Cadernos Adenauer

ANO XXV
2024

KONRAD ADENAUER STIFTUNG

3

Inovações tecnológicas e democracia

www.kas.de/brasil

Inovações tecnológicas e democracia

Cadernos Adenauer 3
ANO XXV
2024

Inovações tecnológicas e democracia

KONRAD ADENAUER STIFTUNG

EDITOR RESPONSÁVEL
Maximilian Hedrich

CONSELHO EDITORIAL
Antônio Jorge Ramalho
Estevão de Rezende Martins
Fátima Anastasia
Humberto Dantas
José Mario Brasiliense Carneiro
Leonardo Nemer Caldeira Brant
Lúcia Avelar
Mario Monzoni
Rodrigo Perpétuo
Silvana Krause

COORDENAÇÃO EDITORIAL
Reinaldo J. Themoteo

REVISÃO
Reinaldo J. Themoteo

CAPA, PROJETO GRÁFICO E DIAGRAMAÇÃO
Claudia Mendes

ISSN 1519-0951
Cadernos Adenauer XXV (2024), nº3
Inovações tecnológicas e democracia
Rio de Janeiro: Fundação Konrad Adenauer, dezembro 2024.
ISBN 978-65-89432-53-1

FUNDAÇÃO KONRAD ADENAUER
Representação no Brasil: Rua Guilhermina Guinle, 163 · Botafogo
Rio de Janeiro · RJ · 22270-060
Tel.: 0055-21-2220-5441 · Telefax: 0055-21-2220-5448
adenauer-brasil@kas.de · www.kas.de/brasil

Sumário

Apresentação

O desenvolvimento tecnológico produz variados impactos na vida das pessoas, e tais novidades têm chegado em velocidade cada vez maior, englobando leis, instituições e costumes. Vivemos em uma época de transformações velozes, na qual as inovações tecnológicas reconfiguram os paradigmas da democracia. A velocidade e o alcance dessas inovações desafiam nossas instituições, princípios e valores. Tais impactos demandam muitas vezes a assimilação de novas realidades pelo arcabouço legal dos países, com graus variados de dificuldade para tipificar em forma de lei a tecnologia, seus usos e consequências. As instituições democráticas são testadas de várias formas, confrontadas com inovações que produzem significativas mudanças no modo como vivemos, é a chamada disrupção. Esta publicação apresenta um conjunto de artigos que analisam algumas das principais inovações tecnológicas desenvolvidas nas últimas décadas, bem como o seu impacto nas democracias atuais.

A revolução digital vem modificando a forma como vivemos, trabalhamos e nos relacionamos. A inteligência artificial, computação quântica, a Internet das Coisas e as plataformas digitais estão redefinindo os parâmetros sociais e testando limites. Por outro lado, essas inovações também trazem perigos: desigualdade, desinformação, manipulação e vigilância. É da maior importância refletir sobre os fundamentos da democracia à luz das novas tecnologias, a fim de oferecer respostas adequadas aos novos desafios.

Esta publicação traz seis capítulos que abordam diferentes aspectos das relações entre inovações tecnológicas e democracia: 1. Inovações Disruptivas e Democracia: Uma resposta a partir do constitucionalismo digital, investigando a necessidade de uma abordagem constitucional para regulamentar as tecnologias emergentes. 2. A desinformação como risco global: A contribuição do Brasil para o debate da regulação da Inteligência Artificial, analisando o papel da IA na disseminação de informações falsas. 3. Computação Quântica: Desafios e oportunidades, examinando o impacto potencial da computação quântica na sociedade, englobando as oportunidades e possíveis desafios envolvidos. 4. A urgência da regulação das plataformas digitais, discutindo a necessidade de regulamentação para proteger direitos fundamentais. 5. Ética e Inteligência Artificial: Desafios na modulação e regulação dos algoritmos, abordando questões éticas no desenvolvimento de IA. E, por fim, 6. Internet das Coisas, inovação e desafios: Oportunidades, riscos e o papel do Estado em sociedades datificadas, trazendo reflexões sobre o impacto da IoT na governança.

O objetivo, com a reunião desde conjunto de artigos, é contribuir para uma compreensão mais profunda das relações entre tecnologia e democracia, propor reflexões sobre a importância do desenvolvimento de políticas públicas eficazes, e estimular o debate sobre os desafios e oportunidades das inovações tecnológicas, bem como os seus impactos nas democracias. Esperamos que este número da série Cadernos Adenauer possa inspirar reflexões sobre a necessidade de empreender esforços de modo que as inovações tecnológicas sejam empregadas de modo benéfico para as pessoas bem como para a democracia, em sentido mais amplo.

Maximilian Hedrich
Diretor da Fundação Konrad Adenauer no Brasil

Inovações Disruptivas e Democracia: uma resposta a partir do constitucionalismo digital

João Victor Archegas

Resumo

O artigo explora os desafios impostos pelas inovações tecnológicas disruptivas à democracia contemporânea e propõe o conceito de constitucionalismo digital como uma possível solução. Estruturado em três seções, o trabalho aborda inicialmente o impacto das plataformas digitais e da sociedade algorítmica na redistribuição de poder entre Estados-nação e empresas de tecnologia, sugerindo a necessidade de novos paradigmas regulatórios. Na segunda seção, são analisadas três principais frentes de inovação – inteligência artificial (IA), plataformas digitais de mídias sociais e realidade mista – e seus impactos sobre processos democráticos, como eleições e a moderação de conteúdo online. Na última seção, a corregulação é apresentada como um modelo híbrido de governança, no qual Estado e plataformas colaboram para garantir a proteção dos direitos fundamentais e o respeito aos princípios constitucionais. O artigo conclui que o constitucionalismo digital oferece um caminho para a adaptação das estruturas jurídicas (de proteção de direitos e da democracia) à era digital.

Abstract

The article explores the challenges posed by disruptive technological innovations to contemporary democracy and proposes the concept of digital constitutionalism as a possible solution. Structured in three sections, the paper initially addresses the impact of digital platforms and the algorithmic society on the redistribution of power between nation-states and technology companies, suggesting the need for new regulatory paradigms. The second section analyzes three main fronts of innovation – artificial intelligence (AI), digital social media platforms and mixed reality – and their impact on democratic processes, such as elections and the moderation of online content. In the last section, co-regulation is presented as a hybrid model of governance, in which the state and platforms collaborate to guarantee the protection of fundamental rights and respect for constitutional principles. The article concludes that digital constitutionalism offers a path for adapting legal structures (for the protection of rights and democracy) to the digital age.

1. Introdução: Um distúrbio no ecossistema constitucional

Inovações tecnológicas "disruptivas" – é dizer, novas tecnologias que mudam fundamentalmente a forma como interagimos uns com os outros e a realidade ao nosso redor – podem apresentar uma bênção ou uma maldição para a democracia liberal. Tudo depende de como e com qual propósito são implementadas. É essa a visão apresentada por Brad Smith, presidente da Microsoft, em seu livro "Armas e Ferramentas"[1]. Para Smith, embora não seja novidade que novas tecnologias podem criar novas realidades, a questão que se coloca diante de nós em relação ao nosso futuro é: como canalizar todo esse potencial disruptivo para

1 SMITH, Brad. BROWNE, Carol Ann. **Armas e Ferramentas**: O futuro e o perigo da era digital. Rio de Janeiro: Alta Books, 2021.

o bem da humanidade? O presente trabalho busca contribuir com essa discussão a partir do constitucionalismo digital.

Neste artigo, dividimos a análise em três partes principais para abordar os desafios impostos pelas inovações disruptivas ao desenvolvimento da democracia na era digital. No primeiro tópico, exploramos a emergência da sociedade algorítmica, destacando como plataformas digitais transnacionais moldam interações sociais e políticas, muitas vezes rivalizando com o poder estatal. Discutimos o caso do X no Brasil, que ilustra os limites da jurisdição do Estado no ambiente digital e como isso reforça a importância de pensar em novos paradigmas de regulação. A partir dessa análise, introduzimos o conceito de constitucionalismo digital, sugerindo a adaptação de estruturas constitucionais clássicas para lidar com o poder das plataformas digitais.

O segundo tópico traz um panorama inicial das inovações disruptivas e seus impactos na democracia, com foco em três frentes principais. Primeiro, discutimos o uso de inteligência artificial (IA) nas eleições, abordando os desafios regulatórios trazidos pela IA generativa na propaganda eleitoral. Em seguida, analisamos o papel das plataformas digitais na desinformação, ressaltando como as redes sociais têm sido instrumentalizadas para propagar conteúdos falsos e prejudicar o debate público. Finalmente, refletimos sobre a moderação de conteúdo em um cenário de realidade mista, explorando os desafios de moderação em ambientes digitais mais imersivos.

No terceiro e último tópico, propomos soluções a partir do constitucionalismo digital. Discutimos, assim, o conceito de IA constitucional, que busca alinhar a tomada de decisões de sistemas de IA a princípios constitucionais, e examinamos o papel da corregulação na moderação de conteúdo e comportamento em plataformas digitais, sugerindo que a colaboração entre Estado e plataformas pode criar um ambiente mais transparente e responsável. Ao final, avaliamos algumas vantagens no modelo de moderação oferecido pelo Oversight Board da Meta, propondo novos mecanismos para aprimorar a governança digital de forma constitucionalmente orientada com a participação do Estado.

1.1 Uma nova sociedade e um novo paradigma de poder

As transformações sociais operadas por tecnologias digitais são estudadas desde os primórdios da Internet comercial. Um dos principais expoentes deste campo de investigações é o sociólogo espanhol Manuel Castells, para quem a Internet é responsável por uma nova forma de organização social. Essa nova realidade social-digital ficou conhecida, a partir do seu trabalho, como "sociedade em rede"[2]. Ao invés de uma sociedade estruturada a partir de instituições hierárquicas tradicionais, temos uma sociedade baseada em redes globais de interação a partir de uma nova plataforma econômica, qual seja, a economia da informação.

Muita coisa mudou na seara digital, entretanto, desde que Castells publicou pela primeira vez sua obra sobre o tema em 1996. A economia da informação foi aos poucos se transformando em economia da atenção, inserida em um contexto de capitalismo da vigilância como se refere Shoshana Zuboff[3]. Não se trata mais apenas de coleta, processamento e transmissão de dados, mas sim do emprego de técnicas preditivas para o direcionamento de anúncios online que, por sua vez, se transformam em fortes incentivos econômicos para manter usuários de plataformas digitais ativos por mais tempo. Não faltam estudos sobre os impactos dessa nova dinâmica socioeconômica em nossa esfera pública, incluindo maior polarização política[4].

