

VIGILÂNCIA E MONITORAMENTO NA SOCIEDADE DA INFORMAÇÃO: CONTRIBUIÇÕES DO CONSTITUCIONALISMO DIGITAL PARA A GOVERNANÇA DA INTERNET

SURVEILLANCE AND MONITORING IN THE INFORMATION SOCIETY: CONTRIBUTIONS OF DIGITAL CONSTITUTIONALISM TO INTERNET GOVERNANCE

Rodrigo Vitorino Souza Alves

Professor da Faculdade de Direito da Universidade Federal de Uberlândia (Graduação e Pós-Graduação). Doutor em Direito pela Universidade de Coimbra. Pesquisador líder do Centro Brasileiro de Estudos em Direito e Religião – Cedire e do Laboratório de Direitos Humanos – LabDH.

Thobias Prado Moura

Doutorando em Direito e Segurança na Universidade Nova de Lisboa. É pesquisador do WhatNext.Law, vinculado ao Cedis da Nova School of Law, do Laboratório de Direitos Humanos – LabDH e Membro do Internet Society. *E-mail:* thobiasp.moura@hotmail.com.

Luma Laura Damasceno Góes

Advogada. Mestranda pela University of Toronto. Graduada em Direito pela Universidade Federal de Uberlândia. *Visiting Student Researcher* na University of Ottawa. Pesquisadora do Laboratório de Direitos Humanos – LabDH. Cofundadora do Núcleo de Traduções do Centro Brasileiro de Estudos em Direito e Religião – Cedire. *E-mail:* lumalaura@gmail.com.

Resumo: Este artigo tem como escopo analisar o tema da vigilância digital e seus desdobramentos em matéria de direitos humanos e fundamentais, a partir da perspectiva da governança da internet, em especial nos contextos do Brasil e da União Europeia, dois atores com destaque em âmbito global nessa

temática. Para tanto, por meio de pesquisa bibliográfica e documental, buscou-se identificar se e como a vigilância impacta na fruição dos direitos fundamentais, discutir o conceito de “constitucionalismo digital” como uma possível resposta aos desafios colocados pela vigilância digital, e realizar uma análise comparativa das especificidades dos modelos de governança do Brasil e da União Europeia. Ao final, conclui-se que, diante dos riscos oferecidos pela intensificação dos processos de vigilância digital, mostra-se imprescindível a adoção de uma abordagem *multistakeholder* para que a governança da internet se coadune com a garantia dos direitos humanos fundamentais e a observância dos princípios do Estado democrático de direito.

Palavras-chave: Governança digital. Governamentalidade algorítmica. Constitucionalismo digital. Proteção de dados. Direitos humanos.

Abstract: The scope of this article is to analyze digital surveillance and its consequences relating to human and fundamental rights, from the perspective of Internet Governance, especially in the context of Brazil and the European Union, two actors with global distinction in this field. Therefore, through bibliographic and documentary research, we sought to identify if and how surveillance impacts the enjoyment of fundamental rights, to discuss the concept of “Digital constitutionalism” as a suitable response to the challenges posed by digital surveillance, and to conduct a comparative analysis concerning the specificities of the Brazilian and the European model of governance. Ultimately, we concluded that, given the risks imposed by the intensification of digital surveillance processes, it is essential to adopt a multistakeholder approach for Internet Governance to be compatible with the guarantees of fundamental human rights and with the observance of the Rule of Law and democracy principles.

Keywords: Digital governance. Algorithmic governmentality. Digital constitutionalism. Data protection. Human rights.

Sumário: **1** Vigilância digital: a técnica econômica e seu governo algorítmico – **2** Constitucionalismo digital: uma resposta à cibervigilância? – **3** Governança da internet: uma resposta pautada no constitucionalismo digital – **4** Considerações finais – Referências

Summary: **1** Digital surveillance: the economic technique and its algorithmic government – **2** Digital constitutionalism. An answer to cybersurveillance? – **3** Internet Governance: a response based on Digital Constitutionalism – **4** Final considerations – References

1 Vigilância digital: a técnica econômica e seu governo algorítmico

A sociedade moderna é o resultado de uma série de transformações sociais que impactaram a ordenação social como um todo, bem como as relações sociais mediadoras do indivíduo. Ela é fruto de uma mudança em seu processo de produção, estruturado historicamente e determinado por meio da experiência e do poder.

O papel do Estado nessa nova dinâmica entre sociedade e tecnologia é o de organizar as forças sociais dominantes para impulsionar o desenvolvimento e a inovação a partir do domínio tecnológico por meio de sua capacidade produtiva. Antoinette Rouvroy e Thomas Berns conceituam a “governamentalidade algorítmica” justamente como a tentativa de clarificar os fenômenos que levaram a essa nova

forma de governo.¹ Rouvroy afirma que a governamentalidade algorítmica traduz-se na hipótese de um governo basear-se no processamento algorítmico de grandes volumes de dados (*big data*) e não em políticas, leis e normas sociais.²

A grande capacidade de armazenamento de dados somente passou a ser possível a partir da Revolução Tecnológica moderna, que permitiu saltos computacionais gigantescos e a evolução exponencial do processamento de dados. Nessa esteira, sua presença, cada vez mais onipresente em toda a sociedade – seja em seu ambiente público, seja no privado – permitiu que a coleta de dados fosse grande o suficiente para que se pudesse vasculhá-los com a intenção de descobrir padrões e ajustar a alocação de recursos apropriadamente.

No entanto, ainda que tais processos contribuam para a maximização da eficiência dos sistemas produtivo e social, o enfoque estritamente em sua otimização apresenta sérios problemas emancipatórios nos processos de tomada de decisão. Isso porque, revestidos de “técnica”, tais mecanismos ignoram não somente o político, como também quantidades de informação qualitativa, a citar-se a cultura, valores morais e informações de cunho individual ou coletivo, que subsidiam a tomada de decisão, são relevantes à construção da noção de justiça, e que, por isso, permanecem cruciais para se alcançar as finalidades e objetivos comuns da sociedade.³

Por isso, a intensificação do uso desses mecanismos algorítmicos, na tentativa de simplificar a complexidade da vida social, pode se converter em um motor de injustiças, sobretudo quando se prescinde de valores e imperativos éticos compartilhados pela comunidade.^{4 5} A moderação automatizada de conteúdo, da forma como é feita pelas plataformas digitais, coloca em risco, por exemplo, a liberdade de expressão, o direito à privacidade, a dignidade da pessoa humana, e o direito

¹ ROUVROY, Antoinette; BERNIS, Thomas. Gouvernamentalité algorithmique et perspectives d'émancipation. *Réseaux*, v. 177, n. 1, p. 163-196, 2013. Disponível em: <http://dx.doi.org/10.3917/res.177.0163>.

² ROUVROY, Antoinette. Entrevista com Antoinette Rouvroy: governamentalidade algorítmica e a morte da política. *Revista de Filosofia Moderna e Contemporânea*, Brasília, v. 8, n. 3, dez. 2020.

³ BERNIS, Thomas; ALMEIDA, Maria Cecília Pedreira de; ALVES, Marco Antonio Sousa. Tornar a revolta impossível. *Revista de Filosofia Moderna e Contemporânea*, v. 8, n. 3, p. 29-37, 31 jan. 2021. Disponível em: <http://dx.doi.org/10.26512/rfmc.v8i3.36260>.

⁴ BARTH, Carlos Henrique. É possível evitar vieses algorítmicos? *Revista de Filosofia Moderna e Contemporânea*, Brasília, v. 8, n. 3, p. 43-44, dez. 2021.

⁵ Tais mecanismos não se interessam pelo indivíduo, mas sim pela quantidade de dados que ele produz. Esses dados são transformados em relações estatísticas, nem sempre interdependentes, e que podem refletir preconceitos sociais, como o racismo. O Colégio Nacional de Defensores Públicos Gerais (Condege) mapeou 58 erros em processos algorítmicos de reconhecimento facial entre junho de 2019 e março de 2020, somente no Rio de Janeiro. Em 80% desses casos, aqueles que foram acusados no inquérito eram negros, sendo que em 86% das ocorrências se decretou a prisão preventiva do suspeito (DEFENSORIA PÚBLICA DO ESTADO DO RIO DE JANEIRO. *Relatório sobre o reconhecimento fotográfico em sede policial*. 2020. Disponível em: <https://www.defensoria.rj.def.br/uploads/arquivos/33e974efa1004184954cc1b08ac2f253.pdf>. Acesso em: 6 abr. 2022).

de acesso à informação, pois ainda que uma das justificativas da implementação de tal funcionalidade seja a entrega de conteúdo personalizado e direcionado aos interesses dos usuários, o uso de filtragem algorítmica implica necessariamente a transformação da internet em um ambiente que oculta conteúdos, limitando o acesso a certas informações.^{6 7}

O recurso à técnica computacional sem a consideração abrangente de aspectos ético-morais resulta em prejuízos à autonomia humana e às relações sociais, problema intensificado pela ascensão da vigilância digital, entendida como o monitoramento de cada atividade presente no ciberespaço, como a coleta de dados armazenados em um disco rígido, ou a transferência de dados e seu compartilhamento por meio virtual.⁸ Os programas de monitoramento de atividade *on-line* não apenas coletam, mas também processam e classificam o conteúdo encontrado nos bancos de dados.

Nesse contexto, a governamentalidade algorítmica reduz a comunidade a um ativo de vigilância⁹ com vistas a manter a estabilidade e perpetuar o contrato, o fim e o meio de um biopoder.¹⁰ Na visão de Edson Teles, esse novo agenciamento confunde sujeito e objeto, a natureza e a cultura, o público e o privado, o humano e

⁶ Na linha de como os mecanismos de navegação estão se configurando, a internet estaria se transformando em um espaço no qual é mostrado o que se acha que é de nosso interesse, mas é ocultado de nós aquilo que desejamos ou eventualmente precisamos ver. Desse modo, pode-se dizer que a *filter bubble* e seu caráter prejudicialmente paternalista pode implicar restrições a direitos e a garantias fundamentais, à autonomia dos indivíduos e à liberdade de expressão, sendo prejudicial de forma geral para o debate na esfera pública conectada (MAGRANI, Eduardo. *Democracia conectada: a internet como ferramenta de engajamento político-democrático*. Curitiba: Juruá, 2014).

⁷ Assim, além de nitidamente macular o direito dos internautas de ter conhecimento de certos conteúdos, tem-se uma limitação excessiva da liberdade de expressão e manifestação, a título de exemplo, rememore-se o caso do Sociólogo e Professor da Universidade Federal do ABC, Sérgio Amadeu, que teve seu vídeo censurado pelo *YouTube*, sob a justificativa de que possuiria “conteúdo perigoso ou depreciativo”, quando na realidade se tratava de material crítico ao *Google*, intitulado “Por que as plataformas declararam guerra ao PL 2630?” (DIAS, Tatiana. *YouTube veta impulsionamento de vídeo crítico ao Google*. *Centro de Estudos da Mídia Alternativa Barão de Itararé*, 2022. Disponível em: <https://baraodeitarare.org.br/site/noticias/comunicacao/youtube-veta-impulsionamento-de-video-critico-ao-google>. Acesso em: 5 abr. 2022).

⁸ LYON, David; ZUREIK, Elia. *Computers, surveillance, and privacy*. Minneapolis: University of Minnesota Press, 1996. p. VII.

⁹ O conceito de ativo de vigilância é entendido pela autora como a combinação entre dados, extração e análise realizada pelo processo de acumulação de dados e informação e capturado a partir de operações automatizadas. Desse modo, tais dados se transformam em ativos, pois atraem investimentos e constroem uma nova forma de mercado chamada pela autora de “capitalismo de informação” que nutre o “capitalismo de vigilância” (ZUBOFF, Shoshana. *Big other: capitalismo de vigilância e perspectivas para uma civilização de informação*. In: BRUNO, Fernanda et al. *Tecnopolíticas da vigilância: perspectivas da margem*. São Paulo: Boitempo, 2018. p. 40-41).

¹⁰ ZUBOFF, Shoshana. *A era do capitalismo de vigilância: a luta por um futuro humano na nova fronteira do poder*. Rio de Janeiro: Intrínseca, 2021.

a máquina, o discursivo e o funcional, ao reduzir a subjetividade a um mero estudo sobre a externalidade das ações individuais, ignorando a coletividade e seus valores.¹¹

A grande base de dados que retroalimenta essa nova forma de governo é comumente chamada de *big data*.¹² Esta somente é possível, pois a extração de dados inaugura um novo capitalismo, o capitalismo de vigilância, que pode ameaçar a liberdade alcançada pelo Estado democrático de direito:¹³

Os capitalistas de vigilância possuem amplos direitos de privacidade e, portanto, muitas oportunidades para segredos. Estes são cada vez mais utilizados para privar as populações de escolha no que diz respeito a que partes de sua vida desejam manter em sigilo. [...] Os capitalistas de vigilância exploraram de forma hábil um lapso na evolução social, uma vez que o rápido desenvolvimento de suas habilidades de vigiar para o lucro em muito suplantou a compreensão pública e o eventual desenvolvimento de leis e regulamentações legais.¹⁴

Não há somente uma acumulação de dados, mas também uma acumulação de direitos,¹⁵ isso porque a lógica que sustenta esse novo capitalismo é a de uma

¹¹ TELES, Edson. Ação política híbrida e a dissolução da cidadania. *Revista de Filosofia Moderna e Contemporânea*, v. 8, n. 3, p. 84, 31 jan. 2021. Disponível em: <http://dx.doi.org/10.26512/rfmc.v8i3.34494>.

¹² Aqui, o termo é utilizado para caracterizar o processo de coleta de dados de indivíduos que é feito a todo o momento pelos diversos aparelhos tecnológicos (relógios, celulares, computadores) e que faz parte da nova lógica de acumulação. Essa coleta massiva intenciona prever o comportamento humano para produzir receitas e controlar o mercado (ZUBOFF, Shoshana. *Big other: capitalismo de vigilância e perspectivas para uma civilização de informação*. In: BRUNO, Fernanda et al. *Tecnopolíticas da vigilância: perspectivas da margem*. São Paulo: Boitempo, 2018. p. 19).

¹³ ZUBOFF, Shoshana. *A era do capitalismo de vigilância: a luta por um futuro humano na nova fronteira do poder*. Rio de Janeiro: Intrínseca, 2021.

¹⁴ ZUBOFF, Shoshana. *Big other: capitalismo de vigilância e perspectivas para uma civilização de informação*. In: BRUNO, Fernanda et al. *Tecnopolíticas da vigilância: perspectivas da margem*. São Paulo: Boitempo, 2018. p. 47-48.

