 34/7 de 2017), onde o direito à privacidade fora reforçado à luz da Declaração Universal dos Direitos Humanos (KEMER, 2018).

Neste capítulo final da pesquisa foi proposto uma abordagem sobre três desafios que a governança da internet enfrenta mundialmente, mas a questão brasileira foi abordada em todos, uma vez que no capítulo anterior foi feito um apanhado da legislação nacional. A visualização de tais desafios é importante para análise do andamento das legislações sobre a temática e para a identificação de pontos que possam vir a ser lapidados em normativas futuras.

CONSIDERAÇÕES FINAIS

Esta monografia tratou da governança da internet num âmbito global e voltada para a perspectiva brasileira. Sobre a questão global, passamos pelo entendimento conceitual, uma vez que abordamos o que é internet, entretanto sem se ater a questão técnica, que guarda a sua importância, mas não para esta pesquisa. Posteriormente vislumbramos o conceito de governança global da internet e quais atores que fazem parte. O primeiro capítulo formou o terreno para a compreensão do tema que nos rodeia diariamente, mas que por justamente estarmos imersos nele, não conseguimos dimensionar o quanto somos afetados e deveríamos nos preocupar e ter cautela.

Sobre o Brasil, o capítulo dois evocou a atuação do país na governança da internet. Como demonstrado na pesquisa, o Brasil está, de algum modo, na vanguarda da preocupação com o tema. Desde os anos 90 com a criação do Comitê Gestor da Internet no Brasil (CGI.br) e avançando com a atuação ativa na ONU nos anos 2000, o país se mostra preocupado com a segurança no ambiente virtual, privacidade e proteção de dados. Como também, com a criação de legislações domésticas com temática relacionada, seja com um Marco Civil da Internet, que inclusive foi elogiado internacionalmente, a LGPD ou com leis que tipificam crimes cibernéticos.

Por fim, no terceiro capítulo fora feita uma seleção com três desafios que a governança da internet enfrenta mundialmente. A democracia com a quantidade de dados e manipulação que pode ser feita com eles, merece atenção mundial, até pelo movimento que se observa mundialmente das notícias falsas. O Brasil está em um momento de votação de um projeto de lei que justamente busca coibir essa prática. A jurisdição e crime, no qual se faz urgente o diálogo e coesão entre países para que haja a correta verificação e julgamento de delitos. E, a privacidade que é a questão que permeia diversas temáticas quando tratamos de ambiente virtual. A sua proteção, como vimos, é uma pauta importante de defesa por parte do Brasil e do mundo.

A escolha dos desafios foi pautada em tudo o que abordamos ao longo da pesquisa, portanto não existe a pretensão de auferir que existam somente esses, tendo cada um deles o potencial de se tornarem pesquisas próprias. Mas de mostrar que os desafios vão surgindo ao

longo do avanço das tecnologias, como, por exemplo, a questão em voga atualmente da inteligência artificial.

Considerando tudo o que foi abordado ao longo dos capítulos desta pesquisa, não se buscou chegar à uma conclusão fechada e binária sobre se algum país está fazendo certo ou errado ao tratar a governança da internet. O cerne sobre a temática foi apresentar um levantamento bibliográfico e fazer com que o enquadramento desta pesquisa sirva para levantar novas questões e debates a serem trabalhadas em pesquisas futuras.

REFERÊNCIAS BIBLIOGRÁFICAS

ARAÚJO, Janaína. **Dez anos de vigência da Lei Carolina Dieckmann: a primeira a punir crimes cibernéticos.** 2023. Disponível em: <https://www12.senado.leg.br/radio/1/noticia/2023/03/29/dez-anos-de-vigencia-da-lei-carolina-dieckmann-a-primeira-a-punir-crimes-ciberneticos>. Acesso em: 13 jun. 2023.

BALKIN, Jack M.. Digital Speech and Democratic Culture: a theory of freedom of expression for the information society. **New York University Law Review**, Nova Iorque, v. 79, p. 1-58, abr. 2004. Disponível em: <https://www.nyulawreview.org/issues/volume-79-number-1/digital-speech-and-democratic-culture/>. Acesso em: 19 jun. 2023.