Assim como a expansão da Internet comercial trouxe consigo uma nova forma de organização social, a revolução das plataformas digitais que dominam o nosso cotidiano – das redes sociais aos mecanismos de busca, passando por aplicações de mensageria privada e *marketplaces* – está, aos poucos, pautando uma nova manifestação social: a "sociedade algorítmica". Nas palavras de Jack Balkin, esta nova forma de or-

2 CASTELLS, Manuel. **A sociedade em rede**. São Paulo: Paz & Terra, 2013.

3 ZUBOFF, Shoshana. **A era do capitalismo de vigilância**. São Paulo: Intrínseca, 2021.

4 Ver, em linhas gerais, SUNSTEIN, Cass. **#Republic**: Divided democracy in the age of social media. Princeton: Princeton University Press, 2018.

ganização social é caracterizada por plataformas digitais transnacionais que se posicionam entre os tradicionais Estados-nação e os indivíduos para "governar populações através do uso de algoritmos e inteligência artificial"[5]. É dizer, a governança privada de plataformas digitais – que, por sua vez, tem um impacto significativo e imediato no ecossistema constitucional estatal – está cada vez mais automatizada e baseada em algoritmos.

Some-se isso ao fato de que o sonho ciberlibertário dos anos 90 nunca se concretizou. Pelo contrário, a Internet, em especial nas últimas duas décadas, possibilitou a ascensão de algumas poucas empresas ao status de "império na nuvem"[6], concentrando cada vez mais poder (econômico e político) em relação às estruturas sociais modernas. Os visionários do "ciberespaço" nos prometeram uma Internet que iria nos libertar de instituições poderosas ao empoderar os "internautas". Nada obstante, "em vez de tornarem o poder estatal obsoleto, [as plataformas] passaram a rivalizá-lo"[7]. Em outras palavras, plataformas e estados competem por poder na arena transnacional, muitas vezes em pé de igualdade. Daí a ideia de Kate Klonick de que as plataformas seriam os "novos governadores" da era digital, pautando diretamente diversos aspectos da nossa vida em sociedade[8].

Não tardou para que as externalidades negativas desta concentração fossem sentidas em democracias ao redor do mundo. A mesma Internet creditada pela primavera árabe no início de 2011 seria culpada pela desinformação que levou à invasão do Capitólio dez anos depois, em 2021, em Washington. O otimismo deu lugar ao pessimismo; em 2020, 49%

---

5 BALKIN, Jack. Free Speech in the Algorithmic Society: Big Data, Private Governance, and New School Speech Regulation. **UC Davis Law Review**, v. 51, 2018, 1151.

6 LEHDONVIRTA, Vili. **Cloud Empires**: How digital plataformas are overtaking the state and how we can regain control. Cambridge: MIT Press, 2022.

7 *Ibidem*, p. 205. Tradução livre.

8 KLONICK, Kate. The New Governors: The people, rules, and processes governing online speech. **Harvard Law Review**, v. 131, 2018.

dos especialistas ouvidos pelo Pew Research Center disseram que até 2030 a tecnologia provavelmente irá enfraquecer a democracia ao invés de fortalecê-la[9]. Esse pessimismo, por sua vez, alimentou um processo de "techlash" que perdura até hoje. Nas palavras de Rachel Botsman, "antes vistos como salvadores da democracia, os titãs da era digital agora são vistos como uma ameaça à verdade ou, no mínimo, bilionários inertes que falham em monitorar seu próprio quintal"[10].

1.2 O caso do X no Brasil e os limites do Estado

Por mais incômoda que essa realidade seja, é preciso enfrentar suas consequências com pragmatismo. Falar de inovações disruptivas é falar de grandes empresas de tecnologia que moldam relações socioeconômicas a partir dos seus produtos e serviços. Essa regra vale, inclusive, para aquela que é talvez a principal dentre as recentes inovações disruptivas: a inteligência artificial (IA)[11]. A concentração de poder neste setor é inegável: 96% dos grandes modelos de IA hoje são criados por empresas e o setor privado tem 29 vezes mais poder computacional que universidades[12]. Para entender os impactos das novas tecnologias na democracia e o que pode ser feito sobre isso, portanto, deve-se antes enfrentar a relação entre empresas de tecnologia – em especial plataformas digitais – e o Estado.

---

9 ANDERSON, Janna. RAINIE, Lee. Many Tech Experts Say Digital Disruption Will Hurt Democracy. **Pew Research Center**, 21 de fevereiro de 2020. Disponível em <https://www.pewresearch.org/internet/2020/02/21/many-tech-experts-say-digital-disruption-will-hurt-demo cracy/>.

10 BOTSMAN, Rachel. Dawn of the Techlash. **The Guardian**, 11 de fevereiro de 2018. Disponível em <https://www.theguardian.com/commentisfree/2018/feb/11/dawn-of-the-techlash>.

11 Para uma introdução ao estudo da IA, ver ARCHEGAS, João Victor. MAIA, Gabriella. O que é inteligência artificial (IA)? Análise em três atos de um conceito em desenvolvimento. **Cadernos Adenauer**, v. XXIII, n. 2, 2022, 9-28.

12 EASTWOOD, Brian. Industry now dominates AI research. **MIT Sloan**, 18 de maio de 2023. Disponível em <https://mitsloan.mit.edu/ideas-made-to-matter/study-industry-now-dominates-ai-research>.

No contexto brasileiro, essa relação foi marcada pelo recente atrito entre a rede social X (antigo Twitter) e o Supremo Tribunal Federal. Após a empresa descumprir diversas ordens de remoção de perfis no âmbito do inquérito das fake news por ordem de Elon Musk, o atual dono da plataforma, o ministro Alexandre de Moraes determinou o seu bloqueio em território nacional no dia 30 de agosto de 2024. Com o intuito de garantir a eficácia da medida, Moraes também ordenou a aplicação de multa diária no valor de R$ 50 mil para quem se valesse de subterfúgios tecnológicos, em especial VPNs, para continuar acessando a rede social dentro do Brasil. A previsão de multa foi amplamente criticada por especialistas, sendo vista como desproporcional e inexequível, além de desconsiderar os usos legítimos de VPNs para segurança cibernética e privacidade na Internet[13].

A ordem de bloqueio, entretanto, logo mostrou suas principais falhas. A relação entre Internet, Direito e Jurisdição é complexa. Ao mesmo tempo em que a Internet desafia os limites territoriais do Estado, não se pode desconsiderar que a infraestrutura que permite o funcionamento da rede é formada por cabos e servidores que estão situados dentro dos limites de um determinado território – que, por sua vez, é controlado por um determinado Estado[14]. Assim, embora seja possível proibir que o X use a infraestrutura digital brasileira para ofertar seus serviços no Brasil, pouco pode ser feito (pelo menos de forma legítima e legal) a respeito de usuários dentro do país que queiram acessar tal plataforma por meio da infraestrutura digital de outra nação através de VPNs.

---

13 FIGUEIREDO, Pedro Augusto; LIMA, Pedro. Multa de 50 mil a quem acessar X com VPN é exagerada, desproporcional e inexequível, dizem juristas. **Terra**, 30 de agosto de 2024. Disponível em <https://www.terra.com.br/byte/multa-de-50-mil-a-quem-acessar-x-com-vpn-e-exagerada-desproporcional-e-inexequivel-dizem-juristas.html>

14 Sobre a relação entre Internet, infraestrutura digital e jurisdição, ver GOLDSMITH, Jack. WU, Tim. **Who Controls the Internet?** Illusions of a borderless world. Oxford: Oxford University Press, 2006.

Ademais, ordens de bloqueio nunca são totalmente implementadas. O Brasil conta com milhares de provedores de conexão à Internet, pequenos e grandes. Algumas dessas operadoras não bloquearam o X, seja por falta de capacidade técnica ou por simplesmente ignorarem a notificação que receberam da Anatel, fazendo com que a plataforma continuasse disponível em algumas regiões do país. Outro episódio que reforça esse argumento foi a implementação da tecnologia de proxy reverso da Cloudflare em relação aos servidores do X em setembro de 2024, fazendo com que a rede social voltasse a ser acessada por alguns usuários brasileiros temporariamente em setembro de 2024.

1.3 Constitucionalismo digital

A situação do X no Brasil ilustra o argumento de Vili Lehdonvirta apresentado acima no sentido de que empresas de tecnologia passaram a rivalizar com o poder estatal na arena transnacional. Algumas dessas empresas se comportam como "Corporações-nação", adotando padrões de governança que impactam direta e profundamente o exercício de direitos humanos e fundamentais de bilhões de pessoas ao redor do mundo. Consequentemente, diversas plataformas digitais passaram a testar os limites do poder estatal na era digital. Veja-se, nesse sentido, o posicionamento da Meta em relação ao parlamento australiano em 2021[15] e a crise entre o Telegram e o Kremlin a partir de 2018[16], apenas para citar alguns exemplos. Em ambos os casos, as empresas conseguiram reverter,

15 ARCHEGAS, João Victor. Trouble Down Under: O Facebook coloca seu poder de barganha à prova na Austrália. **ITS Rio**, 26 de fevereiro de 2021. Disponível em <https://feed.itsrio.org/trouble-down-under-o-facebook-coloca-seu-poder-de-barganha-%C3%Ao-prova-na-a ustr%C3%A1lia-606e868b50e0>.

16 REUTERS. Russia lifts ban on Telegram messaging app after failing to block it. **Reuters**, 18 de junho de 2020. Disponível em <https://www.reuters.com/article/technology/russia-lifts-ban-on-telegram-messaging-app-after-failing-to-block-it-idUSKBN23P2DY/>.

com base no exercício do seu poder privado, uma decisão adotada por Estados-nação em relação aos seus serviços.

Esses e outros exemplos que se acumulam ao longo da última década deixam evidente que estamos diante de uma nova configuração do poder na era digital. Isso não significa, é claro, que os estados devem abandonar qualquer pretensão regulatória para se curvar às demandas das empresas de tecnologia. Mas é fato que grandes plataformas digitais possuem um maior poder de barganha em relação ao poder estatal, forçando países como Brasil, Austrália e Rússia a recalcular a rota diante da ineficácia de certas medidas. E é justamente esse novo arranjo transnacional que nos permite pensar a respeito de um dos temas centrais deste artigo: o constitucionalismo digital. Como se sabe, o constitucionalismo está ancorado em uma longa tradição que se debruça sobre a necessidade de implementação de limitações constitucionais ao exercício do poder[17]. É dizer, trata-se de "restringir o poder arbitrário e garantir um governo limitado"[18].

A partir do momento em que plataformas digitais se transformam em "governadores" da era digital, pautando o exercício de direitos humanos e fundamentais dos seus usuários, é preciso refletir também sobre o estabelecimento de limites constitucionais nesta nova fronteira do poder[19]. Isso é ainda mais urgente quando se reconhece o alcance limitado do poder estatal sobre a arena digital. Como explica Nicolas Suzor, "empresas de tecnologia desempenham um papel central na governança de nossas ações, mas os seus poderes são exercidos de uma maneira que não se coaduna com os padrões de legitimidade que nos acostumamos

17 MCILWAIN, Charles Howard. **Constitutionalism**: Ancient and Modern. edição revisada. Ithaca: Cornell University Press, 1947.