¹⁵ A acumulação de direitos é um fenômeno intrinsecamente relacionado ao caráter comercializável de tais dados, direitos como acesso à informação e privacidade são tidos como produtos rentáveis e que, por assim serem, tornaram-se exemplos claros de tal acumulação. Não é incomum que sites de jornais e revistas *on-line* divulguem manchetes, mas exijam cadastro (fornecimento de dados) e assinatura paga para que os interessados tenham acesso ao conteúdo integral; com igual frequência companhias telefônicas oferecem planos *zero rating*, também denominados de planos com acesso patrocinado, nos quais o acesso a certas plataformas é limitado e não enseja desconto no pacote de internet contratado, prática que privilegia alguns conteúdos em relação a outros, que macula a neutralidade da rede, fragiliza o direito de acesso à informação e facilita a disseminação de *fake news*, por dificultar a verificação da veracidade da informação compartilhada; outra prática recorrente e que representa a acumulação de direitos, no caso, direito à privacidade e à proteção de dados, é a estratégia de captação de informação de clientes empregada por empresas, entre outras, do setor farmacêutico, as quais condicionam a elegibilidade para benefícios e promoções ao fornecimento do número de inscrição junto ao Cadastro de Pessoa Física (CPF), do *e-mail*, do nome completo dos interessados, ou, ainda, de dados biométricos dos clientes, conduta que levou a Secretaria Nacional do Consumidor, órgão vinculado ao Ministério de Justiça e Segurança Pública,

transparência total. Entretanto, a acumulação não é recíproca, mas unilateral com vistas a sustentar as assimetrias do poder dentro de uma infraestrutura global automatizada e institucionalizada. O direito à privacidade é relativizado para manter uma vigilância constante.

Com a expansão cada vez maior da tecnologia e de seu impacto na sociedade, diversas iniciativas, nas últimas duas décadas, ganharam corpo buscando estabelecer limites à acumulação predatória desses dados e proteger os direitos dos cidadãos. Essas iniciativas compõem um leque extremamente variado, que engloba desde declarações em prol da proteção desses direitos, até pronunciamentos oficiais de organizações intergovernamentais e legislações de fato.

Apesar disso, todas essas iniciativas confluem para um mesmo fim, garantir a proteção de um conjunto relativamente abrangente de direitos, princípios e normas de governança digital que tornem o mundo *on-line* compatível com os direitos fundamentais.¹⁶ Essa proteção se mostra ainda mais relevante em um contexto em que a internet se torna cada dia mais indissociável da vida das pessoas. Em janeiro de 2021, constatou-se que cerca de 60% da população mundial utiliza a internet em suas atividades diárias, chegando a 90% na Europa e na América do Norte, sendo que a maioria dos indicadores do Relatório Digital Global, produzido pelo *We Are Social*, mostrou notável aumento neste número nos últimos 12 meses, a exemplo do *e-commerce*, que cresceu consideravelmente como resultado das tentativas de mitigação dos riscos de propagação de Covid-19, e do tempo que os usuário da internet passam conectados diariamente, aproximando-se de 7 horas diárias.¹⁷

Esse aumento cada vez mais crescente no uso da internet e das plataformas digitais demanda reflexão sobre a regulação dos serviços tecnológicos, com impacto na sociedade, para a proteção dos direitos dos cidadãos. É nesse contexto que surge o fenômeno constitucionalismo digital, conforme veremos a seguir.

a notificar grandes empresas do ramo para que prestassem esclarecimentos sobre o tratamento de tais informações (OLIVEIRA, Eliane. Redes de farmácia entram na mira do governo por uso de dados pessoais em programas de descontos. *O Globo*, 2021. Disponível em: <https://oglobo.globo.com/economia/defesa-do-consumidor/redes-de-farmacias-entram-na-mira-do-governo-por-uso-de-dados-pessoais-em-programas-de-descontos-25278675>. Acesso em: 13 maio 2022).

¹⁶ GILL, Lex; REDEKER, Dennis; GASSER, Urs. Towards digital constitutionalism?: mapping attempts to craft an internet bill of rights. *Berkman Klein Center For Internet & Society Research Publication*, Cambridge, v. 15, nov. 2015. p. 2-5.

¹⁷ WE ARE SOCIAL. *Digital 2021: global overview report*. 2021. Disponível em: <https://wearesocial.com/uk/blog/2021/01/digital-2021-uk/>. Acesso em: 27 abr. 2021.

2 Constitucionalismo digital: uma resposta à cibervigilância?

O “constitucionalismo digital” é conceituado como “uma tentativa de conectar as diversas iniciativas que buscam articular uma gama de direitos políticos, normas de governança e definir limites ao exercício do poder na Internet”.¹⁸ Sua configuração espacial-normativa revela sua importância não apenas ao materializar a existência de valores, objetivos e interesses comuns, mas também por se apresentar como resposta às ameaças comuns frequentemente vistas no ambiente digital, entre elas o problema da vigilância.¹⁹

Esse novo marco normativo refere-se a uma série de “novos direitos” e princípios de governança cada vez mais numerosos e que dialogam com a legislação doméstica, os tratados internacionais e as práticas de governança da internet.²⁰ Sua natureza “protoconstitucional”²¹ (não se confundindo com o sentido tradicional do constitucionalismo ou com um documento normativo-estatal que está posicionado no topo de uma ordem jurídica nacional) permite observar ações coordenadas tanto no âmbito local desses países, quanto globalmente.

¹⁸ Os autores ainda defendem que as constituições possuem, como papel fundamental, não apenas estabelecer limites ao poder estatal, mas também criar instituições que permitam ações coletivas e coordenadas (GILL, Lex; REDEKER, Dennis; GASSER, Urs. Towards digital constitutionalism?: mapping attempts to craft an internet bill of rights. *Berkman Klein Center For Internet & Society Research Publication*, Cambridge, v. 15, nov. 2015. p. 2-3).

¹⁹ De acordo com o filósofo Byung-Chul Han: “com o auxílio de técnicas refinadas cria-se a ilusão de uma vigilância permanente. Aqui a transparência se dá apenas unilateralmente. E é nisso que reside sua perspectividade, que dá fundamento à estrutura de poder e domínio. Na aperspectividade, ao contrário, não se estabelece olho central algum, não se dá qualquer subjetividade ou soberania central. Se os presos do panóptico de Bentham têm ciência de estarem constantemente sendo observados por um vigia, ilusoriamente os habitantes do panóptico digital imaginam estar em total liberdade” (HAN, Byung-Chul. *Sociedade da transparência*. Petrópolis: Vozes, 2017. Edição Digital. p. 54).

²⁰ REDEKER, Dennis. Towards a European Constitution for the Internet? *Bremen International Graduate School Of Social Sciences: Comparative Institutionalization and Mobilization in European and Transnational Digital Constitutionalism*, University Of Bremen And Jacobs University Bremen, v. 1, n. 1, p. 1-21, nov. 2019. Disponível em: https://www.giga-net.org/2019symposiumPapers/22_Redeker_Towards-a-European-Constitution.pdf. Acesso em: 31 mar. 2021.

²¹ “It is therefore important to state at the outset that our use of the term ‘constitutional’ is not intended to describe how these documents are situated within a set of legal authorities, nor is it meant to suggest that the documents studied are in fact ‘constitutions’ in the classical legal sense. Rather, the term has been adopted here as a powerful shorthand to capture the common thread which binds a set of otherwise divergent initiatives; that each one seeks to engage with political rights, governance norms, and limitations on the exercise of power on the Internet in some fundamental way. They might turn out to be, in other words, ‘pre-’ or ‘proto-constitutional’ documents in the sense of intellectual building blocks for the constitutional material of the digital sphere, while lacking any preeminent status within a hierarchy of legal rules” (GILL, Lex; REDEKER, Dennis; GASSER, Urs. Towards digital constitutionalism?: mapping attempts to craft an internet bill of rights. *Berkman Klein Center For Internet & Society Research Publication*, Cambridge, v. 15, nov. 2015. p. 3).

O constitucionalismo digital não se limita a proteger o usuário contra eventuais abusos, uma vez que estabelece mecanismos de salvaguarda que asseguram que nenhuma entidade, seja ela da esfera pública, seja privada, esteja acima dos direitos individuais fundamentais das pessoas que utilizam a internet. Iniciativas estruturais relacionadas ao constitucionalismo digital projetam valores e princípios constitucionais para a realização de direitos políticos e até limitam o exercício do poder na internet, seja no âmbito público, seja no âmbito privado.²² Nesse sentido, Edoardo Celeste²³ destaca que declarações que versam sobre direitos fundamentais na internet:²⁴

- (i) reconhecem a existência de novos direitos fundamentais na internet, como o direito de acesso à internet, o direito ao esquecimento ou o direito à neutralidade da rede;
- (ii) limitam a capacidade de violação de direitos fundamentais na rede, como ocorre com as leis de proteção de dados; e, ainda,
- (iii) estabelecem novas formas de controle social sobre as instituições públicas, como o dever de transparência das informações.

No entender de Berman,²⁵ as garantias constitucionais teriam reduzida efetividade na esfera privada do mundo digital, vez que em decorrência da “arquitetura” das plataformas digitais, o poder coercitivo destas se mostra muito mais efetivo do que o da lei.²⁶ Ao tratar da “arquitetura” do mundo digital, Lessig constata que as plataformas são codificadas para serem circunscritas e delimitadas conforme os interesses de quem gere as chamadas *big techs*. Ante tal colocação, se pensarmos na “arquitetura” das plataformas como um elemento influenciador da “lei do ciberespaço” vemos que elas fixam valores e garantem liberdades a depender da vontade daquele que as programou, delegando importância e valor a certos direitos, muitas vezes, em detrimento de outros.²⁷ Ademais, as tecnologias digitais atualmente guiam cada vez mais o processo decisório, tanto no âmbito público, quanto no âmbito privado, a respeito do que observam Filgueiras e Almeida:

²² MENDES, Gilmar Ferreira; FERNANDES, Victor Oliveira. Constitucionalismo digital e jurisdição constitucional: uma agenda de pesquisa para o caso brasileiro. *Revista Brasileira de Direito*, v. 16, n. 1, p. 1-33, jan./abr. 2020. p. 8.

²³ CELESTE, Edoardo. Digital constitutionalism: a new systematic theorisation. *International Review of Law, Computers & Technology*, v. 33, n. 1, p. 76-99, 2 jan. 2019.

²⁴ Para o desenvolvimento do presente estudo, foram objeto de análise: da União Europeia, a Declaração de Princípios de Governança da Internet e o Regulamento Geral de Proteção de Dados, no contexto brasileiro, o Marco Civil da Internet e a Lei Geral de Proteção de Dados, bem como a *Charter for Innovation, Creativity and Access to Knowledge* e o *NETMundial, Multistakeholder Statement* no âmbito internacional.

²⁵ BERMAN, Paul Schiff. Cyberspace and the State Action Debate: the cultural value of applying constitutional norms to private regulation. *University Of Colorado Law Review*, v. 71, p. 1263-1310, 23 maio 2000.

²⁶ SUZOR, Nicolas. Digital constitutionalism: using the rule of law to evaluate the legitimacy of governance by platforms. *Social Media + Society*, v. 4, n. 3, p. 205630511878781, jul. 2018.

²⁷ LESSIG, Lawrence. *Code and other laws of cyberspace*. New York: Basic Books, 1999. p. 20-23.

Por exemplo, plataformas digitais como Amazon, Google, Facebook, Apple, Uber, Twitter, YouTube, Microsoft, e Airbnb, controlam o acesso global à informação, serviços e produtos. Elas desempenham um papel significativo ao determinar os parâmetros de acesso ao mercado e à liberdade de expressão através do uso de algoritmos. O poder e o efeito desses algoritmos não são perceptíveis ou discerníveis para a maioria da população global. Além disso, as decisões do setor público também são cada vez mais ditadas por sistemas algorítmicos de governança. Por exemplo, algoritmos preditivos são usados por Estados para calcular o risco de reincidência criminal de futuros detentos e por meio disso estabelecer sentenças em julgamentos.²⁸

Ao tratarmos as tecnologias digitais como parte de um conjunto comum de recursos, cria-se um leque de possibilidades que podem beneficiar toda a comunidade por meio da expansão e difusão de conexões, conhecimentos, serviços e novas formas de comunicação. Por outro lado, identifica-se o problema não apenas da possibilidade de acumulação quase que infinita de dados e informações, mas também da possibilidade de que os resultados de sua exploração beneficiem apenas certos grupos²⁹ ou que tais resultados destruam os laços sociais da comunidade ante o enaltecimento de diferenças, preconceitos e condutas discriminatórias que ao longo da história se buscam combater.³⁰ Por exemplo, o perigo da concentração do poder acumulado pelas *big techs*, em especial Amazon, Alphabet (Google), Facebook, Twitter, Apple e Microsoft, surge de sua capacidade de controlar a infraestrutura

²⁸ FILGUEIRAS, Fernando; ALMEIDA, Virgílio. *Governance for the digital world: neither more state nor more market*. [s.l.]: Springer International Publishing, 2020. p. 2. Tradução nossa.

²⁹ O sistema tende a beneficiar, por exemplo, indivíduos brancos em detrimento de negros, pois a instrumentalização desta nova lógica é elaborada principalmente com base em estatísticas criminais comuns, uma pseudocorrelação que objetiva categorizar e organizar indivíduos em grupos. Nesse sentido, os critérios de justiça aplicáveis são determinados mensurando o risco de um criminoso e de determinado grupo para a sociedade a partir da atribuição de um valor número a essas características individuais e sociais, e que são comparadas com outras características já disponíveis de diferentes sujeitos já criminalizados (FEELEY, Malcolm; SIMON, Jonathan. *Actuarial justice: the emerging new criminal law*. In: NELKEN, David (Org.). *The futures of criminology*. Londres: Sage, 1994. p. 174).

³⁰ A acumulação massiva de dados, em conjunto com técnicas de *profiling*, permite o direcionamento de conteúdo filtrado e selecionado com base nos interesses e ideais do indivíduo. Tal prática fortalece posições extremistas, amplificando discursos de ódio e a disseminação de *fake news*, bem como restringindo excessivamente a liberdade de expressão. Magrani destaca que “o problema reside, no entanto, no excesso da filtragem, tanto por parte das empresas quanto dos próprios indivíduos que sem ter consciência se limitam se afastando de pontos de vista divergentes dos seus [...] Isto gera por vezes uma dupla falsa impressão: primeiramente por considerar a extensão do debate maior do que efetivamente foi; em segundo lugar, por gerar uma falsa sensação de consenso. Nesta dupla falsa impressão, pode estar o embrião para o extremismo ideológico e nocivo para a esfera pública democrática” (MAGRANI, Eduardo. *Democracia conectada: a internet como ferramenta de engajamento político-democrático*. Curitiba: Juruá, 2014. p. 119-125).

fundamental para o acesso à informação, bem como para a efetivação da liberdade de expressão e direito à privacidade.³¹

Lex Gill *et al.* analisaram um conjunto de iniciativas intraestatais que têm sido encontradas em diversas partes do mundo. No entender dos autores, essas iniciativas geraram documentos legislativos, com fortes características constitucionais. Esses documentos compartilham quatro dimensões que nos permitem visualizar tais características: (i) seu conteúdo substantivo que trata de questões políticas fundamentais, como o reconhecimento de direitos fundamentais na esfera digital e a criação de novos direitos específicos ao mundo digital; (ii) sua pretensão de explorar direitos (coletivos e individuais), estabelecer limites ao poder estatal, bem como ampliar o escopo de normas de governança; (iii) a natureza principiológica destes diplomas, preocupados com sua legitimidade e reconhecimento político pela comunidade; e (iv) seu caráter abrangente, buscando alcançar a totalidade dos sujeitos e atores públicos e privados.³²

Depreende-se, portanto, que os direitos e princípios, que se almejam assegurar também no meio virtual, podem ser divididos em sete grandes grupos: liberdades e direitos básicos; limites gerais ao poder estatal; governança da internet e participação civil; direito à privacidade e vigilância; acesso à internet e educação digital; abertura e estabilidade nas redes; e direitos econômicos e responsabilidade.³³

Tabela 1³⁴

(continua)

Liberdades e direitos básicos
Liberdade de manifestação e de expressão; liberdade de informação; liberdade de religião ou crença; liberdade de associação e de reunião/protesto; direito à segurança pessoal e dignidade; proteção às crianças; não discriminação; diversidade cultural e linguística.
Limites gerais ao poder estatal
Democracia e o Estado democrático de direito; direito ao devido processo legal; acesso à justiça.
Governança da internet e participação civil
Governança participativa e com abordagem <i>multistakeholder</i> ; transparência; dados abertos; direito à participação; inclusão digital.