BAPTISTA, Rodrigo. **Lei com penas mais duras contra crimes cibernéticos é sancionada.** 2021. Elaborada por Agência Senado. Disponível em: <https://www12.senado.leg.br/noticias/44diçoes44/2021/05/28/lei-com-penas-mais-duras-contr-crimes-ciberneticos-e-sancionada>. Acesso em: 13 jun. 2023.

BRASIL. **Constituição da República Federativa do Brasil.** 1988. Brasília, Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 13 jun. 2023.

BRASIL. **Promulga a Convenção Americana sobre Direitos Humanos (Pacto de São José da Costa Rica), de 22 de novembro de 1969.** 1992. Brasília, Disponível em: https://www.planalto.gov.br/ccivil_03/decreto/d0678.htm. Acesso em: 13 jun. 2023.

BRASIL. Portaria Interministerial MCT/MC nº 147, de 31.05.1995. Cria o Comitê Gestor Internet Brasil. **Ministério da Ciência, Tecnologia e Inovações.** Brasília, DF, 01 de junho de 1995. Disponível em: https://antigo.mctic.gov.br/mctic/opencms/legislacao/portarias_interministeriais/migracao/Portaria_Interministerial_MCTMC_n_147_de_31051995.html. Acesso em: 7 jun 2023.

_____. Decreto nº 4.829, de 3 de setembro de 2003. Dispõe sobre a criação do Comitê Gestor da Internet no Brasil – CGIbr, sobre o modelo de governança da Internet no Brasil, e dá outras providências. **Diário Oficial [da] República Federativa do Brasil**, Poder Executivo. Brasília, DF, 4 de setembro de 2003. Disponível em: <https://pesquisa.in.gov.br/imprensa/jsp/visualiza/index.jsp?jornal=1&pagina=24&data=04/09/2003>. Acesso em: 7 jun 2023.

_____. **Lei nº 12.737, de 30 de novembro de 2012.** Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 – Código Penal; e dá outras providências. 2012. Brasília, Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/112737.htm. Acesso em: 09 jun. 2023.

_____. **Lei nº 12.965, de 23 de abril de 2014.** Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. 2014. Brasília, Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/112965.htm. Acesso em: 09 jun. 2023.

_____. **Lei nº 13.709, de 14 de agosto de 2018.** Lei Geral de Proteção de Dados Pessoais (LGPD). 2018. Brasília, Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/113709.htm. Acesso em: 17 jun. 2023.

_____. **Lei nº 14.132, de 31 de março de 2021.** Acrescenta o art. 147-A ao Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), para prever o crime de perseguição; e revoga o art. 65 do Decreto-Lei nº 3.688, de 3 de outubro de 1941 (Lei das Contravenções Penais). 2021^a. Brasília, Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/lei/114132.htm. Acesso em: 13 jun. 2023.

_____. **Lei nº 14.155, de 17 de maio de 2021.** Altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), para tornar mais graves os crimes de violação de dispositivo informático, furto e estelionato cometidos de forma eletrônica ou pela internet; e o Decreto-Lei nº 3.689, de 3 de outubro de 1941 (Código de Processo Penal), para definir a competência em modalidades de estelionato. 2021^b. Brasília, Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/Lei/L14155.htm. Acesso em: 13 jun. 2023.

CANABARRO, Diego. Governança Global da Internet: Aspectos Conceituais, Questões da Agenda Contemporânea e Prospectos para o Estudo do Tema. In: OPPERMANN, Daniel (ed.). **Internet Governance in the Global South: history, theory, and contemporary debates.** São Paulo: Núcleo de Pesquisa em Relações Internacionais (Nupri) – Universidade de São Paulo (USP), 2018. P. 74-108. Disponível em: https://nupri.prp.usp.br/pdf/Internet_Governance_in_the_Global_South_Daniel_Oppermann.pdf. Acesso em: 29 maio 2023.

CERT.BR, Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil. **Sobre a Cartilha de Segurança para Internet**. Elaborada por NIC.BR (Núcleo de Informação e Coordenação do Ponto BR). [2021]. Disponível em: <https://cartilha.cert.br/sobre/>. Acesso em: 8 jun 2023.

CGI.BR, Comitê Gestor da Internet no Brasil -. **Princípios para o Uso e a Governança da Internet no Brasil**. Resolução CGI.br/RES/2009/003/P. São Paulo: CGI.br, 2009. Disponível em: <https://www.cgi.br/media/docs/publicacoes/1/cgi-decalogo.pdf>. Acesso em: 7 jun 2023.