18 SARTORI, Giovanni. Constitutionalism: A preliminary discussion. **The American Political Science Review**, v. 56, n. 4, 1962, p. 855. Tradução livre.

19 ARCHEGAS, João Victor. **Constitucionalismo Digital**: Limites constitucionais na nova fronteira do poder. Belo Horizonte: Fórum, 2025.

a esperar dos nossos governos"[20]. O constitucionalismo digital, assim, nos ajuda a pensar em soluções eficazes para as externalidades negativas apresentadas por inovações disruptivas. Isso se dá, portanto, através da constitucionalização da governança interna de grandes empresas de tecnologia.

Vale destacar que isso não significa a substituição do constitucionalismo estatal por um constitucionalismo "cosmopolita" como argumentam os críticos do conceito. Como bem pontua Neil Walker, ainda que o "constitucionalismo ofereça um caminho para um novo quadro de autoridade legal para além do Estado, ele deve, necessariamente, continuar a lidar com um intenso tráfego vindo da direção do Estado"[21]. Daí a ideia de que o constitucionalismo digital continua tendo como ponto de referência o constitucionalismo estatal, não constituindo propriamente uma revolução conceitual como alguns acreditam. Por meio do método sociológico de generalização e reespecificação, estruturas e funções constitucionais são "calibradas cuidadosamente de acordo com a episteme idiossincrática do regime transnacional em questão"[22], trazendo, assim, limites constitucionais para dentro de plataformas digitais. Exemplos práticos de como essa metodologia pode ser aplicada serão apresentados a seguir.

2. Inovações Disruptivas e Democracia

Para os fins do presente artigo, como dito anteriormente, inovações disruptivas são novas tecnologias que mudam fundamentalmente a forma como interagimos uns com os outros e a realidade ao nosso redor. Considerando os impactos da sociedade algorítmica no desenvolvi-

20 SUZOR, Nicolas P. **Lawless**: The secret rules that govern our digital lives. Cambridge: Cambridge University Press, 2019, p. 106. Tradução livre.

21 WALKER, Neil. Taking constitutionalism beyond the state. **Political Studies**, v. 56, n. 3, 2008, p. 540. Tradução livre.

22 TEUBNER, Gunther. Quod omnes tangit: Transnational constitutions without democracy? **Journal of Law and Society**, v. 45, n. S1, 2018, p. 27. Tradução livre.

mento da democracia liberal moderna, serão apresentadas, a seguir, três inovações que merecem nossa especial atenção: inteligência artificial, plataformas digitais e realidade mista. Essas inovações servirão de fio condutor para a discussão a respeito da relação entre inovações disruptivas e democracia, pavimentando o caminho para algumas propostas de como aliviar eventuais tensões a partir dos aportes oferecidos pelo constitucionalismo digital.

2.1 Inteligência artificial e eleições

Quando se fala em inteligência artificial (IA), é preciso desmistificar algumas pré-compreensões. Não se trata de um campo apenas técnico, dominado por cientistas e engenheiros, mas sim de um campo fundamentalmente político e, por isso, humano. É dizer, a IA, paradoxalmente, não é "artificial", tendo em vista que é formada por recursos humanos e naturais, e também não é «inteligente», uma vez que em sua base está um intenso treinamento computacional e por reforço humano – sem o qual, vale reforçar, a IA não é capaz de agir ou resolver problemas[23]. Não há, pelo menos no estado atual de desenvolvimento tecnológico, uma IA "autônoma" ou "racional". Tal visão segue restrita aos filmes e livros de ficção científica.

Assim, com o intuito de oferecer uma primeira aproximação conceitual, é possível afirmar que "a IA é um braço da computação cujo objetivo primordial é desenvolver programas computacionais capazes de automatizar ações inteligentes"[24], ou seja, ações antes desempenhadas apenas (ou principalmente) por seres humanos. Embora o campo da IA seja vasto e diversificado, englobando desde aspiradores-robô até

23 Para uma discussão sobre a natureza da IA, ver CRAWFORD, Kate. **Atlas of AI**: Power, politics, and the planetary costs of artificial intelligence. New Haven: Yale University Press, 2021.

24 ARCHEGAS, João Victor. MAIA, Gabriella. O que é inteligência artificial (IA)? Análise em três atos de um conceito em desenvolvimento. **Cadernos Adenauer**, v. XXIII, n. 2, 2022, p. 13.

assistentes virtuais por voz, as principais discussões hoje sobre seus limites éticos e impactos sociais giram em torno da chamada IA generativa. Baseadas em uma metodologia de aprendizado profundo (*deep-learning*), IAs generativas são modelos capazes de criar novos textos, imagens, vídeos e áudios de alta qualidade a partir da base de dados sobre as quais são construídas.

A questão que se coloca, assim, é que uma IA generativa será mais eficiente quanto mais diversificada for sua base de dados. Em sentido contrário, as limitações de uma IA generativa, incluindo riscos como outputs discriminatórios, são diretamente proporcionais à falta de diversidade em sua base de dados. Daí a necessidade de se pensar em governança da IA, buscando a proteção de certos princípios para o seu bom funcionamento como a não discriminação, equidade, confiabilidade, segurança, accountability, privacidade e transparência[25]. Já em relação aos seus potenciais impactos para a democracia na era digital, emerge como prioritária a discussão sobre quais são os limites para o uso da IA generativa nas eleições.

Esse foi um dos temas regulamentados pelo Tribunal Superior Eleitoral (TSE) em sua Resolução nº 23.732 de 2024. Antecipando o uso de IA pelas candidaturas durante o pleito municipal de 2024, o TSE aprovou, de forma pioneira, três principais regras: (1) a proibição do uso de *deep fakes* – isto é, conteúdo digital em forma de áudio, vídeo ou uma combinação de ambos para criar, substituir ou alterar imagem ou voz de qualquer pessoa –; (2) o dever de informar, de forma clara e explícita, sempre que a candidatura usar IA para gerar ou modificar peças de propaganda eleitoral que não constituam *deep fakes*; e (3) a vedação do uso de chatbots ou avatares para simular conversas com a pessoa candidata ou qualquer outra pessoa real. Em linhas gerais, o TSE buscou estabelecer as condições mínimas para que a IA seja usada de uma forma ética, sem enganar o eleitorado ou distorcer as condições do pleito.

25 *Ibidem*, p. 23-26.

2.2 Plataformas digitais e desinformação

Como ensina Helen Margetts, plataformas digitais, em especial redes sociais, são responsáveis por uma forte "turbulência política" na era digital27[26]. Isso se deve ao fato de que hoje a política é cada vez menos "institucional" e cada vez mais estruturada em torno de pequenos atos políticos desempenhados na Internet. Ou seja, usuários de redes sociais participam da vida política não como antes – se filiando ao seu partido político de escolha ou organizando protestos em vias públicas, por exemplo –, mas sim doando doses homeopáticas do seu tempo a uma determinada causa política por meio de likes, comentários e compartilhamentos.

Isso significa que elementos e estruturas tradicionais, que antes funcionavam como estabilizadores da democracia, agora podem ser ignorados e ultrapassados nas redes sociais, fazendo com que aqueles pequenos atos políticos escalem de forma imprevisível – é isso, portanto, que configura uma "turbulência política". Para usar uma linguagem mais coloquial, informações podem "viralizar" nas redes de forma imprevisível, impactando de forma profunda o debate público e político. Assim, a mesma tecnologia que solucionou desafios de coordenação política no oriente médio e impulsionou a Primavera Árabe também pode ser instrumentalizada para espalhar desinformação e enfraquecer a democracia.

É sobre essa dinâmica, portanto, que devemos nos concentrar quando o assunto é democracia e redes sociais. Pessoas e grupos mal intencionados se valem desta nova realidade tecnopolítica para viralizar conteúdos desinformativos, comprometendo nossa integridade informacional de forma inorgânica e coordenada. Criam-se, assim, verdadeiras "máquinas da mentira", ou seja, "um sistema de pessoas e tecnologias

26 MARGETTS, Helen. Rethinking Democracy with Social Media. **Political Quarterly Monograph Series**, 2019, 107-23.

que distribui mensagens falsas a serviço de uma agenda política"[27]. Nada obstante, é importante destacar que embora nosso sistema constitucional proteja a liberdade de expressão, não há um direito fundamental à liberdade de viralização. É preciso que plataformas digitais atuem de forma incisiva contra "máquina da mentira" e campanhas de comportamento inautêntico coordenado.

2.4 Realidade mista e moderação

Uma nova fronteira da discussão sobre a moderação de conteúdo e comportamento na Internet está se apresentando a partir de tecnologias de realidade mista (ou *mixed reality*). Trata-se, na prática, da junção de funcionalidades da realidade virtual (VR) e da realidade aumentada (AR) para oferecer aos usuários de plataformas digitais uma experiência mais realista e imersiva na Internet. Um bom exemplo de como essa tecnologia pode ser implementada – que, vale dizer, é ainda muito cara e inacessível para a maior parte da população global – é o óculos de realidade mista da Apple, o Apple Vision Pro. Trata-se, na prática, de um computador em forma de headset que mistura elementos digitais com o mundo ao seu redor, possibilitando uma experiência digital mais "natural" e fluida.

Embora muito do que o "metaverso" prometeu entre 2021 e 2022 não tenha se concretizado até hoje, é evidente que a indústria de novas tecnologias está apostando cada vez mais em dispositivos e experiências baseadas na visão oferecida pela realidade mista para um futuro digital cada vez mais imersivo. É difícil dizer com certeza quando e como isso se tornará *mainstream*, mas já é possível antecipar alguns dos impactos dessa inovação disruptiva, em especial no campo da moderação de conteúdo e comportamento. Em outras palavras, a realidade mista

27 HOWARD, Philip. **Lie Machines**: How to save democracy from troll armies, deceitful robots, fake news operations, and political operatives. New Haven: Yale University Press, 2020, p. 13. Tradução livre.

vai mudar consideravelmente a forma como plataformas digitais limitam o que se fala e faz no espaço digital, com claras repercussões para a democracia.

Atualmente, plataformas digitais, em especial redes sociais, precisam moderar quatro tipos básicos de conteúdo (ou uma combinação deles): texto, imagem, áudio e vídeo. Em plataformas que se baseiam em realidade mista, novas dimensões de conteúdo são contempladas, dificultando ainda mais o trabalho de moderação. Considere, por exemplo, os gestos do usuário e até mesmo a personalização do ambiente digital no qual diferentes usuários poderão interagir[28]. Tudo isso passa a ser objeto de moderação e exige novas soluções para combater problemas como assédio, discurso de ódio e desinformação. A pergunta que se deve fazer, assim, é se as empresas de tecnologia que apostam em soluções de realidade mista estão ou não se preparando de forma adequada para essa nova fronteira da moderação na era digital.