³¹ FILGUEIRAS, Fernando; ALMEIDA, Virgílio. *Governance for the digital world: neither more state nor more market*. [s.l.]: Springer International Publishing, 2020. p. 2; 17.

³² GILL, Lex; REDEKER, Dennis; GASSER, Urs. Towards digital constitutionalism?: mapping attempts to craft an internet bill of rights. *Berkman Klein Center For Internet & Society Research Publication*, Cambridge, v. 15, nov. 2015. p. 2-3.

³³ GILL, Lex; REDEKER, Dennis; GASSER, Urs. Towards digital constitutionalism?: mapping attempts to craft an internet bill of rights. *Berkman Klein Center For Internet & Society Research Publication*, Cambridge, v. 15, nov. 2015. p. 10-13.

³⁴ GILL, Lex; REDEKER, Dennis; GASSER, Urs. Towards digital constitutionalism?: mapping attempts to craft an internet bill of rights. *Berkman Klein Center For Internet & Society Research Publication*, Cambridge, v. 15, nov. 2015. p. 7-10.

(conclusão)

Direito à privacidade e vigilância
Direito à privacidade; proteção de dados; controle e autodeterminação; direito ao anonimato; proteção contra a vigilância; direito ao uso da criptografia; direito ao esquecimento.
Acesso à internet e educação digital
Direito de acesso; celeridade e acessibilidade; acesso e competências no ambiente de trabalho; conscientização dos usuários e educação; alfabetização digital e midiática.
Abertura e estabilidade das redes
Segurança da rede; neutralidade da rede; padrões abertos; interoperabilidade e não fragmentação; estabilidade e confiabilidade da rede; recursos de <i>softwares</i> abertos e gratuitos; direito ao equipamento.
Direitos econômicos e responsabilidade
Inovação; competitividade; desenvolvimento econômico; propriedade intelectual; responsabilidade dos intermediários; responsabilidade empresarial; proteção ao consumidor.

O cidadão que vive sob o primado do Estado democrático de direito conjectura poder ter a certeza de que será protegido ante manifestações de discriminação, violência, entre outros.³⁵ É por isso que iniciativas em favor do “constitucionalismo digital” podem oferecer contribuições para que os direitos básicos dos cidadãos sejam assegurados também no mundo virtual.

No campo legal, desde o início dos anos 2000, observou-se a criação de diplomas legislativos que consagram uma série de liberdades digitais e direitos – diplomas que podem ser traduzidos como iniciativas que objetivavam limitar o vasto poder até então conferido a atores privados no mundo *on-line*, e que, portanto, corroboraram o solo fértil sobre o qual o constitucionalismo digital se desenvolveu, tendo em vista se inclinarem a um fim comum: ampliar o grau de proteção dos direitos fundamentais no meio digital –, além de uma nova abordagem na tomada de decisões que envolvam aqueles que discutem e controlam o ciberespaço. No contexto da União Europeia, adotou-se a Declaração de Princípios de Governança da Internet e o Regulamento Geral sobre a Proteção de Dados – RGPD; no Brasil, o Marco Civil da Internet e mais recentemente a Lei Geral de Proteção de Dados – LGPD são os instrumentos normativos mais significativos. Todos esses exemplos propõem uma descentralização do poder estatal para definir políticas públicas digitais, dividindo genericamente os atores em: (i) representantes do Estado; (ii) representantes do setor privado; (iii) representantes da sociedade civil; e (iv) representantes das organizações internacionais.

³⁵ TAMANAHA, Brian Z. *On the rule of law: history, politics, theory*. Cambridge: Cambridge University Press, 2004. p. 180.

Além disso, a necessidade de proteção de todos os usuários em todos os países exorta a uma abordagem que seja supranacional. É por isso que existem certas similitudes nos marcos legais existentes, além de respostas próximas, e coletivamente coordenadas. Essa tendência de cooperação resta clara em documentos como *Charter for Innovation, Creativity and Access to Knowledge*, *NETMundial Multistakeholder Statement* e as discussões que anualmente envolvem milhares de pessoas no *Internet Governance Forum* (IGF).³⁶ Mesmo assim, a governança do mundo digital não se dá apenas pela adoção de normas legais. Esse tipo de governança se insere em uma complexa teia de poder, na qual diferentes atores globais definem políticas, e uma complexa rede de normas formais e informais, que organizam diferentes camadas e processos que conectam o uso da tecnologia com a sociedade.³⁷

O mundo digital constitui um viver em risco permanente, ao frequentemente criar novos riscos aos sujeitos individuais,³⁸ abalar as bases institucionais de governos e empresas e ser capaz de gerar catástrofes globais, a exemplo do, não tão distante, escândalo envolvendo a empresa britânica Cambridge Analytica.³⁹ Suas causas e consequências não se limitam a uma localidade, e as crescentes tentativas de incremento da segurança e controle não são suficientes em nosso atual estágio de desenvolvimento. A interdependência global maximiza os riscos, já que há um controle descentralizado e a prevenção de seus efeitos ainda é frágil.⁴⁰

³⁶ GILL, Lex; REDEKER, Dennis; GASSER, Urs. Towards digital constitutionalism?: mapping attempts to craft an internet bill of rights. *Berkman Klein Center For Internet & Society Research Publication*, Cambridge, v. 15, nov. 2015. p. 14.

³⁷ FILGUEIRAS, Fernando; ALMEIDA, Virgílio. *Governance for the digital world: neither more state nor more market*. [s.l.]: Springer International Publishing, 2020. p. 3.

³⁸ Nesse ambiente, potencializam-se as violações de direitos como privacidade e liberdade de expressão, bem como facilita-se a perseguição a movimentos políticos ou a ativistas de direitos humanos, e dissemina-se conteúdo de ódio, de grupos antissemitas, neonazistas, entre outros (MONTEIRO, Artur Pericles Lima; CRUZ, Francisco Brito; SILVEIRA, Juliana Fonteles da; VALENTE, Mariana G. *Armadilhas e caminhos na regulação da moderação de conteúdo: diagnósticos & recomendações*. São Paulo: Internet Lab, 2021. Disponível em: <https://itsrio.org/wp-content/uploads/2021/07/Protecao-de-Dados-e-Transparencia-em-Moderacao-de-Conte%C3%BAdo.pdf>. Acesso em: 4 abr. 2022).

³⁹ A referida empresa britânica valeu-se de dados pessoais identificáveis, de cerca de 87 milhões de usuários do Facebook, com o intuito de influenciar as escolhas eleitorais dos seus titulares ao lhes direcionar vídeos, textos e fotos de candidatos selecionados. Apesar da impossibilidade de se mensurar o impacto do uso de tais dados em nível global, é notório que sua conduta exerceu considerável influência sobre as eleições dos Estados Unidos, o *Brexit* e eleições em países emergentes, como o Quênia, a Nigéria e o México (MONTESANTI, Beatriz. Além dos EUA: como a Cambridge Analytica atuava em eleições pelo mundo. *UOL*, 2018. Disponível em: <https://noticias.uol.com.br/internacional/ultimas-noticias/2018/03/24/como-a-cambridge-analytica-atuava-para-alem-dos-eua.htm>. Acesso em: 10 out. 2021; WONG, Julia Carrie. The Cambridge Analytica scandal changed the world – but it didn't change Facebook. *The Guardian*, 2019. Disponível em: <https://www.theguardian.com/technology/2019/mar/17/the-cambridge-analytica-scandal-changed-the-world-but-it-didnt-change-facebook>. Acesso em: 10 out. 2021).

⁴⁰ FILGUEIRAS, Fernando; ALMEIDA, Virgílio. *Governance for the digital world: neither more state nor more market*. [s.l.]: Springer International Publishing, 2020. p. 62-63.

O constitucionalismo digital, embora não seja um constitucionalismo global no sentido tradicional, constitui-se em um protoconstitucionalismo, que se propõe a enfrentar problemas em níveis globais ainda pouco discutidos, em virtude de um processo decisório comunitário deficiente, seja pela promoção de um ambiente de livre mercado predatório, pela incapacidade das atuais formas de organização social de gerar respostas efetivas aos problemas enfrentados em nível transnacional, ou ainda pela preferência por respostas intraestatais que fragilizam o modelo *multistakeholder* e ignoram a perspectiva de que internet é um bem público global.⁴¹

Essa nova dinâmica decisória se fundamenta na compreensão da comunidade sob uma perspectiva moral, ética e política que enxerga o indivíduo não como mero ativo de vigilância, mas como aquele que possui um papel ativo na construção do bem-público alinhado aos objetivos coletivos globais de defesa dos direitos humanos, em especial, o combate à desigualdade e a promoção da liberdade.

Passaremos agora a analisar as reações intersetoriais a essa nova dinâmica política da modernidade, em especial, as experiências brasileira e europeia.

3 Governança da internet: uma resposta pautada no constitucionalismo digital

3.1 Abordagens locais coordenadas e o constitucionalismo digital

Embora se reconheça a necessidade de definição de normas estatais voltadas à regulação do ambiente digital, a fixação de normas pelo Estado – dadas as características do ambiente digital – não poderá prescindir das relações estabelecidas entre os regimes jurídicos transnacionais que versam sobre o domínio da internet, tampouco ignorar os avanços regulatórios implementados por outros atores, entre os quais estão incluídos os não governamentais. Como se observa, é crescente o protagonismo de órgãos de monitoramento internacionais e de organismos de governança multissetoriais.^{42 43}

⁴¹ O vasto poderio das *big techs* e sua quase ilimitada influência sobre a “arquitetura” do sistema maculam o processo decisório comunitário, por meio de uma tendência à supervalorização da proteção ao livre mercado, fato que, consequentemente, tende a incapacitar a sistemática atual a, de forma ativa, combater abusos originários do âmbito transnacional ou promover o modelo *multistakeholder*.

⁴² MENDES, Gilmar Ferreira; FERNANDES, Victor Oliveira. Constitucionalismo digital e jurisdição constitucional: uma agenda de pesquisa para o caso brasileiro. *Revista Brasileira de Direito*, v. 16, n. 1, p. 1-33, jan./abr. 2020. p. 20-22.

⁴³ Como órgãos de monitoramento de atuação expressiva, faz-se oportuno destacar iniciativas como o “Estamos Vigilando”, promovida pelo Centro pela Justiça e o Direito Internacional – Cejil, em conjunto com o *Open Knowledge Brasil*, a organização não governamental *Derechos Digitales*, a *Fundación para la Libertad de*

Esse novo modelo regulatório, de governança global e multissetorial, implica o afastamento relativamente ao modelo tradicional de regulação, exclusivamente estatal ou centrado no Estado. Por isso que medidas locais de edição de leis para “reterritorializar” o ciberespaço são percebidas por diferentes atores como uma ameaça ao livre mercado, que pode levar a uma fragmentação da rede, distanciando-se de seu particular modo de constituição e funcionamento.

Se, de um lado, há dificuldades ou riscos na regulação local da internet, de outro, a ausência de atuação estatal (democrática e constitucional) pode colocar em risco direitos fundamentais e humanos no âmbito digital.⁴⁴ O ecossistema da internet permite que decisões sejam discutidas e decididas tanto no âmbito local, regional e mundial, de maneira que, se as respostas nacionais levarem em consideração os princípios e direitos básicos já consolidados sob a ótica da governança da internet, sua atuação tão somente vem agregar à efetiva proteção dos direitos fundamentais dos cidadãos, mesmo que em detrimento das *big techs*.

3.1.1 A estratégia brasileira

No contexto brasileiro, o país aprovou dois importantes marcos legislativos, o Marco Civil da Internet (MCI), em 2014, e a Lei Geral de Proteção de Dados (LGPD), em 2018. Ambos os instrumentos normativos, guardadas suas especificidades, tinham como escopo proteger os usuários no ambiente digital, atuando para garantir os direitos consagrados constitucionalmente também no ambiente virtual. Nesse sentido, o MCI estabeleceu princípios, garantias, direitos e deveres para quem faz uso da rede, e delimitou a responsabilização de intermediários por eventuais danos aos usuários. A LGPD, por sua vez, regulou o tratamento de dados, estabelecendo limites, direitos e deveres aos usuários, controladores e responsáveis pelo tratamento de dados.

Prensa (FLIP) e o Instituto de Derechos Humanos de la UCA, os quais atuam na proteção dos direitos digitais no âmbito latino-americano, tendo, inclusive, denunciado à Comissão Interamericana de Direitos Humanos ataques do Estado da Nicarágua e El Salvador contra jornalistas e ativistas de direitos humanos. Ademais, em relação aos organismos de governança multissetorial, as *Dynamic Coalitions* promovidas no âmbito do *Internet Governance Forum* (IGF), são exemplo de tal protagonismo, pois são compostas por *experts* dos setores público e privado, bem como da sociedade civil.

⁴⁴ A esse respeito, a Resolução das Nações Unidas A/HRC/38/L.10/Rev.1, adotada em 4.7.2018 pelo Conselho de Direitos Humanos, afirma que os mesmos direitos que são reconhecidos às pessoas no ambiente *off-line* devem ser protegidos *on-line*, independentemente das fronteiras ou do meio. Além disso, ao mesmo tempo que reconhece a natureza global e aberta da internet como um motor do progresso e desenvolvimento em suas variadas formas, convoca os Estados a adotarem remédios efetivos para combater as violações de direitos humanos no ambiente digital e encoraja os Estados a implementarem as medidas necessárias para assegurar a liberdade e a segurança na internet.

O Marco Civil da Internet, por exemplo, conferiu centralidade a cláusulas gerais de proteção da liberdade de expressão (art. 3º, inc. I), da privacidade (art. 3º inc. II) e da preservação da natureza participativa da rede (art. 3º, inc. VII), de maneira a estabelecer limites à garantia desses direitos tanto em âmbito público quanto em âmbito privado.