CGI.BR, Comitê Gestor da Internet no Brasil -. **Composição do CGI.br**. São Paulo: CGI.br, 2023^a. Disponível em: <https://www.cgi.br/membros/>. Acesso em: 7 jun 2023.

_____, Comitê Gestor da Internet no Brasil -. **História do CGI.br**. São Paulo: CGI.br, 2023b. Disponível em: <https://www.cgi.br/historicos/>. Acesso em: 8 jun 2023.

CUNHA, Rogério Sanches. **Lei 14.132/21: Insere no Código Penal o art. 147-A para tipificar o crime de perseguição**. 2021. Disponível em: <https://meusitejuridico.editorajuspodivm.com.br/2021/04/01/lei-14-13221-insere-no-codigo-penal-o-art-147-para-tipificar-o-crime-de-perseguiacao/>. Acesso em: 13 jun. 2023.

DEPUTADOS, Câmara dos. **PL 2630/2020**. 2023. Disponível em: <https://www.camara.leg.br/propostas-legislativas/2256735>. Acesso em: 15 jun. 2023.

DPCE, Defensoria Pública Geral do Estado do Ceará -. **Lei Carolina Dieckmann: 10 anos da lei que protege a privacidade dos brasileiros no ambiente virtual**. 2022. Elaborada por DPCE. Disponível em: <https://www.defensoria.ce.def.br/noticia/lei-carolina-dieckmann-10-anos-da-lei-que-protege-a-privacidade-dos-brasileiros-no-ambiente-virtual/>. Acesso em: 13 jun. 2023.

EU, European Commission -. **The Digital Services Act package**: uma contribuição para a análise do debate nacional frente a um desafio global. Uma contribuição para a análise do debate nacional frente a um desafio global. 2023. Disponível em: <https://digital-strategy.ec.europa.eu/en/policies/digital-services-act-package>. Acesso em: 17 jun. 2023.

FMP, Fundação Escola Superior do Ministério Público do Rio Grande do Sul -. **LEI CAROLINA DIECKMANN: VOCÊ SABE O QUE ESSA LEI REPRESENTA?** 2021. Elaborada por FMP. Disponível em: <https://fmp.edu.br/lei-carolina-dieckmann-voce-sabe-o-que-essa-lei-representa/>. Acesso em: 13 jun. 2023.

GIDDENS, Anthony. **As Conseqüências da modernidade**. São Paulo: Editora UNESP, 1991.

GROSSMANN, Luís Osvaldo. **Governança na Internet: muito além do multilateralismo x multissetorialismo**. 2014. Elaborada por NIC.BR (Núcleo de Informação e Coordenação do Ponto BR). Disponível em: <https://nic.br/noticia/na-midia/governanca-na-internet-muito-alem-do-multilateralismo-x-multissetorialismo/> Acesso em: 29 maio 2023.

GODOY, Claudio Luiz Bueno de. Privacidade. **Enciclopédia jurídica da PUC-SP**. Celso Fernandes Campilongo, Alvaro de Azevedo Gonzaga e André Luiz Freire (coords.). Tomo: Direito Civil. Rogério Donnini, Adriano Ferriani e Erik Gramstrup (coord. de tomo). 1. ed. São Paulo: Pontifícia Universidade Católica de São Paulo, 2017. Disponível em: <https://enciclopediajuridica.pucsp.br/verbete/474/edicao-1/privacidade>. Acesso em: 22 jun. 2023.

HAESBAERT, Rogério. **Dos Múltiplos Territórios á Multiterritorialidade**. Porto Alegre. 2004. Disponível em: < <http://www.ufrgs.br/petgea/Artigo/rh.pdf>>. Acesso em: 18 maio 2023.

HAESBAERT. **O Mito da Desterritorialização: Do “fim dos territórios” à multiterritorialidade**. Rio de Janeiro: Bertrand Brasil, 2011.

HAJE, Lara. **Projeto do Senado de combate a notícias falsas chega à Câmara**. 2020. Elaborada por Agência Câmara de Notícias. Disponível em: <https://www.camara.leg.br/noticias/673694-projeto-do-senado-de-combate-a-noticias-falsas-chega-a-camara/>. Acesso em: 17 jun. 2023.