3. Uma resposta a partir do constitucionalismo digital

Feito esse primeiro mapeamento de inovações disruptivas que têm ou terão um impacto no desenvolvimento dos predicados da democracia moderna, a questão que fica é: o que devemos fazer? Ou seja, precisamos de estratégias claras de como mitigar impactos negativos, evitando que a tecnologia seja instrumentalizada como uma arma apontada para o coração da democracia, e, ao mesmo tempo, potencializar seus impactos positivos. Afinal, não se pode perder de vista o potencial democratizante das inovações tecnológicas e os inúmeros benefícios associados a uma Internet livre, aberta e participativa. Para nos ajudar na formula-

28 Isso pode envolver, assim, gestos considerados ofensivos como aqueles usados por grupos supremacistas ou até mesmo espaços digitais personalizados que foram criados para simular atentados terroristas do passado, como aconteceu no Roblox em relação ao atentado de Christchurch. Ver, nesse sentido, BRANDOM, Russell. Roblox is struggling to moderate recreations of mass shootings. **The Verge**, 17 de agosto de 2021.

ção de uma resposta, é preciso voltar ao conceito de constitucionalismo digital apresentado acima.

A partir do conceito de constitucionalismo digital, é possível vislumbrar um paradigma de corregulação, no qual Estado e plataformas digitais compartilham a responsabilidade pela definição de normas e limites para o exercício de poder no ambiente digital. Esse paradigma é uma resposta à constatação de que as grandes plataformas tecnológicas, ao atuarem como mediadoras de informações e comportamentos, exercem funções típicas de governança, muitas vezes comparáveis ao poder estatal. Assim, a corregulação não apenas reconhece a necessidade de limites constitucionais para além das fronteiras do Estado-nação, mas também propõe que esses limites sejam construídos de forma colaborativa, envolvendo tanto os mecanismos estatais de regulação quanto as estruturas internas de governança das plataformas.

Essa dinâmica de corregulação tem implicações profundas para a relação entre o Estado e as plataformas digitais. Tradicionalmente, o constitucionalismo pressupunha um Estado soberano responsável por regular e garantir os direitos fundamentais de seus cidadãos. No entanto, no contexto da era digital, as plataformas detêm um poder sem precedentes sobre a esfera pública, o que desafia o modelo clássico de regulação estatal. Nesse novo cenário, as plataformas não são meros agentes econômicos, mas verdadeiros atores políticos que influenciam diretamente a formação da opinião pública, a disseminação de informações e o exercício de liberdades. Assim, a corregulação emerge como um modelo mais eficaz, no qual o Estado, ao invés de impor unilateralmente regras, atua em parceria com as plataformas para garantir que os direitos e valores constitucionais sejam respeitados.

Por fim, o processo de constitucionalização da governança interna das plataformas revela-se crucial para a proteção dos direitos fundamentais na era digital. Ao internalizar valores como transparência, accountability e o respeito aos direitos fundamentais, as plataformas passam a operar sob parâmetros que evitam a arbitrariedade e o abuso de poder. Este processo não implica na substituição do Estado como

regulador, mas sim em um mecanismo de complementação, no qual o poder regulatório é compartilhado e adaptado às particularidades do ambiente digital. A constitucionalização da governança interna é, portanto, uma ferramenta indispensável para garantir que o poder privado, exercido pelas plataformas, seja controlado e limitado, em conformidade com os princípios constitucionais que regem a vida democrática.

3.1 Inteligência artificial constitucional

Como visto acima, um dos principais desafios para a democracia em termos de inovações disruptivas é o uso de IA, em especial no contexto eleitoral. Essa discussão está intimamente conectada a um problema que permeia o desenvolvimento e a implementação de ferramentas de IA, qual seja, a falta de transparência. Alguns autores passaram a se referir a essa realidade por meio de termos como "caixa preta algorítmica" ou "sociedade da caixa preta"[29], uma alusão ao fato de que ferramentas de IA são pouco transparentes e é quase impossível compreender todas as nuances do seu funcionamento. Isso coloca em risco a proteção de direitos fundamentais na era digital, justamente por uma falta crônica de *accountability* e controle em relação a algoritmos que desempenham funções essenciais para nossa sociedade (desde análise de crédito até criação de textos e imagens).

O constitucionalismo digital, ao seu turno, aponta para a necessidade de se promover a constitucionalização de subsistemas da sociedade global que gradualmente estão se desprendendo da órbita gravitacional do Estado-nação. Isso inclui, como visto acima, plataformas digitais e grandes empresas de tecnologia. Ou seja, para garantir que a IA atue de forma a proteger e não ameaçar direitos fundamentais, é preciso, acima de tudo, promover a constitucionalização de sua governança. Isso significa, em outras palavras, ajustar o funcionamento de sistemas de IA à

29 PASQUALE, Frank. **The Black Box Society**: The secret algorithms that control money and information. Cambridge: Harvard University Press, 2016.

luz da lógica operacional do sistema de proteção de direitos fundamentais que é próprio do constitucionalismo moderno. Daí a ideia de uma "Inteligência Artificial Constitucional".

Embora seja importante que o Estado promova a regulação do uso da IA, criando mecanismos capazes de mitigar seus principais riscos – como é o caso do AI Art na União Europeia e o Projeto de Lei nº 2.338/2023 no Brasil –, o constitucionalismo digital reconhece que empresas de tecnologia se tornaram as "novas governadoras" da arena digital e, por isso, é preciso estabelecer limites constitucionais também nesta nova fronteira do poder. No caso da IA, isso pode se traduzir em novas metodologias de treinamento de modelos de linguagem natural (ou LLMs), fazendo com que os outputs dos sistemas de IA sejam calibrados em relação aos valores e princípios constitucionais de uma determinada comunidade ou população.

Veja-se, nesse sentido, a proposta de uma IA constitucional por parte da Anthropic. Segundo a empresa, a ideia é "oferecer modelos de linguagem valores explícitos determinados por uma constituição ao invés de valores determinados de forma implícita por feedback humano em larga escala"[30]. É dizer, a metodologia de treinamento de modelos de linguagem dominante atualmente, o reforço por feedback humano, acaba por estabelecer valores que guiam o comportamento do modelo de forma implícita. Isso apenas intensifica o problema mencionado acima de falta de transparência e accountability em sistemas de IA. A IA constitucional, ao seu turno, aposta em uma metodologia de treinamento adversativo, fazendo com que o modelo, por meio de feedback oferecido pela própria IA, "use um conjunto de princípios para tomar decisões sobre seus outputs"[31].

30 Informação retirada do site da Anthropic sobre seu projeto "Claude's Constitution". Disponível em <https://www.anthropic.com/news/claudes-constitution>

31 *Ibidem*.

3.2 Corregulação e moderação

Ao invés de uma substituição do constitucionalismo estatal por um suposto constitucionalismo cosmopolita, o constitucionalismo digital aponta para a emergência de um ecossistema constitucional eminentemente híbrido. Em outras palavras, o termo "digital" em "constitucionalismo digital" é adjunto adverbial e, por isso, não serve de justificativa para uma nova e autônoma vertente da teoria constitucional moderna[32]. Consequentemente, "sua legitimidade [...] depende das pontes de transição (ou então das colisões normativas) entre o regime constitucional do Estado-nação e o regime transnacional em questão"[33]. O constitucionalismo digital existe em referência ao constitucionalismo estatal, se materializando a partir da reespecificação de elementos e estruturas constitucionais em um novo contexto social.

Assim, a solução para as principais distorções causadas por inovações disruptivas não é nem a regulação direta ou clássica pelo Estado nem a autorregulação pelas próprias empresas de tecnologia. É preciso, cada vez mais, apostar em técnicas de corregulação, onde "um órgão estatal oferece direcionamentos aos membros de determinado setor no estabelecimento de suas regras e princípios, retendo a prerrogativa de intervir quando necessário"[34]. Ou seja, trata-se justamente da construção de pontes de transição entre o ecossistema constitucional estatal e a governança interna de plataformas digitais, promovendo a constitucionalização desta em referência direta àquele. Veja-se, assim, que o constitucionalismo estatal segue sendo um importante ponto de referência para o constitucionalismo digital.

Um exemplo de como isso se dá na prática é a moderação em plataformas digitais, em especial redes sociais. Essas empresas controlam o

---

32 CELESTE, Edorado. **Digital Constitutionalism**: The role of Internet Bills of Rights. Nova Iorque: Routledge, 2023, p. 82.

33 ARCHEGAS, João Victor. **Constitucionalismo Digital**: Limites constitucionais na nova fronteira do poder. Belo Horizonte: Fórum, 2025, p. 148.

34 *Ibidem*, p. 61.

comportamento e o discurso de bilhões de usuários ao redor do mundo, impactando diretamente o exercício de seus direitos fundamentais. Assim, é importante que a moderação se dê de forma transparente e racional, oferecendo um sistema de proteção ao invés de violação de direitos. Para isso acontecer, entretanto, é importante que a governança digital esteja alinhada a alguns preceitos do constitucionalismo moderno, como a separação de poderes. É isso, por exemplo, que o Oversight Board da Meta oferece ao Instagram e Facebook: "uma tentativa de institucionalizar um espaço autônomo e independente de dissenso interno [...] capaz de criar uma atmosfera de accountability e responsabilidade em relação ao conteúdo e comportamento dos seus usuário"[35].

Atuando como uma espécie de "suprema corte" para a moderação nas plataformas da Meta, o Board é uma instituição independente que decide casos de moderação em última instância e de forma vinculante, levando em consideração não apenas as regras e princípios da empresa como também o Direito Internacional dos Direitos Humanos. Embora seja um passo na direção correta, o modelo do Oversight Board pode e deve ser aprimorado, servindo até mesmo de referência para outros arranjos regulatórios. É possível pensar, por exemplo, em uma espécie de Oversight Board criado pelo Estado e gerido de forma multissetorial que possa servir de ponte de transição entre o constitucionalismo estatal e a governança interna de grandes plataformas digitais, sempre a partir de uma perspectiva de corregulação.

4. Conclusão

A partir das discussões apresentadas, fica evidente que plataformas digitais e grandes empresas de tecnologias – responsáveis, por sua vez, pelas principais inovações disruptivas da era digital – exercem um poder significativo sobre a esfera pública, muitas vezes rivalizando ou até ultrapassando o poder estatal. Essa realidade exige uma nova abor-

35 *Ibidem*, p. 161.

dagem regulatória, na qual Estado e plataformas colaboram para estabelecer regras claras e eficazes, de modo a preservar os direitos fundamentais e evitar que o poder privado seja exercido de maneira arbitrária. O constitucionalismo digital oferece um referencial teórico valioso para enfrentar esses desafios, propondo a generalização e reespecificação de mecanismos constitucionais para a governança interna destas empresas.