Sob uma perspectiva do constitucionalismo digital, mesmo não tendo *status* constitucional, sua aspiração de regular a internet através de uma linguagem constitucional, concentrando-se em princípios amplos que visam proteger os direitos e limitar o poder estatal *on-line*, caracteriza-o como um marco normativo digital de teor constitucional.⁴⁵ Além disso, embora detenha âmbito de proteção próprio, o diploma guarda estreita conexão com outros direitos e princípios de matriz constitucional, assim como com a proteção internacional dos direitos humanos.

No que tange à LGPD, há de se notar que esta incorporou uma série de institutos, princípios e regras do Regulamento Geral de Proteção de Dados da União Europeia (RGPD). É nesse diploma, por exemplo, que se encontram especificados os direitos do titular da proteção de dados – arts. 17 e 18 –, que devem ser aplicados em sintonia com os preceitos constitucionais, bem como com a normativa internacional. Somente depois da adoção e entrada em vigor da LGPD foi que o Brasil veio a reconhecer a proteção de dados como um direito fundamental, também no ambiente digital, por meio da Emenda Constitucional nº 115, promulgada em 10.2.2022, ao incluir no art. 5º da Constituição Federal o inc. LXXIX: “é assegurado, nos termos da lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais”.

Importante registrar, todavia, que o Supremo Tribunal Federal (STF), por meio das ações diretas de inconstitucionalidade (ADIs) nºs 6.387, 6.389, 6.390 e 6.393, já havia reconhecido a matéria como tendo *status* de direito fundamental. Dessa forma, Sarlet ressalta que após a decisão do STF:

Tais atores devem, no âmbito e limites de suas respectivas funções, competências e atribuições, aplicar e concretizar o direito à proteção de dados assegurando-lhe a máxima eficácia e efetividade concreta, tanto na condição de direito subjetivo negativo (não intervenção arbitrária no seu âmbito de proteção), quando por força de sua dimensão

⁴⁵ MONCAU, Luiz Fernando Marrey; ARGUELHES, Diego Werneck. The Marco Civil da Internet and digital constitutionalism. In: FROSIO, Giancarlo. *Oxford Handbook of Online Intermediary Liability*. Oxford: Oxford University Press, 2020. p. 189-213.

objetiva, levando a sério os respectivos deveres de proteção e o critério da proibição de proteção insuficiente.⁴⁶

A decisão ainda se conecta diretamente ao sistema de proteção de direitos humanos das Nações Unidas e à normativa europeia. Isso porque o Comitê da ONU para Direitos Humanos, ao interpretar o alcance do art. 17 do Pacto Internacional de Direitos Civis e Políticos, assim como a própria jurisprudência do Tribunal Europeu de Direitos Humanos (TEDH) e do Tribunal de Justiça da União Europeia (TJUE), há algum tempo têm reconhecido como direito fundamental a proteção de dados.⁴⁷ A respeito do entendimento do Comitê, é importante ressaltar que já em 1988 se reconhecia a proteção de dados como um direito humano. Nos termos do Comentário Geral nº 16 do Comitê de Direitos Humanos:

A coleta e armazenamento de informações pessoais em computadores, bancos de dados e outros dispositivos, seja por autoridades públicas ou por pessoas físicas ou jurídicas, deve ser regulamentada por lei. Medidas efetivas devem ser tomadas pelos Estados para assegurar que as informações relativas à vida privada de uma pessoa não cheguem às mãos de pessoas que não estejam autorizadas por lei para recebê-las, processá-las e usá-las, e nunca devem ser usadas para fins incompatíveis com o Pacto. Para ter a proteção mais eficaz de sua vida privada, todo indivíduo deve ter o direito de verificar, de uma forma inteligível, quais dados pessoais são armazenados em arquivos de dados automáticos e com quais objetivos. Cada indivíduo deve também ser capaz de verificar quais autoridades públicas ou indivíduos ou órgãos privados controlam ou podem controlar seus arquivos. Se tais arquivos contiverem dados pessoais incorretos ou tiverem sido coletados ou processados de maneira contrária às disposições da lei, todo indivíduo deve ter o direito de solicitar retificação ou a eliminação.⁴⁸

Dessa maneira, tais normativas e decisões dialogam justamente com a necessidade de uma resposta adequada aos desafios sociais atuais que exigem

⁴⁶ SARLET, Ingo Wolfgang. Fundamentos constitucionais: o direito fundamental à proteção de dados. In: BIONI, Bruno *et al.* *Tratado de Proteção de Dados Pessoais*. Rio de Janeiro: Forense, 2021. p. 50.

⁴⁷ SARLET, Ingo Wolfgang. Fundamentos constitucionais: o direito fundamental à proteção de dados. In: BIONI, Bruno *et al.* *Tratado de Proteção de Dados Pessoais*. Rio de Janeiro: Forense, 2021. p. 28.

⁴⁸ NÚCLEO DE ESTUDOS INTERNACIONAIS. *Comentários Gerais dos Comitês de Tratados de Direitos Humanos da ONU*. São Paulo: Núcleo de Estudos Internacionais, 2018. Disponível em: <https://www.defensoria.sp.def.br/dpesp/repositorio/0/Comentários%20Gerais%20da%20ONU.pdf>. Acesso em: 15 set. 2021.

a reinterpretação de direitos e garantias fundamentais que restrinjam os abusos tanto do poder público quanto da esfera privada.

O Brasil se destaca no debate sobre a governança da internet, por continuamente participar e sediar conferências e eventos que discutem a regulamentação da internet e as restrições à vigilância. Nesse sentido, em 2007, o Rio de Janeiro sediou o Fórum de Governança da Internet (FGI) das Nações Unidas, e em 2015 foi a vez de João Pessoa fazê-lo, além de que, em 2014, São Paulo sediou a Conferência NetMundial, que tratou da Governança Global da Internet, e que foi vista como uma resposta ao escândalo Snowden.⁴⁹

Ao final deste último, apresentou-se uma Declaração Multissetorial, que abordou questões como a neutralidade da internet e a vigilância em massa, pontos considerados prioritários pela diplomacia brasileira e que já haviam sido tratados pelo MCI, aprovado no mesmo ano; contudo, tal declaração perdeu força e acabou não sendo efetiva.

Todavia, mesmo com dois diplomas robustos voltados à proteção dos usuários brasileiros, o Estado mostrou-se lento em combater as violações cometidas por agentes que coletam, acumulam e tratam dados, de maneira que, mesmo aprovadas desde 2018, as sanções previstas na LGPD somente puderam ser aplicadas após agosto de 2021.⁵⁰ Isso se deu pela pressão de diferentes setores, que ainda não haviam se adequado às novas exigências legais e por entenderem que a normativa poderia reduzir a inovação e gerar altos custos para implementação de políticas de privacidade e *compliance*, em especial diante de limitações de ordem estrutural, pessoal e financeira.⁵¹

Além disso, a nomeação e estruturação da Agência Nacional de Proteção de Dados (ANPD) são recentes, não tendo esta aplicado nenhuma sanção até maio de 2022, o que representa um prejuízo à proteção de dados. Além das sanções terem entrado em vigor somente em agosto de 2021, outro motivo para a falta de aplicação de sanções se dá pela falta de uma resolução para estabelecimento dos

⁴⁹ Para mais informações, ver: VERBLE, Joseph. The NSA and Edward Snowden: surveillance in the 21st century. *Revista SIGCAS Computer and Society*, v. 44, n. 3, p. 14-20, 2014. Disponível em: <https://doi.org/10.1145/2684097.2684101>.

⁵⁰ O retardo da aplicação das disposições sancionatórias da LGPD se deu sob a alegação de que as empresas não teriam tido tempo suficiente para se adaptar à nova lei e que, por isso, sua efetividade estaria ameaçada; consequentemente, o Estado brasileiro prorrogou por três anos a eficácia das disposições que previam sanções. No ano de 2021, com o advento da pandemia de Covid-19, apesar de não efetivado, novo adiamento da vigência das disposições sancionatórias chegou a ser debatido quando da propositura do Projeto de Lei nº 500/21.

⁵¹ MELO, Maria Heloísa Chiaverini de *et al.* Uma análise de conjuntura da Lei Geral de Proteção de Dados Pessoais (LGPD): tramitação, aprovação e vigência. *Revista Humanidades e Inovação*, v. 8, n. 47, 2021.

critérios de dosimetria de sanções e penas, ou seja, de uma norma que estipule critérios e parâmetros na aplicação da LGPD.⁵²

Observa-se que persiste alguma dependência da economia brasileira, visto que não há alternativas nacionais para as *big techs* e suas plataformas, ou seja, Meta (Facebook), Microsoft, Alphabet (Google) e Apple dominam praticamente sozinhas suas respectivas plataformas digitais. No caso da Amazon, há ainda alguma concorrência no setor de vendas *on-line*, mas a vantagem comparativa e o poderio financeiro da Amazon podem liquidar a concorrência em pouco tempo.

No contexto brasileiro, atualmente, há sérias preocupações com relação à liberdade de expressão *on-line*, principalmente porque, por todo o mundo, propostas de moderação de conteúdo vêm ganhando força. Nesse sentido, um dos aspectos mais preocupantes dessas propostas é a moderação de conteúdo feito pelas próprias plataformas digitais, especialmente por aquelas que detêm o maior número de usuários e o poder econômico.

O debate sobre a moderação de conteúdo se dá de maneira conjunta com o crescimento desenfreado de *fake news*, desinformação, campanhas de ódio e discriminação na internet. Aliado a isso, percebe-se que as políticas internas das grandes plataformas digitais são também motivo de preocupação, sobretudo quando há falta de transparência na elaboração e aplicação das políticas de moderação de conteúdo internas, ou quando ocorre interferência indevida na esfera e no debate públicos por parte de grandes atores econômicos.

Além disso, a Declaração Latino-Americana sobre Transparência das Plataformas de Internet salienta que a transparência é “necessária, urgente e obrigatória”:

A exigência de transparência de seus processos de moderação e filtragem de conteúdo, inclusive algorítmica, processos de filtragem, incluindo a transparência algorítmica, se torna uma questão de direitos humanos e de aprofundamento democrático, bem como indispensável para empoderar os usuários frente ao poder de regulamentação privada.⁵³

Nesse contexto, a atuação das plataformas no combate à desinformação pode ser problemática tanto em razão do excesso quanto da insuficiência, situações com

⁵² GUIMARÃES, Arthur. ANPD: Definição de critérios de dosimetria de pena é ‘prioridade zero’. *Jota*, 2022. Disponível em: <https://www.jota.info/coberturas-especiais/protecao-de-dados/anpd-definicao-de-criterios-de-dosimetria-de-pena-e-prioridade-zero-11042022>. Acesso em: 10 maio 2022.

⁵³ TEDIC. *Declaración Latinoamericana sobre Transparencia de las Plataformas de Internet*. 2021. Disponível em: <https://www.tedic.org/declaracion-latinoamericana-sobre-transparencia-de-las-plataformas-de-internet/>. Acesso em: 15 abr. 2022.

o potencial de provocar grandes impactos na efetivação dos direitos humanos. Esses atores privados são, frequentemente, responsáveis pela mediação de conflitos que envolvem direitos fundamentais básicos, e muitas vezes agem antes mesmo do Poder Público ou da Justiça. Assim, as plataformas digitais exercem uma função normativa ao estabelecerem termos de uso de seus serviços.⁵⁴ Elas detêm poder suficiente para julgar e decidir quais conteúdos ofendem os termos de uso de suas plataformas, assim como para determinar a exclusão de determinada pessoa, sem que haja qualquer interferência dos órgãos interestatais.

Além disso, não há soluções desenvolvidas pelo poder público que sejam capazes de enfrentar esses problemas de maneira adequada e suficiente. Atualmente, a imensa maioria, senão todos os computadores dos poderes Executivo, Legislativo e Judiciário do país utilizam os sistemas operacionais da Microsoft⁵⁵ e, considerando a experiência com a pandemia de Covid-19, o Governo federal fez uma parceria com a Cisco, para realização de conferências virtuais, reuniões pelo programa Cisco Webex, em detrimento da plataforma Conferência Web, criação nacional universitária, e que possui propósito similar.⁵⁶

Outra parceria público-privada que evidencia a soberania das *big techs* no Brasil foi aquela feita por ocasião da Copa do Mundo da Fifa em 2014, em que o governo, em colaboração com as empresas IBM, Waze e Moovit, criou centros integrados de comando e controle para questões de segurança e gestão urbana. No chamado “urbanismo inteligente”:

As possibilidades de controle oferecidas pelas TICs e tecnologias inteligentes criam o que pode ser considerado a segunda camada territorial, digitalmente constituída, baseada na apreensão, codificação e gestão de dados e informações. No âmbito dessa camada, informação, fluxo de pessoas e veículos, troca de dados entre máquinas e sistemas inteligentes etc., são codificados e comparados com padrões de comportamento e resultados esperados para produzir métodos de classificação social e espacial e, conseqüentemente, controles de acesso físicos e digitais. Se algo se desvia desses padrões, ações são desencadeadas nesta e também na primeira camada (em

⁵⁴ CELESTE, Edoardo. Terms of service and bills of rights: new mechanisms of constitutionalisation in the social media environment? *International Review of Law, Computers and Technology*, v. 33, n. 2, p. 122-138, 2018.

⁵⁵ PAYÃO, Felipe. Governo Temer vai abandonar software livre para comprar produtos Microsoft. *Tecmundo*, 2016. Disponível em: <https://www.tecmundo.com.br/microsoft/111214-governo-temer-abandonar-software-livre-comprar-produtos-microsoft.htm>. Acesso em: 6 set. 2021.

⁵⁶ WAKKA, Wagner. Cisco fecha acordo com Ministério da Ciência para investimentos em digitalização. *Canaltech*, 2020. Disponível em: <https://canaltech.com.br/governo/cisco-fecha-acordo-com-ministerio-da-ciencia-para-investimentos-em-digitalizacao-165586/>. Acesso em: 6 set. 2021.

uma espécie de controle oficial e soberano do território). Um exemplo óbvio disso é o já mencionado COR,⁵⁷ que coloca o território da cidade do Rio de Janeiro sob controle do ponto de vista da gestão urbana cotidiana.⁵⁸

Dessarte, apesar desses desafios, a abordagem brasileira para o enfrentamento desses problemas vem se destacando por seu progressismo, que se desenvolve em ritmo acelerado. Muito embora o chamado Sul global esteja acostumado a se basear nas experiências americana e europeia, o Brasil tem tomado importantes decisões e discutido a questão à luz de uma abordagem holística e que considera as particularidades estruturais, culturais, políticas e de identidade da governança da internet do país.

O país tem digitalizado sua sociedade e criado metodologias em sua lógica interna da governança da internet, mudando o paradigma histórico de que a evolução da sociedade se dá primeiramente no Norte global.