KEMER, Thaíse. A Política Externa Brasileira na Governança da Internet: do Direito à Privacidade ao Direito à Participação. In: OPPERMANN, Daniel (ed.). **Internet Governance in the Global South: history, theory, and contemporary debates**. São Paulo: Núcleo de Pesquisa em Relações Internacionais (Nupri) – Universidade de São Paulo (Usp), 2018. P. 363-397. Disponível em: https://nupri.prp.usp.br/pdf/Internet_Governance_in_the_Global_South_Daniel_Oppermann.pdf. Acesso em: 29 maio 2023.

LUCERO, Everton. **Governança da Internet: aspectos da formação de um regime global e oportunidades para a ação diplomática**. Brasília: Fundação Alexandre de Gusmão, 2011. 236 p. Disponível em: http://funag.gov.br/loja/download/822-Governanca_da_Internet.pdf. Acesso em: 08 maio 2023.

MACASKILL, Ewen; DANCE, Gabriel. **NSA Files: Decoded**. What the revelation mean for you. 2013. Elaborada por The Guardian. Disponível em: <https://www.theguardian.com/world/interactive/2013/nov/01/snowden-nsa-files-surveillance-revelations-decoded>. Acesso em: 9 jun 2023.

MEDEIROS, Rosa Maria Vieira. Território, espaço de identidade. In: SAQUET, Marcos Aurelio; SPOSITO, Eliseu Savério (Org.). **Territórios e territorialidades: teorias, processos e conflitos**. São Paulo: Expressão Popular, 2009. P. 217-227.

MJ, Ministério da Justiça -. **A importância do marco civil e seu 48dições48o**. [2015a]. Elaborada por Ministério da Justiça. Disponível em: <http://pensando.mj.gov.br/marcocivil/a-importancia-do-marco-civil-e-seu-historico/>. Acesso em: 12 jun. 2023.

MJ, Ministério da Justiça -. **Marco Civil da Internet**. [2015b]. Elaborada por Ministério da Justiça. Disponível em: <http://pensando.mj.gov.br/marcocivil/>. Acesso em: 12 jun. 2023.

NASCIMENTO, Lorena Carneiro do; SBAITE, Mariana; SOARES, Paulo Vinícius de Carvalho. **100 PERGUNTAS SOBRE LGPD: legislação, mapeamento, implementação e dúvidas comuns**. LEGISLAÇÃO, MAPEAMENTO, IMPLEMENTAÇÃO E DÚVIDAS COMUNS. 2020. Elaborada por LBCA. Disponível em: https://d3351uupugsy2.cloudfront.net/cms/files/92859/1611860270FAQ_100_Perguntas_sobr_e_LGPD.pdf. Acesso em: 17 jun. 2023.

NETMUNDIAL. **NETmundial Multistakeholder Statement**. 2014. Disponível em: <https://netmundial.br/wp-content/uploads/2014/04/NETmundial-Multistakeholder-Document.pdf>. Acesso em: 9 jun 2023.

NIC.BR, Núcleo de Informação e Coordenação do Ponto BR. **Atividades**. 2023. Disponível em: <https://www.nic.br/atividades/>. Acesso em: 8 jun 2023.

NUPP, Núcleo de Pesquisa de Políticas Públicas da Universidade de São Paulo. **Democracia verbete**. [S.I]. Disponível em: https://sites.usp.br/nupps/wp-content/uploads/sites/762/2020/12/Anexo_02_Democracia-verbete.pdf. Acesso em: 19 jun. 2023.

OLIVEIRA, Fábio Cesar dos Santos. Democracia e internet: a revolução digital e os desafios à representação política. **Revista de Informação Legislativa**, Brasília, v. 199, p. 143-161, jul./set. 2013. Disponível em:

https://www12.senado.leg.br/ril/edicoes/50/199/ril_v50_n199_p143.pdf. Acesso em: 19 jun. 2023.

ONU, ORGANIZAÇÃO DAS NAÇÕES UNIDAS. Declaração Universal dos Direitos Humanos. 2009. Elaborada por UNIC/Rio.

PECEQUILO, Cristina Soreanu. **Introdução às Relações Internacionais: Temas, atores e visões**. Petrópolis: Editora Vozes, 2004.

RIVELLI, Fabio. **Balanco de um ano da LGPD**. 2021. Elaborada por LBCA. Disponível em: <https://app-sitelbca.azurewebsites.net/balanco-de-um-ano-da-lgpd/>. Acesso em: 17 jun. 2023.