A corregulação, como vimos, emerge como um modelo mais adequado para essa nova realidade. Ao invés de uma regulação unilateral ou autorregulação total, o modelo híbrido proposto pelo constitucionalismo digital permite que o poder estatal e o privado se complementem, criando um ambiente onde decisões de moderação de conteúdo, por exemplo, são feitas de forma transparente e responsável. Exemplos como o Oversight Board mostram o potencial de mecanismos que, ao internalizarem valores constitucionais, podem mitigar riscos e assegurar a proteção de direitos fundamentais.

Contudo, o caminho para uma verdadeira constitucionalização da governança digital ainda está em construção e deve ser aprimorado de maneira contínua. É necessário avançar para soluções mais robustas e permanentes, que promovam maior accountability e independência na moderação de conteúdo e no desenvolvimento de tecnologias como a inteligência artificial. Só assim será possível garantir que o poder exercido pelas plataformas digitais e grandes empresas de tecnologia em geral esteja alinhado com os princípios democráticos e constitucionais, preservando o potencial positivo da tecnologia enquanto se minimizam suas externalidades negativas. Esse é o caminho para que inovações disruptivas sirvam de instrumentos para a consolidação da democracia na era digital.

João Victor Archegas · Professor de Direito na FAE e Coordenador no Instituto de Tecnologia e Sociedade do Rio de Janeiro (ITS Rio). Mestre e Bacharel em Direito pela Universidade Federal do Paraná (UFPR). *Master of Laws* pela Harvard Law School, onde foi Gammon Fellow de excelência acadêmica. E-mail para contato: j.archegas@itsrio.org

A desinformação como risco global: a contribuição do Brasil para o debate da regulação da Inteligência Artificial

Eleonora Mesquita Ceia
Fernanda Paes Leme Peyneau Rito

Resumo

A liberdade de informação é inerente à democracia, como valor que assegura a participação ativa e consciente do cidadão no processo político. Assim, qualquer estratégia de disseminação de conteúdos intencionalmente falsos como parte de uma agenda política é atentatória contra a democracia. Na última década emergiu internacionalmente uma relação entre movimentos/governos de extrema direita e estratégias/políticas de desinformação nas redes sociais. Mediante o uso da Inteligência Artificial (IA) propagam conteúdos anticientíficos, conspiratórios, discriminatórios e de ódio, de forma a manipular a opinião pública e acentuar a polarização política. O Fórum Econômico Mundial de 2024 elegeu a desinformação como o risco global a ser enfrentado prioritariamente pela comunidade internacional, diante dos riscos à estabilidade internacional e democracia inerentes ao fenômeno. A desinformação constituiu instrumento oficial da política do governo do ex-presidente Jair Bolsonaro, gerando danos e ameaças graves à saúde pública e democracia brasileira. Após essa experiência, medidas legislativas, como o Projeto de Lei nº 2338/2023 que institui o Marco legal da IA, foram

formuladas para conter a desinformação como fenômeno ainda presente na sociedade brasileira, sobretudo em razão da atuação da extrema direita nas redes sociais. A partir do levantamento e análise das propostas de regulação da IA e os posicionamentos do governo brasileiro em fóruns internacionais, a pesquisa busca avaliar como o caso brasileiro pode contribuir para o debate da regulação da IA, no qual a preocupação com restrições excessivas à liberdade de expressão, inovação e ao desenvolvimento socioeconômico é central.

Abstract

Freedom of information is inherent to democracy, as a value that ensures the active and conscious participation of citizens in the political process. Therefore, any strategy of disseminating intentionally false content as part of a political agenda is an attack on democracy. In the last decade, a relationship has emerged internationally between extreme right-wing movements/governments and disinformation strategies/policies on social media. Through the use of Artificial Intelligence (AI) they propagate anti-scientific, conspiratorial, discriminatory and hateful content in order to manipulate public opinion and accentuate political polarization. The 2024 World Economic Forum chose disinformation as the global risk to be faced as a priority by the international community, given the risks to international stability and democracy inherent in the phenomenon. Disinformation was an official policy instrument of former president Jair Bolsonaro's government, generating serious damage and threats to public health and Brazilian democracy. Following this experience, legislative measures, such as Bill 2338/2023 establishing the Legal Framework for AI, were formulated to contain disinformation as a phenomenon still present in Brazilian society, especially due to the actions of the extreme right on social networks. Based on a survey and analysis of AI regulation proposals and the Brazilian government's positions in international forums, the research seeks to assess how the Brazilian case can contribute to the AI regulation debate, in which concern about ex-

cessive restrictions on freedom of expression, innovation and socio-economic development is central.

1. Introdução

A Inteligência Artificial (IA) consiste em uma tecnologia integrada por máquinas virtuais capazes de oferecer uma vasta gama de modalidades de processamento de informações, por meio de aprendizagem, que engloba classificações, previsões e tomada de decisões. A IA pode ser utilizada, idealmente, para duas finalidades principais: uma de cunho tecnológico, quando computadores são usados de forma útil em aplicações práticas de vários setores do cotidiano; e outra de cunho científico, quando modelos e abordagens de IA são utilizados para responder a questões centrais relacionadas ao comportamento e à vida humana[1].

Contudo, nesses potenciais usos é preciso considerar os riscos inerentes ao manejo humano de qualquer tecnologia. É o que E. M. Foster já alertava em sua ficção "A Máquina Parou", escrita em 1909, sobre a relação entre humanidade e tecnologia: a mesma máquina que serve aos humanos, pode passar a controlá-los, em virtude da crescente dependência tecnológica dos indivíduos[2]. De forma mais pessimista, o mesmo alerta recai sobre o entusiasmo irresistível de cientistas – como os descritos por Benjamín Labatut no seu romance "MANIAC", entre eles, John

1 BODEN, Margaret A. **Inteligência Artificial**: uma brevíssima introdução. São Paulo: Unesp, 2020, p. 14-19.

2 "O tempo passou e as pessoas não mais percebiam o defeito. As falhas não haviam sido sanadas mas os tecidos humanos, naqueles dias, tornaram-se tão subservientes que se adaptavam com rapidez aos caprichos da Máquina. [...] Mas chegou o dia em que, sem o menor aviso prévio, sem qualquer indício de fraqueza anterior, todo o sistema de comunicação parou, no mundo todo. E o mundo, tal como era conhecido, acabou". FOSTER, E. M. **A Máquina Parou**. São Paulo: Iluminuras, 2018, p. 56-58.

von Neumann – com o "progresso" proporcionado pela tecnologia, que tem a aptidão de gerar destruição[3].

Na última década emergiu internacionalmente uma relação entre movimentos/governos de extrema direita e estratégias/políticas de desinformação[4] nas redes sociais[5], que se tornaram o ambiente ideal para a formação de "bolhas". Nestas predominam a falta de pluralismo e imparcialidade e, por consequência, a desinformação e a polarização se amplificam, em razão da forma como os algoritmos ali operam, prevendo e determinando o comportamento dos usuários[6]. Mediante o uso da IA são propagados em tais bolhas conteúdos anticientíficos, conspiratórios, discriminatórios e de ódio, de forma a manipular a opinião pública e acentuar a polarização política. Diante disso, o Fórum Econômico Mundial de 2024 elegeu a desinformação como o risco glo-

3 John von Neumann foi o matemático húngaro, inventor do computador moderno, quem teve participação central no desenvolvimento da bomba atômica no âmbito do Projeto Manhattan. O romance de Labatut narra o conteúdo da última carta de von Neumann antes de sua morte a um amigo: "O progresso se tornará incompreensivelmente rápido e complicado. O poder tecnológico em si é sempre uma conquista ambivalente e a ciência é neutra em todo o processo, fornecendo apenas meios de controle aplicáveis a qualquer propósito e indiferente a todos. Não é a destrutividade particularmente perversa de uma invenção específica que cria o perigo. O perigo é intrínseco. Para o progresso não há cura". LABATUT, Benjamín. **MANIAC**. São Paulo: Todavia, 2023, p. 256.

4 A desinformação pode ser explicada como uma estratégia pela qual conteúdo falsos, distorcidos ou incompletos são massiva e deliberadamente difundidos na internet e mídias sociais, para enganar ou manipular os usuários. Tais conteúdos podem integrar campanhas estatais ou agendas políticas internas baseadas em viés ideológico específico, que podem prejudicar a democracia. JAYAKUMAR, S., ANG, B., ANWAR, N.D., **Disinformation and Fake News**, Palgrave Macmillan, Singapore, 2021, p. 7.

5 BARROSO, Luís Roberto; BARROSO, Luna van Brussel. Democracia, mídias sociais e liberdade de expressão: ódio, mentiras e a busca da verdade possível. **Direitos Fundamentais & Justiça**, Belo Horizonte, ano 17, n. 49, 2023, p. 288.

6 LONGO, Erik. The Risks of Social Media Platforms for Democracy: A Call for a New Regulation. In: CUSTERS, Bart; FOSCH-VILLARONGA, Eduard (Eds.). **Law and Artificial Intelligence**. Berlin/Heidelberg: ASSER Press; Springer, 2022, p. 176-177.

bal a ser enfrentado prioritariamente pela comunidade internacional, diante dos riscos à estabilidade internacional e democracia intrínsecos ao fenômeno.

A desinformação constituiu instrumento oficial da política do governo do ex-presidente Jair Bolsonaro, gerando danos e ameaças graves à saúde pública e democracia brasileira[7]. Após essa experiência, medidas legislativas, como o Projeto de Lei 2.338/2023 que institui o Marco Legal da IA, foram formuladas para conter a desinformação como fenômeno ainda presente na sociedade brasileira, sobretudo em razão da atuação da extrema direita nas redes sociais.

A partir do levantamento e análise das propostas de regulação da IA e os posicionamentos do governo brasileiro em fóruns internacionais, a pesquisa busca avaliar como o caso brasileiro pode contribuir para o debate da regulação da IA, no qual a preocupação com restrições excessivas à liberdade de expressão, inovação e ao desenvolvimento socioeconômico é central.

Após essa introdução, o artigo inicia o desenvolvimento do tema, apresentando o contexto internacional em que a desinformação foi elencada como risco global e as razões para tanto. Em seguida, examina as abordagens nacional e internacional de regulação da IA. No Brasil, destaca os debates no Congresso Nacional sobre a regulação da IA, notadamente no que se refere à proteção de direitos no uso de IA generativa e ao combate à desinformação. No plano internacional, explora o conteúdo e os debates em torno da adoção da Resolução 78/L.49 da ONU de março de 2024, com ênfase na participação brasileira nos principais fóruns internacionais. O artigo conclui ressaltando como o Brasil pode contribuir para o debate global acerca dos riscos e potenciais da IA no contexto de combate à desinformação.