Desde cedo, o país internalizou a natureza descentralizada da internet em suas instituições de governança, como se observa na composição e funcionamento do CGI.br.⁵⁹ O CGI.br revolucionou a lógica da governança brasileira, desde 1995, propondo políticas e medidas relacionadas à regulamentação da internet, bem como estabelecendo padrões de procedimentos operacionais por meio de uma abordagem *multistakeholder* que garante a presença de representantes não só do governo, mas da sociedade civil e da iniciativa privada em seus processos decisórios.⁶⁰

Assim, o Brasil emerge como um importante ator do Sul global, fato que ficou ainda mais evidente após o encontro NetMundial em 2014. A abordagem brasileira dialoga com o constitucionalismo digital e vem se preocupando cada vez mais com os excessos da vigilância digital e com a efetivação dos direitos fundamentais de seus usuários-cidadãos, fato que ficou ainda mais evidente com o reconhecimento da proteção de dados como um direito fundamental.

⁵⁷ Por “COR” entende-se a abreviação de Centro de Operações do Rio, que foi uma das vertentes do projeto *Smarties Cities* da IBM e teve papel fundamental na vigilância promovida para realização da Copa do Mundo de 2014.

⁵⁸ FIRMINO, Rodrigo José. Securitização, vigilância e territorialização. In: BRUNO, Fernanda *et al.* *Tecnopolíticas da vigilância: perspectivas da margem*. São Paulo: Boitempo, 2018. p. 77.

⁵⁹ GLASER, Hartmut Richard. Internet Governance in Brazil: A multistakeholder approach. *CGI*, 2009. Disponível em: <https://cgi.br/publicacao/internet-governance-in-brazil-a-multistakeholder-approach/>. Acesso em: 31 mar. 2021.

⁶⁰ SEGURADO, Rosemary. The Brazilian civil rights framework for the internet: a pioneering experience in internet governance. *The Internet and Health in Brazil*, p. 27-45, 25 out. 2018.

3.1.2 A estratégia europeia

A Europa tem uma longa tradição que une ambiente democrático, regulamentação efetiva e a garantia dos direitos humanos. Os traumas da 2ª Guerra serviram como uma mudança de paradigma na ordem jurídico-social europeia e o bloco político-econômico foi o primeiro a considerar a proteção de dados como um direito fundamental, primeiro com a adoção de legislações nacionais que surgiram na década de 1970, como a lei sueca de proteção de dados – *Datalagen*, a lei francesa de proteção de dados pessoais de 1978, intitulada *Informatique et Libertés*, e legislações análogas de outros países.⁶¹

No âmbito da União Europeia (UE), há tempos, legitima-se o direito à privacidade como um direito fundamental do cidadão e que se desdobra na proteção não seletiva dos dados pessoais, ou seja, aos seus cidadãos é dada a certeza de que todos os seus dados estão resguardados independentemente do fim ao qual se prestam ou das informações neles contidas.⁶² Desde 1995, com a aprovação da Diretiva 95/46/CE e depois do Regulamento (EU) 2016/679, que sucedeu à Diretiva em 2018, a União Europeia possui diferentes instrumentos e padrões para a proteção de dados singulares, a regulamentação do tratamento desses dados e sua livre circulação.^{63 64}

Como exemplo, destaca-se a já mencionada Declaração de Princípios de Governança da Internet, adotada pelo Comitê de Ministros do Conselho da Europa em 2011, estabelecendo 10 princípios indissociáveis das iniciativas de governança da internet, para que estas assegurem uma abordagem sustentável, focada nos

⁶¹ DONEDA, Danilo. Panorama histórico da proteção de dados pessoais. In: BIONI, Bruno et al. *Tratado de proteção de dados pessoais*. Rio de Janeiro: Forense, 2021. p. 9.

⁶² GOSNELL, Cymone. The General Data Protection Regulation: American compliance overview and the future of the American business. *Journal of Business & Technology Law*, College Park, v. 15, n. 1, p. 165-187, jan. 2019.

⁶³ GUIMARÃES, João Alexandre; MACHADO, Lecio. *Comentários à Lei Geral de Proteção de Dados: Lei 13.709/2018 com alterações da MPV 869/2020*. Rio de Janeiro: Lumen Juris, 2020. p. 5.

⁶⁴ É importante diferenciarmos a Diretiva do Regulamento. A Diretiva se distingue do regulamento, na medida em que vincula os países-membros da União Europeia quanto ao resultado a alcançar, deixando-os a competência quanto à forma e aos meios. Assim os Estados possuem o dever de transpor as diretivas para o direito interno, sendo que os destinatários das diretivas são os Estados-Membros. Em regra, a diretiva não é diretamente aplicável aos indivíduos, uma vez que necessita de transposição para o direito interno, fazendo com que a norma interna e não a norma da União se aplique aos particulares. Contudo o TJUE, verificados certos requisitos, já conferiu efeito direto à algumas diretivas à luz da necessidade de proteger os cidadãos contra a inércia estatal. Os regulamentos possuem caráter geral, pelo qual se dirigem a todos os sujeitos de direito que se encontrem no âmbito de sua aplicação, sendo obrigatório em todos os seus elementos e diretamente aplicável, não sendo necessário que os Estados-Membros o recepcionem em seus ordenamentos jurídicos internos (BORCHARDT, Klaus-Dieter. *O ABC do direito da União Europeia*. Luxemburgo: Serviço das Publicações da União Europeia, 2011. p. 94-97).

usuários e baseada em direitos. Esses princípios saúdam os direitos humanos, as liberdades fundamentais, a democracia e o Estado de direito.⁶⁵

Por meio da Declaração, o Comitê dos Ministros não apenas orienta que os Estados-Membros se atentem a esses princípios quando da formulação de sua política interna e externa em assuntos que envolvem a internet, mas encoraja outras entidades, ainda que não governamentais, que façam o mesmo.⁶⁶ Ademais, a Declaração expressa a importância de se adotar uma abordagem condizente com a ótica *multistakeholder*, estimulando a participação plena de governos, setor privado, sociedade civil, comunidade técnica e dos próprios usuários, a fim de preservar tanto a integridade e o funcionamento da rede, quanto a confiança dos usuários.⁶⁷

Nos últimos anos, após escândalos que envolveram a Cambridge Analytica e o caso Snowden, o debate a respeito dos riscos potenciais da vigilância, do uso de *big data* e da inteligência artificial exigiram que a União Europeia reforçasse sua atuação nos campos da privacidade e da proteção de dados. Tais esforços existem a partir de uma lógica de constitucionalismo digital com uma pretensão de ser geral e não se limitar aos cidadãos europeus,⁶⁸ isso porque essas demandas não são somente culturais ou restritas à uma localidade, mas, sim, universais, sendo necessária uma integração de normativas convergentes nessa matéria.⁶⁹

A esse respeito, pode-se destacar a complementaridade das competências dos Estados-Membros e da União Europeia para a regulação de matérias associadas aos direitos fundamentais, políticas econômicas e funcionamento da rede, o que pode ser também percebido à luz de um constitucionalismo multinível, conforme proposto por Ingolf Pernice. Para o autor, a política institucional da União Europeia se reparte entre as instituições nacionais e as instituições comuns supranacionais e, embora a União não deva ser considerada uma superestrutura estatal, é possível perceber sua formação a partir de camadas interdependentes e complementares. Seu constitucionalismo multinível possui cinco elementos principais:

⁶⁵ COUNCIL OF EUROPE. *Declaration by the Committee of Ministers on Internet governance principles*. 2011. Disponível em: https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=09000016805cc2f6. Acesso em: 11 maio 2021.

⁶⁶ COUNCIL OF EUROPE. *Declaration by the Committee of Ministers on Internet governance principles*. 2011. Disponível em: https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=09000016805cc2f6. Acesso em: 11 maio 2021.

⁶⁷ COUNCIL OF EUROPE. *Declaration by the Committee of Ministers on Internet governance principles*. 2011. Disponível em: https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=09000016805cc2f6. Acesso em: 11 maio 2021.

⁶⁸ GILL, Lex; REDEKER, Dennis; GASSER, Urs. Towards digital constitutionalism?: mapping attempts to craft an internet bill of rights. *Berkman Klein Center For Internet & Society Research Publication*, Cambridge, v. 15, nov. 2015. p. 6.

⁶⁹ DONEDA, Danilo. Panorama histórico da proteção de dados pessoais. In: BIONI, Bruno et al. *Tratado de proteção de dados pessoais*. Rio de Janeiro: Forense, 2021. p. 10.

(a) o conceito pós-nacional de constituição; (b) o processo constituinte europeu como processo conduzido pelos cidadãos; (c) a Constituição da União Europeia e as Constituições Nacionais; (d) as múltiplas identidades dos cidadãos da União Europeia; e (e) a União Europeia como a União de cidadãos europeus.⁷⁰

Pernice ressalta que o constitucionalismo multinível permite afirmar que a relação entre as constituições nacionais e o direito primário da União Europeia transforma o sistema da União em um sistema constitucional composto.⁷¹ Assim, o autor pressupõe que a vontade dos cidadãos europeus – dos quais emana o poder para celebração dos tratados – gera a legitimidade da União Europeia. A representação dos cidadãos nas esferas das instituições europeias permite definir um objetivo comum que muitas vezes não pode ser conquistado por um Estado atuando só e que confere importância ao princípio da subsidiariedade, base estrutural da democracia dentro da União.⁷²

No contexto digital, Pernice ressalta:

Iniciativas europeias, tais como a Agenda Digital para a Europa e a estratégia para o Mercado Único Digital Europeu [...], preveem passos importantes para alcançar esse objetivo. A legislação da UE sobre proteção de dados, assim como a estratégia da UE para cibersegurança e a criação da Agência da UE para segurança das redes e da informação mostram como estas questões são levadas a sério. Perspectivas mais concretas e propostas para aumentar a legitimidade democrática da UE através da Internet são desejadas. Se for evidente que elas incentivam a transparência, a participação democrática e responsabilização quando necessário, em particular dentro dos domínios econômicos europeu, fiscal e de políticas sociais, elas poderão também servir como um incentivo, além da economia, para a implementação mais rápida de condições que empoderem os cidadãos, desenvolvendo todo seu potencial com o fim de tomar o controle dos poderes da União, por meio da Internet. Entretanto, nós precisamos ter em mente que o acesso à Internet é um assunto com

⁷⁰ LINS, Ricardo Galvão de Sousa; MOREIRA, Thiago Oliveira; GURGEL, Yara Maria Pereira. O constitucionalismo multinível de Ingolf Pernice: uma análise de pontos e contrapontos. *Cadernos de Direito Actual*, n. 15, p. 186-203, jun. 2021. p. 192.

⁷¹ PERNICE, Ingolf. EU Democratic Legitimacy and Multilevel Constitutionalism in the Digital Age. Conference “European Economic Governance and The Future of European Democracy”. *European Constitutional Law Network (Ecln)*, Berlin, v. 1, n. 1, ago. 2015. p. 3.

⁷² PERNICE, Ingolf. EU Democratic Legitimacy and Multilevel Constitutionalism in the Digital Age. Conference “European Economic Governance and The Future of European Democracy”. *European Constitutional Law Network (Ecln)*, Berlin, v. 1, n. 1, ago. 2015.

diversas complexidades. O progresso a nível Europeu pode ampliar a desigualdade digital em relação a outros países que sofrem com o *quasi* monopólio dos provedores de serviços de tecnologia, informação e comunicação que buscam prender os países em desenvolvimento através de uma nova forma de dependência com o Ocidente.⁷³

Dessa forma, pode-se dizer que o constitucionalismo digital também incorpora elementos oriundos dos diferentes níveis constitucionais da Europa.⁷⁴

Quando da Diretiva de 1995, o legislador já se preocupava em assegurar aos indivíduos o controle sobre suas informações pessoais. Assim, a Diretiva adjetivou o consentimento, qualificando-o como “devendo ser livre, informado, inequívoco, explícito e/ou específico”,⁷⁵ em resposta aos problemas de controle “pouco efetivo das informações pessoais por parte do seu titular”.⁷⁶

Tal marco regulatório de proteção de dados teve como paradigma a integração com o mercado a partir de uma lógica de proteção aos direitos fundamentais estabelecidos no art. 8º da Carta de Direitos Fundamentais da UE e em legislações comunitárias derivadas. A abordagem europeia se dá não somente a partir de uma forte proteção ao direito fundamental à privacidade, mas também com uma visão mais ampla de proteção de dados como direito fundamental independente à privacidade, e assume a presunção de que os Estados têm papel ativo na proteção dos direitos individuais de seus cidadãos.⁷⁷

⁷³ PERNICE, Ingolf. EU Democratic Legitimacy and Multilevel Constitutionalism in the Digital Age. Conference “European Economic Governance and The Future of European Democracy”. *European Constitutional Law Network (Ecln)*, Berlin, v. 1, n. 1, ago. 2015. p. 5. Tradução nossa.

⁷⁴ Ao comentar o constitucionalismo digital no contexto europeu, Giovanni de Gregorio salienta que o fenômeno da constitucionalização das esferas privadas globais dentro da sociedade algorítmica não deve ser encarado como isolado, mas como parte do processo de globalização. Nesse sentido, nota-se que os diferentes sistemas jurídicos ainda buscam entender como fazer parte desse novo fenômeno, especialmente porque, com a internet, os sistemas jurídicos tentam expandir o efeito de suas decisões a uma escala global. O autor ressalta que “conjuntos normativos supranacionais e internacionais, como no caso da consolidação do constitucionalismo multinível na experiência europeia, ou a constitucionalização do direito internacional, levam à emancipação dos valores constitucionais a partir de suas raízes locais para um caráter mais global, onde os sistemas constitucionais se encontram cada vez mais em um processo de hibridização global. Nesse quadro, a ascensão da Internet não apenas desafiou os tradicionais princípios westfalianos de soberania e território, como no caso da política monetária, ou sublinhou tensões globais e locais. Essa situação já ficou clara como resultado do caso Licra vs. Yahoo e no debate seguinte sobre a jurisdição da Internet. A consolidação da Internet também levou a questionar a relação entre liberdades e poder na era digital” (GREGORIO, Giovanni de. *Digital constitutionalism in Europe: reframing rights and powers in the algorithmic society*. Cambridge: Cambridge University Press, 2022. p. 10-11).

⁷⁵ BIONI, Bruno. *Proteção de dados pessoais: a função e os limites do consentimento*. Rio de Janeiro: Forense, 2019. p. 161.

⁷⁶ BIONI, Bruno. *Proteção de dados pessoais: a função e os limites do consentimento*. Rio de Janeiro: Forense, 2019.

⁷⁷ MOLNAR-GABOR, Fruzsina. Data protection. In: GROTE, Rainer; LACHENMANN, Frauke; WOLFRUM, Rüdiger. *Max Planck Encyclopedia of Comparative Constitutional Law*. Oxford: Oxford University Press, 2016. p. 8-9. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2883707. Acesso em: 3 abr. 2021.