ROCHA, Maurício Santoro. A Governança Global da Internet. In: SCHMITZ, Guilherme de Oliveira; ROCHA, Rafael Assumpção (org.). **Brasil e o Sistema das Nações Unidas: desafios e oportunidades na governança global**. Brasília: Ipea, 2017. p. 485-511.

ROCHA, Johnny. **Lei Carolina Dieckmann completa 10 anos com baixa efetividade, avalia especialista: para presidente do instituto de proteção das garantias individuais, leis precisam acompanhar ritmo do avanço das tecnologias**. 2022. Disponível em: <https://www.jota.info/justica/lei-carolina-dieckmann-completa-10-anos-com-baixa-efetividade-avalia-especialista-02122022>. Acesso em: 13 jun. 2023.

RUEDIGER, M. A. (Coord.). **Regulação de plataformas digitais: uma contribuição para a análise do debate nacional frente a um desafio global**. Policy paper. Rio de Janeiro: FGV DAPP, 2022. Disponível em: https://democraciadigital.dapp.fgv.br/wp-content/uploads/2022/05/PTEstudo-8_FichaISBN.pdf. Acesso em: 17 jun. 2023.

SARLET, Ingo Wolfgang. **A EC 115/22 e a proteção de dados pessoais como Direito Fundamental**. 2022. Disponível em: <https://www.conjur.com.br/2022-mar-11/direitos-fundamentais-ec-11522-protecao-dados-pessoais-direito-fundamental>. Acesso em: 17 jun. 2023.

SCHWAB, Klaus. **The Fourth Industrial Revolution: what it means, how to respond**. 2016. Disponível em: <https://www.weforum.org/agenda/2016/01/the-fourth-industrial-revolution-what-it-means-and-how-to-respond/>. Acesso em: 26 maio 2023.

UN, United Nations -. **The right to privacy in the digital age**. Resolution no 68/167, 2013. Disponível em: <https://digitallibrary.un.org/record/764407?ln=en>. Acesso em: 22 Jun 2023.

UN, United Nations -. **The right to privacy in the digital age**. Resolution no 69/ 166, 2014. Disponível em: <https://documents-dds-ny.un.org/doc/UNDOC/GEN/N14/707/03/PDF/N1470703.pdf?OpenElement>. Acesso em: 22 Jun 2023.

UN, United Nations. **World Summit on the Information Society (WSIS): "WSIS ACTION LINES: SUPPORTING THE IMPLEMENTATION OF SDGS"**. S.l.. Elaborada por UN. Disponível em: <https://sustainabledevelopment.un.org/index.php?page=view&type=30022&nr=102&menu=3170#:~:text=The%20first%20phase%20took%20place,than%2019%2C000%20representing%20174%20countries..> Acesso em: 24 maio 2023.

VERÍSSIMO JUNIOR, Adalberto Fraga. **Pioneira em proteção de dados, GDPR completa 5 anos de vigência**. 2023. Disponível em: <https://www.linkedin.com/pulse/pioneira-em-prote%25C3%25A7%25C3%25A3o-de-dados-gdpr-completa-5-anos-vig%25C3%25AAncia-lbca/?trackingId=oWtjrcj%2B7RzzfBas5uDuVg%3D%3D>. Acesso em: 17 jun. 2023.

WAGNER, Flávio Rech; CANABARRO, Diego R.. A Governança da Internet: definição, desafios e perspectivas. In: PIMENTA, Marcelo Soares; CANABARRO, Diego Rafael (org.). **Governança Digital**. Porto Alegre: Editora da UFRGS/Cegov, 2014. p. 191-209. Disponível em: <https://lume.ufrgs.br/handle/10183/214562>. Acesso em: 8 maio 2023.

WSIS, World Summit on The Information Society. **Declaration of Principles: Building the Information Society: a global challenge in the new Millennium**. 2003. Elaborada por UN & ITU. Disponível em: <https://www.itu.int/net/wsis/docs/geneva/official/dop.html>. Acesso em: 20 maio 2023.

WSIS, World Summit on The Information Society. **Tunis Agenda For The Information Society**. 2005. Elaborada por UN & ITU. Disponível em: <https://www.itu.int/net/wsis/docs2/tunis/off/6rev1.html>. Acesso em: 07 jun. 2022.