---

7 ARTIGO 19. **Relatório Global de Expressão 2020/2021**: o estágio da liberdade de expressão ao redor do mundo, 2021, p. 23-27. Disponível em: https://artigo19.org/2021/07/29/relatorio-global-de-liberdade-de-expressao-2020-2021/ Acesso em: 8 out. 2024.

2. Democracia, desinformação e risco global

A liberdade de informação é inerente à democracia, como valor que assegura a participação ativa e consciente do cidadão no processo político. Assim, qualquer estratégia de disseminação de conteúdos intencionalmente falsos, negacionismos e conspirações, como parte de uma agenda política é atentatória contra a democracia.

Nessa perspectiva, o potencial da IA como recurso gerador de desinformação, ganhou notoriedade nos principais fóruns internacionais, dentre eles o Fórum Econômico Mundial de 2024, que elegeu a desinformação como o principal risco global no curto prazo (2 anos).

Com a popularização do uso doméstico da internet e o papel central que as plataformas digitais assumiram na vida social, emergiram a preocupação e discussões sobre os impactos da virtualização da vida na democracia e no exercício da cidadania. Desde o acesso efetivo à internet até a garantia de espaços digitais neutros, plurais e democráticos, incluindo o acesso a informações verdadeiras, o que se percebe é que não fomos capazes de garantir a universalização do acesso nem de consolidar os pilares básicos de uma democracia no ambiente digital.

Dada a capilaridade das redes sociais, além de não termos assegurado uma democracia cibernética, o uso da internet, por meio dessas plataformas, redes sociais e demais ferramentas, impacta negativamente, colocando em risco, a democracia real, ao invés de fortalecê-la.

A Declaração Universal da Democracia, assinada em 1997 por representantes de 128 países, dentre eles, o Brasil, define democracia como um "direito básico de cidadania, a ser exercido em condições de liberdade, igualdade, transparência e responsabilidade, com o devido respeito à pluralidade de pontos de vista, no interesse da comunidade"[8].

8 SENADO FEDERAL. Declaração Universal da Democracia. 1997. Disponível em: https://www2.senado.leg.br/bdsf/bitstream/handle/id/243080/000954851.pdf?sequence=1&isAllowed=y Acesso em: 20 out. 2024.

Transportando esse conceito para a realidade criada pela internet, impositivo pensar em democracia cibernética, aqui compreendida como a ampliação dos princípios e mecanismos democráticos tradicionais para o ambiente digital a partir da utilização das tecnologias disponíveis para aumentar a participação cidadã nos processos políticos e na deliberação pública.

Em um primeiro momento, até se imaginou que a tecnologia e a internet fossem potencializar a participação social no processo democrático e no debate público, na medida em que o cidadão se tornaria um sujeito ativo com poderes para colaborar e exigir, por meio das mídias digitais. Mas, essa alteração do *locus* para o exercício da cidadania trouxe dilemas e desafios novos, aqui sistematizados em três grupos: i) inclusão digital; ii) pluralidade e liberdade; iii) veracidade e qualidade informacional.

Esses três grupos de desafios estão interligados e, em muitos casos, se sobrepõem. E, embora não haja uma sequência temporal específica para cada um deles, inegável que afetam diretamente o direito humano e fundamental do acesso à internet[9] e o pleno exercício da cidadania.

O primeiro desafio enfrentado na construção de uma democracia cibernética foi a inclusão digital, que abrange, no mínimo, tanto o acesso à internet quanto o letramento digital. No Brasil, houve avanços significativos em ambas as áreas nos últimos anos. De acordo com dados do IBGE, em 2023, cerca de 72,5 milhões de domicílios brasileiros (92,5% do total de domicílios) tinham acesso à internet[10]. Não obstante a inegável ampliação do acesso, dentre aqueles domicílios que não pos-

9 Na esfera internacional, dentre outros documentos, cita-se o reconhecimento do acesso à internet como direito humano fundamental, nos seguintes documentos da ONU: Resolução A/HRC/17/27, de 2011; Resolução A/HRC/20/L.1331, de 2012; Resolução A/RES/68/167, de 2013; *General Conference* 38 C/53, de 2015; Resolução A/HRC/32/L.20, de 2016.

10 IBGE. Pesquisa Nacional por Amostra de Domicílios (Pnad) Contínua Tecnologia da Informação e Comunicação (TIC), 2023. Disponível em: https://painel.ibge.gov.br/pnadc/ Acesso em: 20 out. 2024.

suem conexão, o principal motivo indicado foi a falta de conhecimento dos moradores sobre como usar a internet (33,2%), seguido do custo financeiro (30%) e da percepção de que não há necessidade de acesso (23,4%).

Os dados indicam que ainda há que se evoluir no sentido de excluir a barreira financeira para o acesso e, principalmente concretizar o letramento digital, ou seja, a capacidade de utilizar as tecnologias digitais de forma crítica e eficaz, inclusive para que as pessoas compreendam as possibilidades de uso da rede para acesso a bens e serviços.

O letramento digital foi incluído na Base Nacional Comum Curricular (BNCC)[11], documento normativo que define os direitos de aprendizagem essenciais para os estudantes da educação básica no Brasil, abrangendo a educação infantil, o ensino fundamental e o ensino médio[12]. Da mesma forma, as diretrizes curriculares nacionais para o ensino superior também incorporaram o letramento digital como competência a ser desenvolvida. Claro que existe um hiato considerável entre a previsão normativa do letramento digital e a sua efetiva concretização, mas a iniciativa é positiva e condizente com a indiscutível necessidade de enfrentamento do primeiro grupo de desafios, a inclusão digital.

Paralelamente, um segundo grupo de desafios a ser enfrentado na construção de uma democracia cibernética, é garantir a pluralidade e a liberdade na rede. Como já referido, as redes sociais se tornaram um

11 O Artigo 26 da Lei de Diretrizes e Bases da Educação Nacional (LDB), Lei nº 9.394/1996, prevê a necessidade de uma base comum nacional para o currículo da educação básica. No entanto, a BNCC propriamente dita foi instituída e regulamentada pelo Ministério da Educação (MEC), por meio da Resolução CNE/CP nº 2/2017, para a educação infantil e o ensino fundamental, e pela Resolução CNE/CP nº 4/2018, para o ensino médio.

12 Nesse sentido, foi incluída na BNCC, a competência geral 5, estabelecendo que os discentes devem ser capazes de "compreender, utilizar e criar tecnologias digitais de informação e comunicação de forma crítica, significativa, reflexiva e ética nas diversas práticas sociais (incluindo as escolares), para se comunicar, acessar e disseminar informações, produzir conhecimentos, resolver problemas e exercer protagonismo e autoria na vida pessoal e coletiva".

ambiente ideal para formação de "bolhas", indicando que, ao contrário do que projetado inicialmente, a internet não se revelou um ambiente plural, livre ou democrático por si só. Isto em razão e a despeito do acesso, mas como consequência do próprio uso que é influenciado por ações algorítmicas enviesadas.

As redes sociais desempenham um papel central no acesso à informação na sociedade contemporânea, principalmente em democracias jovens como a brasileira. No entanto, a informação é controlada e direcionada por um viés algorítmico, que determina o que os usuários veem. Os algoritmos são desenhados para maximizar o engajamento do usuário, de sorte que esse processo pode priorizar informações sem qualquer compromisso com a veracidade e a pluralidade. Consequentemente, restringem o próprio acesso à informação, através da criação de bolhas de filtragem e da ampliação da própria desinformação.

Como os algoritmos são desenhados visando o engajamento do usuário, são estruturados a partir das preferências do próprio usuário, identificadas a partir das pegadas digitais. Significa dizer que, sendo o engajamento o propósito, o algoritmo mostra, para cada um dos usuários, conteúdos que reforçam as opiniões já demonstradas, ocultando ou diminuindo a exposição a perspectivas distintas. Cria-se uma câmara de eco, nas quais os usuários são expostos repetidamente a conteúdos que reforçam suas opiniões preexistentes, ao invés de oferecerem uma visão equilibrada e diversificada. Esse fenômeno leva à primeira onda de desinformação: a disseminação de informações manipuladas ou incompletas, o que afeta diretamente a capacidade de os cidadãos tomarem decisões informadas e exercerem seus direitos plenamente.

Decisões e exercício de direitos são diretamente influenciados pelo conjunto informacional disponível. Assim, as bolhas de filtragem e a ampliação da desinformação, impactam diretamente na liberdade, ressonando para todas as searas da vida, no desenvolvimento da personalidade de cada um e na construção dos espaços públicos.

O terceiro grupo de desafios para a construção de uma democracia cibernética e para o exercício da própria cidadania, é a desinforma-

ção, maior risco global atual, segundo o Relatório de Riscos Globais do Fórum Econômico Mundial de 2024[13].

Por risco global compreende-se a possibilidade de ocorrência de determinado evento ou condição com impacto significativo no produto interno bruto global, nas populações ou nos recursos naturais. A desinformação ocupa o primeiro lugar no ranking dos riscos globais no curto prazo (2 anos) e a quinta posição no horizonte de longo prazo (10 anos). A desinformação engloba a falta de informação em si e, também, a disseminação de informações falsas, com o potencial de amplificar a polarização social (3º risco global no curto prazo e 9º risco global no longo prazo), impactando direitos humanos, saúde pública e desenvolvimento social.

A desinformação foi incluída no grupo de riscos tecnológicos. Assim, para além dos resultados adversos dos usos da tecnologia que, indiscutivelmente, incluiria a desinformação, esta foi eleita autonomamente como risco global. A sua posição em primeiro lugar no ranking de curto prazo está diretamente relacionada aos processos eleitorais relevantes nesse período, como a eleição presidencial no Estados Unidos em novembro de 2024. Mas, para além do recorte temporal, a sua persistência no ranking e, mais do que isso, as inter-relações entre diferentes riscos, evidenciam o seu potencial negativo, incluindo os riscos derivados da censura e vigilância.

Além do impacto imediato, a desinformação alimenta a polarização social, que ocupa a terceira posição no ranking de curto prazo e a nona posição no ranking de longo prazo dos riscos globais. A desinformação, opera decisivamente nas percepções da realidade que, distorcidas intencionalmente ou não, tendem a se tornar mais polarizadas, influenciando narrativas e discursos públicos em questões diversas que vão desde a saúde pública, como se observou durante a pandemia do COVID-19, até

13 WORLD ECONOMIC FORUM. **Global Risks Report 2024**. Disponível em: https://www.weforum.org/publications/global-risks-report-2024/ Acesso em: 20 out. 2024.

a justiça social. Isso cria um risco de monopólio da verdade e silenciamento das vozes das minorias, gerando uma opacidade prejudicial ao diálogo democrático.