Nessa esteira, notável é a construção do direito ao esquecimento, primeiro em sede jurisprudencial, depois dentro da normativa, RGPD. Isso, pois a Agência Espanhola de Proteção de Dados, em 2014, entendeu que nem toda informação é digna de imortalidade, ou seja, que algumas deveriam ser esquecidas, “porque isso é apenas humano”. Sobre esse tema, Zuboff ressalta:

A decisão da Corte de Justiça, reduzida com tanta frequência às considerações técnicas e jurídicas relacionadas a deletar ou suprimir os *links* de dados pessoais, foi na verdade um ponto de inflexão fundamental no qual a democracia começou a se agarrar ao direito ao tempo futuro, tirando-o das poderosas forças de um capitalismo de vigilância determinado a reivindicar autoridade unilateral sobre o futuro digital. Em vez disso, a análise da corte reivindicava o futuro para o modo humano, rejeitando a inevitabilidade da tecnologia do mecanismo de busca do Google e, em seu lugar, reconhecendo que os resultados de buscas são produtos contingentes do interesse econômico específico que guia a ação de dentro das entranhas da máquina: “O operador de um mecanismo de busca está sujeito a afetar de modo significativo os direitos fundamentais à privacidade e à proteção de dados pessoais. Diante da potencial seriedade da interferência” com esses interesses, “ela não pode ser justificada meramente pelo interesse econômico que o operador de tal mecanismo tem nesse processo”.⁷⁸

O caso é paradigmático, primeiramente porque se desdobra na conclusão de que as normas em análise se aplicariam ao Google, ao qual é reconhecida a qualidade de processador e controlador de dados, mas também, e em especial, porque o problema em julgamento é decorrência da crescente digitalização e informatização de várias esferas da vida cotidiana. Julia Powles destaca que, apesar da importância da decisão, há uma série de questões a serem consideradas em relação ao escopo do direito que fora reconhecido, entre elas, como saber quando uma informação não preenche mais os critérios estabelecidos e quem deve fazer esse julgamento.⁷⁹

⁷⁸ ZUBOFF, Shoshana. Big other: capitalismo de vigilância e perspectivas para uma civilização de informação. In: BRUNO, Fernanda et al. *Tecnopolíticas da vigilância: perspectivas da margem*. São Paulo: Boitempo, 2018. p. 80.

⁷⁹ POWLES, Julia. The case that won't be forgotten. *Loyola University Chicago Law Journal*, Chicago, v. 47, n. 2, p. 583-615, 2015.

Além disso, apesar dos grandes avanços já alcançados no que tange à proteção dos direitos dos indivíduos, a autora afirma que a excessivamente rápida implementação da decisão pelo Google influenciou diretamente seu alcance e desdobramentos, pois o Google, além de ditar os limites dessa implementação em seu próprio favor, criou um precedente para outras empresas seguirem.

Powles apresenta cinco aspectos da abordagem adotada pelo Google que limitaram a implementação da decisão em favor da multinacional: i) o formulário desenvolvido para o envio de pedidos similares àquele julgado pelo Tribunal comportava, inicialmente, apenas solicitações relacionadas a informações irrelevantes, desatualizadas ou questionáveis, não alcançando aquelas consideradas incorretas, inadequadas, ou cujo tratamento é excessivo, nos termos da lei; ii) segundo a interpretação dada pelo Google à decisão, a obrigação que lhe era imposta estaria satisfeita com simples notificação *post hoc* aos pedidos por ele entendidos como válidos; iii) a proibição ao tratamento de dados sensíveis não foi sequer levada em consideração; iv) a interpretação dada pelo Google limitou o alcance da decisão apenas aos domínios europeus da empresa; v) os editores originais dos *links* “deslistados” eram notificados apenas se esses utilizassem a ferramenta *webmaster* do Google, e ainda, para eles, a notificação não trazia grandes esclarecimentos.

O RGPD cristalizou o direito ao esquecimento em seu texto no art. 17 ao conferir aos titulares de dados pessoais o direito de solicitar a eliminação de seus dados, elaborando uma série de requisitos para que tal eliminação ocorra. Todavia, ainda há dificuldades na implementação do direito ao esquecimento por meio da desindexação, e as críticas elaboradas por Julia Powles seguem válidas.

Assim, como exemplos de direitos substantivos e processuais, têm-se a necessidade do consentimento expresso para o uso e o tratamento de dados pessoais, a notificação dos usuários quando há algum tipo de vazamento de dados, a proibição de tornar pública informação pessoal, o direito ao apagamento de dados, o direito ao esquecimento, além de restrições contra decisões tomadas por sistemas automatizados e multas para violações ao regulamento, que podem chegar a 4% da receita global da empresa.

Dessarte, sua existência no plano jurídico não significa que a lei impactará positivamente a sociedade. Ela projeta a “possibilidade de empoderamento democrático”, mas que só é observada no plano do real quando os cidadãos contestam as injustiças ou as ilegalidades ocorridas. Assim, a atuação dos cidadãos com o objetivo de invocar a lei para defender os seus direitos é essencial para o sucesso da regulação.⁸⁰

⁸⁰ ZUBOFF, Shoshana. Big other: capitalismo de vigilância e perspectivas para uma civilização de informação. In: BRUNO, Fernanda et al. *Tecnopolíticas da vigilância: perspectivas da margem*. São Paulo: Boitempo, 2018. p. 572.

Esse empoderamento e ação dos cidadãos é pungente na União Europeia. Por exemplo, as cidades de Barcelona e Amsterdã, por meio do projeto Decode, financiado pela União Europeia, vem implementando uma infraestrutura descentralizada de dados que intenta devolver a propriedade o controle de dados e informações aos seus cidadãos, oferecendo:

[...] soluções de gerenciamento de dados e de Internet das Coisas, flexíveis e atentas à privacidade e, ao mesmo tempo, protegendo o direito à privacidade. Baseada na tecnologia de *blockchain*, essa infraestrutura será construída com a participação ativa dos cidadãos, empreendedores sociais, hackers e especialistas em privacidade.⁸¹

Além disso, desde 2012, a Agenda Digital elaborada pela Comissão Europeia recomendou a implementação de padrões abertos dentro de instituições governamentais, a fim de diminuir sua dependência dos proprietários dos *softwares* e dos fornecedores de tecnologia. Essas alternativas se baseiam na noção de que “serviços públicos devem ser desenvolvidos para priorizar o cidadão de forma flexível e interativa, oferecendo serviços melhores em resposta a suas necessidades”.⁸² Isso significa que incorporar padrões abertos fomenta a melhora na qualidade, bem como custos mais baixos e o estabelecimento de programas colaborativos por meio de parcerias para a inovação.

Nesse sentido, a adoção de governança coletiva de dados e práticas colaborativas serve como uma alternativa ao capitalismo de vigilância, ao promover cada vez mais uma soberania tecnológica e uma articulação de uma infraestrutura compartilhada que permite construir bases de dados comuns sem que se caia em uma fragmentação da internet.

O paradigma europeu vem migrando de uma lógica de lucros para uma lógica que tem como objetivo a utilização de tecnologia com objetivo de otimizar o uso de recursos sob a ótica do interesse social e coletivo. Um exemplo importante nesta senda é a Carta de Direitos Fundamentais da União Europeia proposta por intelectuais alemães, políticos, acadêmicos, jornais e representantes de diferentes indústrias.⁸³ A proposta da Carta é impulsionar o diálogo entre os cidadãos, a inicia-

⁸¹ MOROZOV, Evgeny; BRIA, Francesca. O direito à cidade digital: rumo à soberania tecnológica. *In: MOROZOV, Evgeny; BRIA, Francesca. A cidade inteligente: tecnologias urbanas e democracia*. São Paulo: Ubu Editora, 2019. p. 110.

⁸² MOROZOV, Evgeny; BRIA, Francesca. O direito à cidade digital: rumo à soberania tecnológica. *In: MOROZOV, Evgeny; BRIA, Francesca. A cidade inteligente: tecnologias urbanas e democracia*. São Paulo: Ubu Editora, 2019. p. 122.

⁸³ REDEKER, Dennis. Towards a European Constitution for the Internet? *Bremen International Graduate School Of Social Sciences: Comparative Institutionalization and Mobilization in European and Transnational Digital*

tiva privada e os políticos de modo a criar uma mobilização e conscientização em torno da temática, em especial para aqueles que são responsáveis pela formulação de políticas públicas.

Todas essas iniciativas somadas demonstram um alto grau de institucionalização e mobilização em torno da temática da proteção dos direitos aos dados pessoais. Isso porque as cidades, as nações e a própria União Europeia vêm se organizando e reconhecendo que os dados se constituem como um ponto central das relações sociais na contemporaneidade.

Dessa maneira, a abordagem europeia tem se revelado efetiva, pois impõe restrições à extração desses ativos de vigilância, a partir de um regime de dados alternativos que combina uma infraestrutura comunitária, colaborativa e orientada para a persecução de um objetivo comum.

As *big techs* americanas têm sido levadas a se adequar à lógica da proteção de dados para adentrar o poderoso mercado europeu. Padrões éticos e princípios legais convergem na estruturação de garantias necessárias que impedem a consolidação de uma forma de controle social, político ou institucional decorrente do fenômeno da hipervigilância.

A ideia de uma governança coletiva de dados (*data commons*) vem sendo implementada no continente europeu. Dessa maneira, os dados pessoais passam a ser pensados como um recurso coletivo. Entretanto, o Prêmio Nobel de Economia, Elinor Ostrom, ressalta:

a constituição de regras de governança de recursos comuns é mais problemática em grandes grupos e pode ser dificultada quando não há delimitação precisa sobre a natureza do recurso e as possibilidades de limitação de acesso, o que é justamente o caso de dados pessoais, recursos não rivais que podem ser facilmente duplicados e reutilizados.⁸⁴

A UE vem contornando precisamente essas dificuldades a partir de uma estratégia de “infraestrutura espacial comum”, bem como diplomas legislativos robustos e uma política aberta em contraponto ao processo de acumulação predatória de dados por agentes econômicos. A regulamentação do uso de dados se dá a partir de políticas transparentes do uso dos dados, sua origem, sua utilidade e seu destino.

Constitutionalism, University Of Bremen And Jacobs University Bremen, v. 1, n. 1, p. 1-21, nov. 2019. p. 16. Disponível em: https://www.giga-net.org/2019symposiumPapers/22_Redeker_Towards-a-European-Constitution.pdf. Acesso em: 31 mar. 2021.

⁸⁴ ZANATTA, Rafael A. F. Prefácio. In: MOROZOV, Evgeny; BRIA, Francesca. *A cidade inteligente: tecnologias urbanas e democracia*. São Paulo: Ubu Editora, 2019. p. 10.

Desde a década de 1970, tribunais dos Estados-Membros vêm reconhecendo o direito à autodeterminação informativa e a proteção dos dados pessoais, bem como suas instituições políticas vêm promovendo fortes campanhas de maneira a conscientizar e internalizar a importância desses direitos em meio a comunidade.

Há, no contexto europeu, uma forte orientação por um constitucionalismo digital, primeiro, pois desde 2000, o direito à proteção de dados ganhou a condição de direito fundamental de natureza autônoma na Carta de Direitos Fundamentais da União Europeia. Segundo, pois reconhecido seu caráter polivalente (direito negativo e positivo), sua incidência passou a ser multinível e multissetorial, sendo imperioso notar que esse direito passou a existir no plano fático da vida social, ultrapassando a existência nos Tribunais.

Assim, as cidades europeias vêm transformando a realidade social e implementando políticas para digitalização de sua atividade, de modo a diminuir sua dependência das *big techs*, tendência ainda não vista, de forma tão significativa, no Brasil.

Por fim, esses padrões de proteção do cidadão, que dialogam diretamente com o princípio da dignidade da pessoa humana, são exatamente aqueles comumente vistos nas Constituições nacionais. Outrossim, cresce no continente europeu a ideia de que a lógica da proteção dos dados pessoais deve ser expandida por todo o mundo, tendo em vista a sociedade globalizada em que vivemos e como a economia mundial é amplamente conectada, o tratamento de dados, portanto, acaba acontecendo em várias partes do mundo. A União Europeia entende que, para que a proteção de seus cidadãos seja efetiva, é imperativo que haja uma proteção sólida dos direitos à autodeterminação informativa e à proteção de dados em outros lugares além da sua jurisdição.

3.2 A internet como *common global*

O principal ativo desse novo capitalismo digital é a informação. Quem a controla influencia a tomada de decisões globalmente e detém a capacidade de estabelecer novas estruturas de poder.⁸⁵ Dessa forma, a maneira mais adequada de governar o mundo digital está associada à capacidade de enxergarmos seus problemas (desinformação, vieses algorítmicos, extremismo, vigilância) como problemas comuns a todos os países e que as respostas a esses problemas demandam soluções que são construídas e implementadas coletivamente, em diferentes níveis e por diferentes setores.

⁸⁵ FILGUEIRAS, Fernando; ALMEIDA, Virgílio. *Governance for the digital world: neither more state nor more market*. [s.l.]: Springer International Publishing, 2020. p. 13.

Todavia, mesmo que o ecossistema da internet possua em sua base uma grande quantidade de conhecimento e informação, tais bens podem funcionar como contrapostos e seu uso e consumo podem excluir outros indivíduos ou reduzir seus direitos como cidadãos. Filgueiras e Almeida ressaltam:

[A] rivalidade de bens no mundo digital não é intuitiva. Nós estamos lidando essencialmente com bens intangíveis relacionados ao conhecimento. O consumo desses recursos sem uma estrutura de governança pode produzir consequências compartilhadas por todos os cidadãos. Por exemplo, a produção da desinformação por grupos nas mídias sociais contamina o nosso entorno, e cria tensões, polarização, incerteza e racismo. A desinformação é lucrativa nas mídias sociais, e cria barreiras para o acesso da sociedade ao conhecimento.⁸⁶

Tanto a informação quanto o conhecimento são recursos compartilhados dentro de um complexo ecossistema sujeito a dilemas sociais.⁸⁷ Atualmente, existem comportamentos e problemas vistos dentro do mundo digital, como problemas com servidores (que interrompem o funcionamento de um aplicativo em todos os lugares do mundo ao mesmo tempo), *spams*, e desinformação, semelhantes a dilemas associados a outros tipos de bens comuns. Os custos que envolvem fenômenos como ciberataques ou desinformação são pagos por toda a sociedade. Nesse contexto, o desafio é pensar como os “pontos comuns” do mundo digital devem ser governados, para que toda a sociedade seja beneficiada e esses custos, reduzidos.⁸⁸

Nessa perspectiva, uma abordagem sob uma ótica dos *commons* digitais é útil, pois oferece uma compreensão holística do motivo pelo qual os recursos digitais propensos à exploração devem ser governados de maneira coletiva. Quando indivíduos e empresas atuam de forma independente e sem coordenação, agindo de acordo com seus próprios interesses, a exploração pode afetar direitos fundamentais, incluindo-se liberdades, direitos políticos e direitos culturais de outros sujeitos, de maneira muito mais direta e intensa. Interesses individuais que sejam desprovidos de qualquer leitura comunitária contradizem os melhores interesses da comunidade, pois extraem todo o possível desses recursos para interesse próprio ou com o intento de se aumentar seus lucros.

⁸⁶ FILGUEIRAS, Fernando; ALMEIDA, Virgílio. *Governance for the digital world: neither more state nor more market*. [s.l.]: Springer International Publishing, 2020. p. 14. Tradução nossa.

⁸⁷ HESS, Charlotte; OSTROM, Elinor. *Understanding knowledge as a commons: from theory to practice*. Cambridge: The MIT Press, 2007.

⁸⁸ FILGUEIRAS, Fernando; ALMEIDA, Virgílio. *Governance for the digital world: neither more state nor more market*. [s.l.]: Springer International Publishing, 2020. p. 15.

Por esse motivo, uma abordagem que implemente um processo decisório coletivo e multissetorial beneficia toda a comunidade em termos de expansão e difusão de conexões, conhecimentos, serviços e novas formas de comunicação.⁸⁹ Tal construção coletiva, quando aplicada em um ecossistema não somente global, mas também regional e local, é capaz de oferecer grandes avanços na persecução de direitos dos usuários-cidadãos, pois a construção respeita o fato de uma comunidade existir na forma de práticas sociais comuns, tradições culturais e valores socialmente compartilhados.

Filgueiras e Almeida acertadamente defendem:

[O] problema não é a própria extração desse *common*, mas a possibilidade de que os resultados de sua exploração beneficiem apenas alguns grupos ou destruam os laços sociais da comunidade. Os recursos comuns não se esgotam necessariamente, mas podem ser apropriados com facilidade por indivíduos ou grupos para uso puramente privado. A título de exemplo, vemos o perigo da concentração de poder acumulado por Amazon, Google, Facebook, Twitter, Apple e Microsoft que surge através da sua capacidade de controlar a infraestrutura fundacional de nossa vida econômica, informativa e política.⁹⁰

No Brasil, o enfrentamento dos desafios do mundo digital tem sido feito de modo comunitário, participativo e *multistakeholder*. A posição brasileira no contexto internacional sempre foi pautada por esse ideal, fato que pode ser claramente visto na Declaração Multissetorial do Encontro NetMundial, que trouxe a defesa de uma internet unificada e vista a partir do paradigma dos chamados *commons*:

A segurança, estabilidade e resiliência da Internet deve ser um objetivo fundamental de todas as partes interessadas na governança da Internet. Como um recurso global universal, a Internet deve ser um, estável, rede resistente, seguro e confiável seguro. Eficácia na abordagem dos riscos e ameaças à segurança e estabilidade da Internet depende de uma forte cooperação entre os diferentes intervenientes.⁹¹

⁸⁹ FILGUEIRAS, Fernando; ALMEIDA, Virgílio. *Governance for the digital world: neither more state nor more market*. [s.l.]: Springer International Publishing, 2020. p. 17.

⁹⁰ FILGUEIRAS, Fernando; ALMEIDA, Virgílio. *Governance for the digital world: neither more state nor more market*. [s.l.]: Springer International Publishing, 2020. p. 17. Tradução nossa.

⁹¹ COMITÊ GESTOR DA INTERNET NO BRASIL – CGI.BR. *Declaração Multissetorial de São Paulo*: NetMundial. São Paulo: Global Multistakeholder Meeting on the Future of Internet Governance, 2014. Disponível em: https://www.cgi.br/media/docs/publicacoes/4/Documento_NETmundial_pt.pdf. Acesso em: 2 abr. 2021.

Esse ambiente digital multissetorial propiciou ao país ser um dos países mais ativos dentro da política digital global. Na sequência das revelações de Edward Snowden, a então presidente Dilma Rousseff defendeu que “[as] Nações Unidas devem desempenhar um papel de liderança para regular a conduta dos Estados com relação a essas tecnologias”.⁹² A organização do NetMundial reforçou essa postura multissetorial, muito embora esta não tenha obtido êxito, em virtude da falta de apoio de países que geralmente se alinham com as ideias brasileiras, como a Índia e a Rússia.

Além disso, desde a criação do CGI.br, o país se destaca como modelo na gestão de domínios, muito devido ao enorme sucesso advindo de sua abordagem multissetorial aberta, não somente em relação às autoridades governamentais, como também ao setor empresarial e a sociedade civil. O Brasil gradualmente estendeu esse modelo a várias áreas da governança da internet, especialmente como preparativo para sediar o Fórum de Governança da Internet, em 2007.⁹³ Em 2009, a instituição elaborou os chamados Dez Princípios para a Governança e Uso da Internet,⁹⁴ que buscavam promover uma internet construída coletivamente pelos atores participantes do CGI.br e que posteriormente serviram como semente para a construção do Marco Civil da Internet brasileiro.

A trajetória dessas iniciativas, em princípio não vinculativas, em direção a propostas concretas e robustas, levaram à criação de legislação que protege o cidadão e de uma relação colaborativa para com o Estado, que expandiu o debate sobre o constitucionalismo digital. No caso brasileiro, essas experiências enraizaram princípios e direitos digitais no domínio da política formal e em nível estatal, tornando-o um dos países referência na proteção desses direitos, bem como estabelecendo novos marcos na construção do constitucionalismo digital.⁹⁵ Em diálogo com a resposta europeia, o governo brasileiro não busca se fechar em uma abordagem intraestatal, mas aumentar a conectividade internacional na internet, enquanto garante que os dados de seus cidadãos permaneçam dentro do país.⁹⁶

⁹² “The United Nations must play a leading role in the effort to regulate the conduct of States with regard to these technologies” (ROUSSEFF, Dilma. *Statement By H. E. Dilma Rousseff*. President of the Federative Republic of Brazil. 2013. At The Opening Of The General Debate Of The 68TH Session Of The United Nations General Assembly. Disponível em: https://gadebate.un.org/sites/default/files/gastatements/68/BR_en.pdf. Acesso em: 2 abr. 2021) (Tradução nossa).

⁹³ KURBALIJA, Jovan. *Uma introdução à governança da internet*. São Paulo: Comitê Gestor da Internet no Brasil, 2016. p. 204.

⁹⁴ COMITÊ GESTOR DA INTERNET NO BRASIL – CGI.BR. *Princípios para a governança e uso da internet*. 2009. Disponível em: <https://principios.cgi.br>. Acesso em: 2 abr. 2021.

⁹⁵ GILL, Lex; REDEKER, Dennis; GASSER, Urs. Towards digital constitutionalism?: mapping attempts to craft an internet bill of rights. *Berkman Klein Center For Internet & Society Research Publication*, Cambridge, v. 15, nov. 2015. p. 20.

⁹⁶ BAUMAN, Zygmunt *et al.* Após Snowden: repensando o impacto da vigilância. *Revista Eco Póis*, Rio de Janeiro, v. 18, n. 2, p. 8-35, ago. 2015. p. 18.

Somente uma abordagem multissetorial e multilateral de regulação do ciberespaço pode garantir que o conjunto de medidas internas destinadas à criação de capacidades nacionais de proteção à privacidade e aos direitos humanos seja efetivo e alcance todos os países de maneira semelhante, sem que haja abuso de direitos, ou ativos de vigilância que privilegiem um grupo restrito.

No caso europeu, o continente possui posição próxima àquela defendida pelo Brasil. A proteção contra a excessiva vigilância digital e a estratégia de cibersegurança europeia se dão com base em princípios que preservam a noção de ciberespaço aberto, livre e seguro, especialmente para proteção de direitos fundamentais, direitos esses que funcionam como pilar dessa estratégia.⁹⁷

Além disso, seu poder como maior bloco econômico do mundo permite que a União Europeia atue com uma forte política antimonopólio capaz de afetar até mesmo o modelo de negócios das *big techs* americanas. Dessa maneira, muitos de seus acordos e diplomas legislativos servem de base para o restante dos países do mundo, como foi o caso do RGPD. Suas diretrizes exigem que a coleta de dados em solo europeu conte com a notificação dos titulares das informações tratadas, para captação de seus dados, bem como proíbe que a informação seja tornada pública, ou negociada sem o claro consentimento dos usuários. Tal marco regulatório ainda impõe custosas multas às empresas que violarem tais exigências.

A forte atuação europeia na proteção de dados, por meio da garantia de meios processuais e direitos substanciais aos seus cidadãos, torna a região uma das referências quando se trata da temática do constitucionalismo digital. O RGPD, assim como a atuação ativa da União Europeia, em especial da Alemanha, no intuito de estabelecer uma regulação global para a internet, coloca os direitos humanos em perspectiva, mobilizando redes globais em favor da institucionalização do constitucionalismo digital.⁹⁸

Isso ficou bastante claro na fala de abertura do FGI – Berlin, 2019, quando a então chanceler alemã, Angela Merkel, em seu discurso, defendeu:

Se podemos usar a Internet globalmente ou se queremos usar a Internet globalmente, então também temos que pensá-la globalmente. A Internet afeta a todos, mesmo aqueles que não têm acesso. E por isso temos que melhorar o acesso à Internet e a participação igualitá-

⁹⁷ KURBALIJA, Jovan. *Uma introdução à governança da internet*. São Paulo: Comitê Gestor da Internet no Brasil, 2016. p. 101.

⁹⁸ REDEKER, Dennis. Towards a European Constitution for the Internet? *Bremen International Graduate School Of Social Sciences: Comparative Institutionalization and Mobilization in European and Transnational Digital Constitutionalism*, University Of Bremen And Jacobs University Bremen, v. 1, n. 1, p. 1-21, nov. 2019. p. 17. Disponível em: https://www.giga-net.org/2019symposiumPapers/22_Redeker_Towards-a-European-Constitution.pdf. Acesso em: 31 mar. 2021.

ria dentro da transformação digital. [...] Devemos chegar a um acordo sobre como proteger os direitos humanos, a democracia e o Estado de Direito na era digital, e debater sobre como fortalecer a participação igualitária e a segurança na rede, assim como a confiança na rede. [...] No entanto, em geral, a remodelação da governança da Internet é, naturalmente, uma questão que exigirá esforços globais. Ela exigirá que os Estados e as partes interessadas se unam. A Alemanha está pronta para ajudar a moldar uma nova política global para a Internet sob os auspícios das Nações Unidas. Estamos convencidos de que as Nações Unidas e o IGF têm um papel fundamental a desempenhar na obtenção de um consenso global em favor de uma Internet aberta, livre e descentralizada.⁹⁹

O processo de elaboração da Carta de Direitos Fundamentais da União Europeia demonstra justamente a importância da construção de saberes cooperativos, em especial quando conduzidos por meio de reuniões e encontros regionais, com processos decisórios multilaterais sob uma ótica amplamente democrática de direitos humanos.¹⁰⁰ O sucesso da abordagem europeia guarda relação com seus aspectos vinculados a uma coordenação multinível que integra as dimensões econômicas, sociais, ambientais e políticas, e que gera coerência nos procedimentos e aplicações relacionadas à governança da internet.¹⁰¹

Assim como o CGI.br, a arquitetura das instituições europeias, desde o Parlamento europeu, até as organizações comunitárias da sociedade civil, incorpora elementos de governança multilateral e um processo decisório que engloba sociedade civil, iniciativa privada e governo.

⁹⁹ MERKEL, Angela. *Speech by Federal Chancellor Dr Angela Merkel opening the 14th Annual Meeting of the Internet Governance Forum in Berlin on 26 November 2019*. 2019. Disponível em: <https://www.bundesregierung.de/breg-en/news/speech-by-federal-chancellor-dr-angela-merkel-opening-the-14th-annual-meeting-of-the-internet-governance-forum-in-berlin-on-26-november-2019-1701494>. Acesso em: 2 abr. 2021. Tradução nossa.

¹⁰⁰ REDEKER, Dennis. *Towards a European Constitution for the Internet? Bremen International Graduate School Of Social Sciences: Comparative Institutionalization and Mobilization in European and Transnational Digital Constitutionalism*, University Of Bremen And Jacobs University Bremen, v. 1, n. 1, p. 1-21, nov. 2019. p. 18-19. Disponível em: https://www.giga-net.org/2019symposiumPapers/22_Redeker_Towards-a-European_Constitution.pdf. Acesso em: 31 mar. 2021.

¹⁰¹ FILGUEIRAS, Fernando; ALMEIDA, Virgílio. *Governance for the digital world: neither more state nor more market*. [s.l.]: Springer International Publishing, 2020. p. 91.

4 Considerações finais

Quanto mais a sociedade moderna se torna dependente da internet, mais relevante é a sua governança. Dessa maneira, é possível notar a proximidade das visões do Brasil e da União Europeia quando propõem a governança da internet sob uma ótica multilateral e que engloba vários atores. Essa análise é necessária justamente com o intuito de se coibir práticas de vigilância na sociedade contemporânea. O atual processo decisório dá margem para amplas violações de direitos humanos por meio da coleta desenfreada de informações. Em diferentes situações, o modelo de negócios implementado por *big techs* mostrou-se em descompasso com a proteção internacional dos direitos humanos, representando um grave perigo à privacidade dos indivíduos e à própria ordem democrática dos Estados.

O esforço da União Europeia e do Brasil para que a internet seja tratada como um *common* global se insere em um contexto de reafirmação dos direitos humanos na rede digital. Somente por meio de respostas multissetoriais, multilaterais e com um espaço democrático para discussão será possível encontrar soluções para esses problemas, os quais não se limitam a uma localidade ou região, mas que são, antes de tudo, globais.

No entanto, a despeito dos aspectos positivos e dos avanços legislativos decorrentes do vanguardismo europeu e brasileiro, tais desdobramentos não esgotam seu potencial, bem como não satisfazem em absoluto as necessidades sociais. Ao nos voltarmos à realidade brasileira, por exemplo, é evidente que apesar de positiva a abordagem no tocante à tomada de decisão coletiva e à promoção do modelo *multistakeholder* – há tempos empregado no país – a legislação protetiva do direito à proteção de dados pessoais ainda é pouco aplicada e o trabalho da ANPD é relativamente novo, não tendo esta aplicado sanções até o momento. Apesar da inclusão do direito à proteção de dados no rol de direitos fundamentais disposto no art. 5º da Constituição Federal, para que os benefícios do modelo *multistakeholder* brasileiro sejam potencializados, é necessária uma postura mais ativa, aberta e transparente, principalmente dos atores envolvidos com a construção de políticas públicas.

Similarmente, apesar do peso obrigacional que acompanhou o diploma europeu, as garantias conferidas pela RGPD também não esgotam sua capacidade protetiva, pois, mesmo quando judicialmente ordenadas, aspectos essenciais de proteção têm sido negligenciados, em decorrência de o sistema europeu de proteção de dados ser, em certa medida, burocrático, não harmônico e, conseqüentemente, ineficiente. Ao se manterem inertes, os reguladores minam direitos individuais e, como no caso Google Spain, corroboram para que as empresas e a mídia possam

manipular a situação em favor de seus próprios interesses, limitando consideravelmente o alcance da condenação, com déficit de transparência.¹⁰²

Apesar de haver pontos a serem aprimorados, é inegável que as iniciativas mencionadas ao longo deste trabalho impactaram positivamente o contexto atual da proteção de dados pessoais em suas respectivas jurisdições, em vista de criarem *standards* e mecanismos *multistakeholder* que congregam atores em favor do direito à proteção de dados e à autodeterminação informativa, contribuindo para que as *big techs* se adequem a essa nova realidade digital.