Esse cenário, inexoravelmente, nos impõe a reflexão e urgência na regulação da IA, não apenas com um olhar para eventual e inafastável momento patológico, mas essencialmente para o delineamento dos contornos necessários para o uso e desenvolvimento dessa tecnologia em prol dos interesses democráticos.

3. O caso brasileiro de regulação da IA

Nos últimos anos são identificados três momentos da disseminação de desinformação no Brasil: as eleições presidenciais de 2018, que devido à combinação do uso massivo do WhatsApp e do cenário de polarização política, foi o primeiro momento ideal para a difusão digital de notícias falsas no país; a pandemia da COVID-19, cujos efeitos foram manejados desde o início pelo governo Bolsonaro mediante negacionismo e desinformação; e as eleições presidenciais de 2022, marcadas pela disseminação de conteúdos falsos com recurso de IA, como o *deep fake*[14].

As campanhas digitais persistentes de desinformação conjugada com a violência política do bolsonarismo foram determinantes para no início de 2023 se resgatar a discussão do Projeto de Lei nº 2.630, proposto em 2020 pelo Senador Alessandro Vieira[15]. O Projeto prevê a "Lei Brasileira de Liberdade, Responsabilidade e Transparência na Internet", que inclui regras básicas para a moderação do conteúdo nas redes sociais. Vale dizer, regras para retirar e limitar a circulação de conteúdo

14 ZEITEL, Gustavo. Como deepfakes assombram eleições e pavimentam o futuro da arte. **Folha de São Paulo**. 22 de outubro de 2022. Disponível em: https://www1.folha.uol.com.br/ilustrada/2022/10/como-deepfakes-assombram-eleicoes-e-pavimentam-o-futuro-da-arte.shtml Acesso em: 18 out. 2024.

15 SENADO FEDERAL. **Projeto de Lei nº 2.630, de 2020** (Lei das Fake News). Disponível em: https://www25.senado.leg.br/web/atividade/materias/-/materia/141944 Acesso em: 10 out. 2024.

considerados desinformativos, assegurado o direito de recurso e contraditório aos usuários.

Atualmente, conforme o artigo 19 do Marco Civil da Internet (Lei nº 12.965/2014), a plataforma digital é obrigada a retirar um conteúdo infringente somente quando receber uma ordem judicial para fazê-lo[16]. Inclusive este dispositivo respaldou a decisão do Ministro Alexandre de Moraes, do Supremo Tribunal Federal (STF), no final de agosto de 2024, de suspender o funcionamento da plataforma "X" no Brasil[17]. O Projeto de Lei nº 2.630/2020 pretende modificar tal regra ao estipular deveres às plataformas com relação à moderação do conteúdo, por exemplo, o de identificar e excluir conteúdo considerado desinformativo, bem como o de se submeter a uma auditoria externa.

16 Exceções a essa regra geral do artigo 19 são os casos de violação de direitos autorais e de violação à intimidade mediante a exploração de imagens íntimas ("pornografia de vingança"), em que basta a notificação extrajudicial para gerar a responsabilidade de retirada do conteúdo pela plataforma. Ver BRASIL. Lei nº 12.965 de 23 de abril de 2014, que estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm Acesso em: 15 out. 2024.

17 Em sua decisão o Ministro fundamenta a suspensão do "X" em razão do descumprimento de ordens judiciais anteriores, que determinavam a empresa bloquear contas/perfis e a respectiva monetização de determinados usuários que vinham atuando ilicitamente na plataforma. A situação se agrava quando há a evasão dos representantes legais da empresa do país e o próprio Elon Musk declara que manteria o descumprimento das decisões judiciais. Com base no artigo 19 do Marco Civil da Internet, o Ministro declara que esta Lei "prevê a responsabilização civil do provedor de aplicações de internet por danos decorrentes de conteúdo gerado por terceiros e apontado como infringente, caso não sejam realizadas as medidas determinadas por ordem judicial dentro do prazo assinalado e nos limites técnicos do serviço." Ver STF. Supremo Tribunal Federal. **Petição 12.404/DF**, Relator Ministro Alexandre de Moraes, 30 de agosto de 2024, p. 8-9. Disponível em: noticias-stf-wp-prd.s3.sa-east-1.amazonaws.com/wp-content/uploads/wpallimport/uploads/2024/08/30171714/PET-12404-Assinada.pdf Acesso em: 19 out. 2024. Em 8 de outubro de 2024, o Ministro determinou o desbloqueio da plataforma no Brasil, em razão do pagamento pela empresa de mais de R$ 28 milhões em multas pelo descumprimento das ordens judiciais.

O Projeto sofreu críticas por propor novas regras que alegadamente violariam a liberdade de expressão, sobretudo a definição da autoridade responsável por fiscalizar a aplicação da Lei e, em caso de descumprimento, por impor sanções às plataformas[18]. Da mesma forma, enfrentou forte campanha contrária promovida por empresas de tecnologia – como a Google e o Telegram –, que culminou na retirada do Projeto de votação pelo Presidente da Câmara dos Deputados em maio de 2023.

Devido ao fracasso do Projeto de Lei nº 2.630/2020, o Tribunal Superior Eleitoral (TSE) emitiu a Resolução nº 23.732/2024[19], com o objetivo de combater a desinformação nas eleições municipais do mesmo ano. A Resolução do TSE avançou no tema do uso regulado da IA no âmbito eleitoral, estabelecendo, por um lado, que os candidatos podem utilizar IA, desde que informem com clareza aos eleitores sobre o uso da tecnologia. Por outro, a norma impõe a anulação do registro da candidatura e do mandato aos candidatos que utilizem IA, inclusive *deep fakes*, para difamar seus adversários ou o sistema eleitoral.

Para além do impacto dos usos da IA como recurso de desinformação que impacta negativamente a democracia, recebeu atenção nos debates sobre a regulação da tecnologia no Brasil, a proteção de direitos fundamentais, sobretudo da privacidade. Em razão do avanço tecnológico, marcado por novas formas de coleta e tratamento automatizado de informações, a interpretação do conteúdo do direito à privacidade foi ampliada, passando a abarcar a proteção de dados pessoais, isto é, o direito do indivíduo de "controlar o uso das informações que lhe dizem respeito"[20].

---

18 BARROSO; BARROSO, op. cit., p. 306.

19 TSE. Tribunal Superior Eleitoral. **Resolução nº 23.732, de 27 de fevereiro de 2024**, que altera a Resolução TSE nº 23.610 de dezembro de 2019, dispondo sobre a propaganda eleitoral. Disponível em: https://www.tse.jus.br/legislacao/compilada/res/2024/resolucao-no-23-732-de-27-de-fevereiro-de-2024 Acesso em: 10 out. 2024.

20 RODOTÀ, Stefano. **A vida na sociedade da vigilância**: a privacidade hoje. Rio de Janeiro: Renovar, 2008, p. 24-25.

Zuboff explica que o incremento da internet e das novas tecnologias trouxe consigo uma promessa de emancipação em nome da autodeterminação do indivíduo. Porém, tal expectativa não foi atendida, em virtude de o crescimento digital vir acompanhado da consolidação da ordem neoliberal, que gerou maior desigualdade e crise democrática. Vale dizer, as instituições defendem a primazia da agenda de desregulação do livre mercado às custas da realização de direitos fundamentais. Como resultado, os indivíduos ávidos por autodeterminação, no que se refere as suas preferências, liberdades e interesses, não encontram as condições materiais para concretizá-la, dada à ordem econômica excludente[21].

Nesse cenário, emerge o chamado capitalismo de vigilância. No início dos anos 2000, empresas de tecnologia, como, por exemplo a Google, representante desse novo capitalismo digital, passa a cometer abusos e violações contra a privacidade dos seus usuários, em busca de dados comportamentais, para a auferição de lucro. Nossos dados tornam-se a matéria-prima necessária para os processos de produção do capitalismo de vigilância, nos quais a IA exerce um papel central: "essas operações de inteligência de máquina convertem matéria-prima nos altamente lucrativos produtos algorítmicos criados para predizer o comportamento dos usuários"[22].

A maior parte das aplicações atuais de modelos de IA segue a técnica de aprendizado de máquina, que se divide em dois tipos: IA preditiva e IA generativa. Essa técnica está sujeita a uma série de dificuldades: incertezas próprias de todo modelo estatístico de probabilidade; externalidades, como, por exemplo, bases de dados enviesadas e a subjetividade humana que interfere no processo de interpretação de resultados; e o problema da "opacidade", isto é, a falta de transparência em virtude da alta complexidade que envolve as operações desenvolvidas pelos algo-

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

22 Ibid.

ritmos de IA[23]. Essas dificuldades representam sérias ameaças ao direito fundamental à privacidade e ao princípio da não discriminação no âmbito das variadas implementações práticas da IA[24].

Em razão disso, surgiram iniciativas de autorregulação, que por conta da sua própria natureza se mostraram pouco eficientes[25] e propostas de regulação estatal. Estas últimas enfrentam resistências e desafios[26]. A nova lógica de acumulação sob o capitalismo de vigilância é protegida por sigilo e expertise, como também por estratégias políticas e econômicas, dentre as quais se destaca a desregulação. As empresas de tecnologia fundamentam sua aversão à regulação do cyberespaço, com base na incapacidade do Estado de acompanhar o avanço tecnológico promovido por elas e na crença de que a regulação obstaria a inovação e progresso. No entanto, um espaço sem regulação é mais vulnerável a abusos e ganâncias. Com efeito, "essa falta de legislação tem sido uma fator crítico do sucesso do capitalismo de vigilância em sua breve história"[27].

No Congresso Nacional está em debate o Projeto de Lei nº 2.338/2023, de autoria do Senador Rodrigo Pacheco, que propõe regular os usos de IA no país[28]. A proposta adota o modelo de regulação baseada

---

23 "Isso acontece porque a análise de dados realizada por algoritmos ocorre por meio de códigos, que, embora sejam desenvolvidos por humanos, são difíceis de controlar pelos próprios programadores, uma vez colocados em operação". Tradução livre das autoras do original: "This happens because the data analysis made upstream through predictive algorithms takes place through codes that, despite being written by humans, are difficult to control by the creators themselves once put into operation". Ver LONGO, op. cit., p. 177.

24 KAUFMAN, Dora; JUNQUILHO, Tainá; REIS, Priscila. Externalidades negativas da inteligência artificial: conflitos entre limites da técnica e dos direitos humanos. **Revista Direitos e Garantias Fundamentais**, v. 24, n. 3, 2023, p. 45.