Referências

- BARTH, Carlos Henrique. É possível evitar vieses algorítmicos? *Revista de Filosofia Moderna e Contemporânea*, Brasília, v. 8, n. 3, p. 43-44, dez. 2021.
- BAUMAN, Zygmunt *et al.* Após Snowden: repensando o impacto da vigilância. *Revista Eco Pós*, Rio de Janeiro, v. 18, n. 2, p. 8-35, ago. 2015.
- BERMAN, Paul Schiff. Cyberspace and the State Action Debate: the cultural value of applying constitutional norms to private regulation. *University Of Colorado Law Review*, v. 71, p. 1263-1310, 23 maio 2000.
- BIONI, Bruno. *Proteção de dados pessoais: a função e os limites do consentimento*. Rio de Janeiro: Forense, 2019.
- BRUNO, Fernanda *et al.* *Tecnopolíticas da vigilância: perspectivas da margem*. São Paulo: Boitempo, 2018.
- CELESTE, Edoardo. Digital constitutionalism: a new systematic theorisation. *International Review of Law, Computers & Technology*, v. 33, n. 1, p. 76-99, 2 jan. 2019.
- CELESTE, Edoardo. Terms of service and bills of rights: new mechanisms of constitutionalisation in the social media environment? *International Review of Law, Computers and Technology*, v. 33, n. 2, p. 122-138, 2018.
- COMITÊ GESTOR DA INTERNET NO BRASIL – CGI.BR. *Declaração Multissetorial de São Paulo: NetMundial*. São Paulo: Global Multistakeholder Meeting on the Future of Internet Governance, 2014. Disponível em: https://www.cgi.br/media/docs/publicacoes/4/Documento_NETmundial_pt.pdf. Acesso em: 2 abr. 2021.
- COMITÊ GESTOR DA INTERNET NO BRASIL – CGI.BR. *Princípios para a governança e uso da internet*. 2009. Disponível em: <https://principios.cgi.br>. Acesso em: 2 abr. 2021.
- COUNCIL OF EUROPE. *Declaration by the Committee of Ministers on Internet governance principles*. 2011. Disponível em: https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=09000016805cc2f6. Acesso em: 11 maio 2021.
- DEFENSORIA PÚBLICA DO ESTADO DO RIO DE JANEIRO. *Relatório sobre o reconhecimento fotográfico em sede policial*. 2020. Disponível em: <https://www.defensoria.rj.def.br/uploads/arquivos/33e974efa1004184954cc1b08ac2f253.pdf>. Acesso em: 6 abr. 2022.

¹⁰² POWLES, Julia. The case that won't be forgotten. *Loyola University Chicago Law Journal*, Chicago, v. 47, n. 2, p. 583-615, 2015. p. 612.

- DIAS, Tatiana. YouTube veta impulsionamento de vídeo crítico ao Google. *Centro de Estudos da Mídia Alternativa Barão de Itararé*, 2022. Disponível em: <https://baraodeitarare.org.br/site/noticias/comunicacao/youtube-veta-impulsionamento-de-video-critico-ao-google>. Acesso em: 5 abr. 2022.
- DONEDA, Danilo. Panorama histórico da proteção de dados pessoais. In: BIONI, Bruno *et al.* *Tratado de proteção de dados pessoais*. Rio de Janeiro: Forense, 2021.
- FEELEY, Malcolm M.; SIMON, Jonathan. The new penology. In: McLAUGHLIN, Eugene; MUNCIE, John; HUGHES, Gordon (Org.). *Criminological perspectives: essential readings*. 2. ed. Londres: Sage, 2005.
- FEELEY, Malcolm; SIMON, Jonathan. Actuarial justice: the emerging new criminal law. In: NELKEN, David (Org.). *The futures of criminology*. Londres: Sage, 1994.
- FILGUEIRAS, Fernando; ALMEIDA, Virgílio. *Governance for the digital world: neither more state nor more market*. [s.l.]: Springer International Publishing, 2020.
- FIRMINO, Rodrigo José. Securitização, vigilância e territorialização. In: BRUNO, Fernanda *et al.* *Tecnopolíticas da vigilância: perspectivas da margem*. São Paulo: Boitempo, 2018.
- GILL, Lex; REDEKER, Dennis; GASSER, Urs. Towards digital constitutionalism?: mapping attempts to craft an internet bill of rights. *Berkman Klein Center For Internet & Society Research Publication*, Cambridge, v. 15, nov. 2015.
- GLASER, Hartmut Richard. Internet Governance in Brazil: A multistakeholder approach. *CGI*, 2009. Disponível em: <https://cgi.br/publicacao/internet-governance-in-brazil-a-multistakeholder-approach/>. Acesso em: 31 mar. 2021.
- GOSNELL, Cymone. The General Data Protection Regulation: American compliance overview and the future of the American business. *Journal of Business & Technology Law*, College Park, v. 15, n. 1, p. 165-187, jan. 2019.
- GREGORIO, Giovanni de. *Digital constitutionalism in Europe: reframing rights and powers in the algorithmic society*. Cambridge: Cambridge University Press, 2022.
- GUIMARÃES, Arthur. ANPD: Definição de critérios de dosimetria de pena é 'prioridade zero'. *Jota*, 2022. Disponível em: <https://www.jota.info/coberturas-especiais/protecao-de-dados/anpd-definicao-de-criterios-de-dosimetria-de-pena-e-prioridade-zero-11042022>. Acesso em: 10 maio 2022.
- GUIMARÃES, João Alexandre; MACHADO, Lecio. *Comentários à Lei Geral de Proteção de Dados: Lei 13.709/2018 com alterações da MPV 869/2020*. Rio de Janeiro: Lumen Juris, 2020.
- HAN, Byung-Chul. *Sociedade da transparência*. Petrópolis: Vozes, 2017. Edição Digital.
- HESS, Charlotte; OSTROM, Elinor. *Understanding knowledge as a commons: from theory to practice*. Cambridge: The MIT Press, 2007.
- KURBALIJA, Jovan. *Uma introdução à governança da internet*. São Paulo: Comitê Gestor da Internet no Brasil, 2016.
- LESSIG, Lawrence. *Code and other laws of cyberspace*. New York: Basic Books, 1999.
- LINS, Ricardo Galvão de Sousa; MOREIRA, Thiago Oliveira; GURGEL, Yara Maria Pereira. O constitucionalismo multinível de Ingolf Pernice: uma análise de pontos e contrapontos. *Cadernos de Direito Actual*, n. 15, p. 186-203, jun. 2021.
- LYON, David; ZUREIK, Elia. *Computers, surveillance, and privacy*. Minneapolis: University of Minnesota Press, 1996.
- MAGRANI, Eduardo. *Democracia conectada: a internet como ferramenta de engajamento político-democrático*. Curitiba: Juruá, 2014.

MELO, Maria Heloísa Chiverini de *et al.* Uma análise de conjuntura da Lei Geral de Proteção de Dados Pessoais (LGPD): tramitação, aprovação e vigência. *Revista Humanidades e Inovação*, v. 8, n. 47, 2021.

MENDES, Gilmar Ferreira; FERNANDES, Victor Oliveira. Constitucionalismo digital e jurisdição constitucional: uma agenda de pesquisa para o caso brasileiro. *Revista Brasileira de Direito*, v. 16, n. 1, p. 1-33, jan./abr. 2020.

MERKEL, Angela. *Speech by Federal Chancellor Dr Angela Merkel opening the 14th Annual Meeting of the Internet Governance Forum in Berlin on 26 November 2019*. 2019. Disponível em: <https://www.bundesregierung.de/breg-en/news/speech-by-federal-chancellor-dr-angela-merkel-opening-the-14th-annual-meeting-of-the-internet-governance-forum-in-berlin-on-26-november-2019-1701494>. Acesso em: 2 abr. 2021.

MOLNAR-GABOR, Fruzsina. Data protection. In: GROTE, Rainer; LACHENMANN, Frauke; WOLFRUM, Rüdiger. *Max Planck Encyclopedia of Comparative Constitutional Law*. Oxford: Oxford University Press, 2016. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2883707. Acesso em: 3 abr. 2021.

MONCAU, Luiz Fernando Marrey; ARGUELHES, Diego Werneck. The Marco Civil da Internet and digital constitutionalism. In: FROSIO, Giancarlo. *Oxford Handbook of Online Intermediary Liability*. Oxford: Oxford University Press, 2020. p. 189-213.

MONTEIRO, Artur Pericles Lima; CRUZ, Francisco Brito; SILVEIRA, Juliana Fonteles da; VALENTE, Mariana G. *Armadilhas e caminhos na regulação da moderação de conteúdo: diagnósticos & recomendações*. São Paulo: Internet Lab, 2021. Disponível em: <https://itsrio.org/wp-content/uploads/2021/07/Protecao-de-Dados-e-Transparencia-em-Moderacao-de-Conte%C3%BAdo.pdf>. Acesso em: 4 abr. 2022.

MONTESANTI, Beatriz. Além dos EUA: como a Cambridge Analytica atuava em eleições pelo mundo. *UOL*, 2018. Disponível em: <https://noticias.uol.com.br/internacional/ultimas-noticias/2018/03/24/como-a-cambridge-analytica-atuava-para-alem-dos-eua.htm>. Acesso em: 10 out. 2021.

MOROZOV, Evgeny; BRIA, Francesca. O direito à cidade digital: rumo à soberania tecnológica. In: MOROZOV, Evgeny; BRIA, Francesca. *A cidade inteligente: tecnologias urbanas e democracia*. São Paulo: Ubu Editora, 2019.

NÚCLEO DE ESTUDOS INTERNACIONAIS. *Comentários Gerais dos Comitês de Tratados de Direitos Humanos da ONU*. São Paulo: Núcleo de Estudos Internacionais, 2018. Disponível em: <https://www.defensoria.sp.def.br/dpesp/repositorio/0/Comentários%20Gerais%20da%20ONU.pdf>. Acesso em: 15 set. 2021.

OLIVEIRA, Eliane. Redes de farmácia entram na mira do governo por uso de dados pessoais em programas de descontos. *O Globo*, 2021. Disponível em: <https://oglobo.globo.com/economia/defesa-do-consumidor/redes-de-farmacias-entram-na-mira-do-governo-por-uso-de-dados-pessoais-em-programas-de-descontos-25278675>. Acesso em: 13 maio 2022.

PAYÃO, Felipe. Governo Temer vai abandonar software livre para comprar produtos Microsoft. *Tecmundo*, 2016. Disponível em: <https://www.tecmundo.com.br/microsoft/111214-governo-temer-abandonar-software-livre-comprar-produtos-microsoft.htm>. Acesso em: 6 set. 2021.

PERNICE, Ingolf. EU Democratic Legitimacy and Multilevel Constitutionalism in the Digital Age. Conference “European Economic Governance and The Future of European Democracy”. *European Constitutional Law Network (Ecln)*, Berlin, v. 1, n. 1, ago. 2015.

POWLES, Julia. The case that won't be forgotten. *Loyola University Chicago Law Journal*, Chicago, v. 47, n. 2, p. 583-615, 2015.

REDEKER, Dennis. Towards a European Constitution for the Internet? *Bremen International Graduate School Of Social Sciences: Comparative Institutionalization and Mobilization in European and Transnational*

Digital Constitutionalism, University Of Bremen And Jacobs University Bremen, v. 1, n. 1, p. 1-21, nov. 2019. Disponível em: https://www.giga-net.org/2019symposiumPapers/22_Redeker_Towards-a-European-Constitution.pdf. Acesso em: 31 mar. 2021.

ROUSSEFF, Dilma. *Statement By H. E. Dilma Rousseff*. President of the Federative Republic of Brazil. 2013. At The Opening Of The General Debate Of The 68TH Session Of The United Nations General Assembly. Disponível em: https://gadebate.un.org/sites/default/files/gastatements/68/BR_en.pdf. Acesso em: 2 abr. 2021.

ROUVROY, Antoinette. Entrevista com Antoinette Rouvroy: governamentalidade algorítmica e a morte da política. *Revista de Filosofia Moderna e Contemporânea*, Brasília, v. 8, n. 3, dez. 2020.

SARLET, Ingo Wolfgang. Fundamentos constitucionais: o direito fundamental à proteção de dados. In: BIONI, Bruno et al. *Tratado de Proteção de Dados Pessoais*. Rio de Janeiro: Forense, 2021.

SEGURADO, Rosemary. The Brazilian civil rights framework for the internet: a pioneering experience in internet governance. *The Internet and Health in Brazil*, p. 27-45, 25 out. 2018.

SUZOR, Nicolas. Digital constitutionalism: using the rule of law to evaluate the legitimacy of governance by platforms. *Social Media + Society*, v. 4, n. 3, p. 205630511878781, jul. 2018.

TEDIC. *Declaración Latinoamericana sobre Transparencia de las Plataformas de Internet*. 2021. Disponível em: <https://www.tedic.org/declaracion-latinoamericana-sobre-transparencia-de-las-plataformas-de-internet/>. Acesso em: 15 abr. 2022.

VERBLE, Joseph. The NSA and Edward Snowden: surveillance in the 21st century. *Revista SIGCAS Computer and Society*, v. 44, n. 3, p. 14-20, 2014. Disponível em: <https://doi.org/10.1145/2684097.2684101>.

WAKKA, Wagner. Cisco fecha acordo com Ministério da Ciência para investimentos em digitalização. *Canaltech*, 2020. Disponível em: <https://canaltech.com.br/governo/cisco-fecha-acordo-com-ministerio-da-ciencia-para-investimentos-em-digitalizacao-165586/>. Acesso em: 6 set. 2021.

WE ARE SOCIAL. *Digital 2021: global overview report*. 2021. Disponível em: <https://wearesocial.com/uk/blog/2021/01/digital-2021-uk/>. Acesso em: 27 abr. 2021.

WONG, Julia Carrie. The Cambridge Analytica scandal changed the world – but it didn't change Facebook. *The Guardian*, 2019. Disponível em: <https://www.theguardian.com/technology/2019/mar/17/the-cambridge-analytica-scandal-changed-the-world-but-it-didnt-change-facebook>. Acesso em: 10 out. 2021.

ZUBOFF, Shoshana. *A era do capitalismo de vigilância: a luta por um futuro humano na nova fronteira do poder*. Rio de Janeiro: Intrínseca, 2021.

ZUBOFF, Shoshana. Big other: capitalismo de vigilância e perspectivas para uma civilização de informação. In: BRUNO, Fernanda et al. *Tecnopolíticas da vigilância: perspectivas da margem*. São Paulo: Boitempo, 2018.

Informação bibliográfica deste texto, conforme a NBR 6023:2018 da Associação Brasileira de Normas Técnicas (ABNT):

ALVES, Rodrigo Vitorino Souza; MOURA, Thobias Prado; GÓES, Luma Laura Damasceno. Vigilância e monitoramento na sociedade da informação: contribuições do constitucionalismo digital para a governança da internet. *Direitos Fundamentais & Justiça*, Belo Horizonte, ano 17, n. 49, p. 365-404, jul./dez. 2023.

Submissão: 17.02.2022
Pareceres: 25.03.2022, 03.06.2023
Aceite: 10.07.2023