25 Ibid., p. 46.

26 RODOTÀ, op. cit., p. 51.

27 ZUBOFF, op. cit.

28 SENADO FEDERAL. **Projeto de Lei nº 2.338, de 2023**. Disponível em: https://www25.senado.leg.br/web/atividade/materias/-/materia/157233 Acesso em: 18. out. 2024.

na categorização de risco. Nele é estabelecido o grau dos riscos inerentes aos diferentes usos da IA, a saber: i) riscos inaceitáveis, em que são vedados a implementação e o uso de sistema de IA; ii) altos riscos, que podem ser assumidos mediante o cumprimento de exigências impostas pela lei e os agentes se sujeitam ao regime de responsabilidade objetiva pelo dano causado (são os usos da IA para os fins de segurança pública, educação, administração da justiça e saúde, entre outros); e iii) os demais riscos, que podem ser assumidos mediante o cumprimento de exigências legais, menos rígidas que as aplicadas para os casos de alto risco, e os agentes se sujeitam ao regime de responsabilidade subjetiva[29].

O Projeto é bastante extenso no que tange às obrigações estabelecidas aos agentes da cadeia de produção (fornecedor, aplicador e distribuidor). São, ao total, 57 obrigações direcionadas solidariamente entre os três agentes. Prevê também deveres específicos para usos de IA no setor público[30].

O PL 2.338/2023 prevê ainda o direito da pessoa à explicação sobre decisões tomadas por sistemas de IA, com fundamento no princípio da transparência e do devido processo legal. Contudo, a efetividade do direito à explicação é atualmente submetido a sérias restrições. A primeira é determinada pela Lei Geral de Proteção de Dados (LGPD), a Lei nº 13.853/2019, que condiciona o direito à revisão das decisões tomadas unicamente com base no tratamento automatizado de dados pessoais ao resguardo dos segredos comercial e industrial. A segunda restrição é o problema da opacidade, já apontado acima, derivado da alta complexidade e abstração própria das operações desenvolvidas por algoritmos

29 FRAZÃO, Ana. Classificação de riscos: a solução adotada pelo PL2338/23. Jota. 4 de abril de 2024. Disponível em: https://www.jota.info/opiniao-e-analise/colunas/ia-regulacao-democracia/classificacao-de-riscos-a-solucao-adotada-pelo-pl-2338-23 Acesso em: 20 out. 2024.

30 ITS. Instituto de Tecnologia & Sociedade do Rio. **Matriz comparada de obrigações: PL 2338/2023 vs. EU AI act**. 16 de agosto de 2024. Disponível em: https://itsrio.org/pt/publicacoes/relatorio-matriz-comparada-de-obrigacoes-pl-2338-2023-vs-eu-ai-act-2/ Acesso em: 18 out. 2024.

de IA, que dificulta a transparência algorítmica e, por consequência, a efetividade do direito à explicação[31].

4. A posição do Brasil na agenda global de proteção da integridade da informação

Em julho de 2024, o Conselho Nacional de Ciência e Tecnologia, órgão de assessoramento da Presidência da República, cuja composição conta com a participação da sociedade civil, lançou a Proposta de Plano Brasileiro de IA 2024-2028, "IA para o bem de todos". Com o orçamento previsto de R$ 23,03 bilhões, a Proposta é baseada nos pilares da inclusão, infraestrutura, soberania tecnológica e de dados, capacitação de pessoas e apoio ao processo regulatório em IA. O documento considera a IA uma "ferramenta capaz de alavancar o desenvolvimento social e econômico do Brasil" e, sob esse olhar, ressalta a importância do país garantir sua independência tecnológica e, por isso, busca promover o protagonismo global do Brasil no assunto e a cooperação internacional em pesquisa e desenvolvimento em IA com países da América Latina e do Caribe[32].

O tema da relação entre informação e democracia não é novo na agenda internacional. Porém, desde a emergência da infodemia no contexto da pandemia da COVID-19[33] e o avanço do negacionismo climático, a discussão sobre integridade da informação vem ganhando cada vez mais destaque no âmbito da ONU[34]. Conforme a Organização, o ter-

31 KAUFMAN, op. cit., p. 50-52.

32 BRASIL. Ministério da Ciência, Tecnologia e Inovação. **IA para o Bem de Todos**. 2024. Disponível em: https://www.gov.br/mcti/pt-br/acompanhe-o-mcti/cct/legislacao/arquivos/IA_para_o_Bem_de_Todos.pdf Acesso em: 8 out. 2024.

33 ARTIGO 19. **Infodemia e COVID-19**: a informação como instrumento contra os mitos. 2021. Disponível em: https://artigo19.org/wp-content/blogs.dir/24/files/2021/05/Infodemia-e-a-COVID-19-%E2%80%93-A-informacao-como-instrumento-contra-os-mitos.pdf Acesso em: 8 out. 2024.

34 Em junho de 2024, a ONU lançou os "Princípios Globais para a Integridade da Informação", que consideram os riscos oriundos do avanço da IA e englobam

mo integridade da informação diz respeito à garantia da circulação de informações precisas e confiáveis, que resta ameaçada atualmente pelo risco global da desinformação, potencializada pelos modelos de IA generativa[35]. A mesma definição é utilizada em documentos do governo brasileiro[36].

A partir da própria experiência recente do Brasil, de ataques à democracia fomentados por campanhas digitais de desinformação contra a credibilidade do voto eletrônico, o Presidente Luís Inácio Lula da Silva, desde o início do seu governo, em 2023, tem sido uma voz constante a favor da formulação de respostas globais contra a desinformação[37]. Embora a ONU, desde 2018, já contasse com programas relacionados à garantia da integridade da informação e sua relevância para a democracia, é apenas a partir de 2023, que o Brasil passa a integrar tais iniciativas, entre elas, a Parceria Internacional para a Informação e a Democracia e a Declaração Global para Integridade da Informação On-line[38].

---

recomendações para atingir o objetivo urgente de mitigar os danos gerados pela disseminação de desinformação. Entre elas, está a recomendação para as empresas de tecnologia definirem modelos de negócio que não priorizem o engajamento sobre os direitos humanos. Ver ONU. Princípios Globais das Nações Unidas para a Integridade da Informação: Recomendações para Ação de Múltiplas Partes Interessadas. 2024. Disponível em: ONU_PrincipiosGlobais_IntegridadeDaInformacao_20240624.pdf Acesso em: 15 out. 2024.

35 DOURADO, Tatiana. Cooperações internacionais face à desinformação on-line: União Europeia, Brasil e o princípio de uma abordagem global. In: LEIMANN-LOPEZ, Carmen; THEMOTEO, Reinaldo J. (Orgs.). **As relações Brasil-Europa diante do mundo em transformação**. Rio de Janeiro: Konrad Adenauer Stiftung, 2023, p. 41.

36 Para uma leitura crítica do termo "integridade da informação" ver SANTOS, Nina. Por que precisamos discutir a chamada "integridade da informação?". **Diplomatique**. 6 de fevereiro de 2024. Disponível em: https://diplomatique.org.br/integridade-da-informacao/ Acesso em: 10 out. 2024.

37 DOURADO, op. cit., p. 40.

38 DOURADO, op. cit., p. 46.

Em março de 2024, a Assembleia Geral da ONU adota a Resolução 78/L.49, sua primeira relativa ao tema da IA. Com um tom bem menos impositivo do que o rascunho anterior de dezembro de 2023, a Resolução assume, conforme sua natureza de ato não vinculante, uma abordagem de recomendação e orientação para as ações a serem tomadas pelos países-membros da ONU no tema da IA[39].

Assim, conclama os países desenvolvidos a cooperar com os países em desenvolvimento no acesso inclusivo e equitativo aos benefícios da IA, como também incentiva todos os países a facilitar o desenvolvimento de estruturas capazes de proteger os indivíduos contra usos abusivos da IA e outras práticas nocivas contra seus direitos. Aos Estados a Resolução garante um alto grau de discrição na implementação de suas ações, conforme sua legislação e seus interesses nacionais.

Com efeito, sobre o tema da IA os países possuem interesses muito divergentes[40]. Os Estados Unidos, por sediarem grandes empresas de tecnologia – como a Google e a Microsoft – têm interesses alinhados aos dessas corporações no que se refere à promoção de negócios, inovação e receita. Por sua vez, a União Europeia adota parâmetros rigorosos de proteção à privacidade, por meio de uma estrutura legal de controle do uso excessivo de dados pessoais dos usuários das redes sociais. Por último, os países do Sul Global, entre eles do continente africano e da América Latina, têm como pauta principal preocupações relativas à inclusão digital e à garantia de sua soberania digital frente aos interesses comerciais e políticos de grandes empresas de tecnologia.

Em consonância, o Presidente Lula defende utilizar a posição estratégica do Brasil na presidência do G20 em 2024 e do BRICS em 2025 para

39 KNAUER, Annika. The First United Nations General Assembly Resolution on Artificial Intelligence. 2 de abril de 2024. Disponível em: The First United Nations General Assembly Resolution on Artificial Intelligence – EJIL: Talk! Acesso em: 20 out. 2024.

40 KNAUER, op. cit.

pautar os interesses do Sul Global relativos à IA[41]. De fato, o governo brasileiro tem buscado demonstrar no plano internacional que a IA é pauta central de sua política exterior. No seu discurso de abertura da 79ª edição da Assembleia Geral da ONU, o Presidente Lula assim se declarou:

O futuro de nossa região passa, sobretudo, por construir um Estado sustentável, e ciente, inclusivo e que enfrenta todas as formas de discriminação. Que não se intimida ante indivíduos, corporações ou plataformas digitais que se julgam acima da lei. [...] Elementos essenciais da soberania incluem o direito de legislar, julgar disputas e fazer cumprir as regras dentro de seu território, incluindo o ambiente digital. [...] Na área de Inteligência Artificial, vivenciamos a consolidação de assimetrias que levam a um verdadeiro oligopólio do saber. Avança a concentração sem precedentes nas mãos de um pequeno número de pessoas e de empresas, sediadas em um número ainda menor de países. Interessa-nos uma Inteligência Artificial emancipadora, que também tenha a cara do Sul Global e que fortaleça a diversidade cultural. Que respeite os direitos humanos, proteja dados pessoais e promova a integridade da informação. E, sobretudo, que seja ferramenta para a paz, não para a guerra. Necessitamos de uma governança intergovernamental da inteligência artificial, em que todos os Estados tenham assento[42].

Nessa perspectiva, o governo brasileiro assume uma posição importante de defesa não somente dos interesses do Sul Global, mas também da soberania estatal em geral contra abusos de grandes empresas de tecnologia. Trata-se de uma tendência crescente em países da União Europeia e América Latina no que se refere a propostas robustas de re-

41 G20. **Brasil propõe debate sobre Inteligência Artificial na ONU e no G20**. 7 de março de 2024. Disponível em: Brasil propõe debate sobre Inteligência Artificial na ONU e no G20 Acesso em: 20 out. 2024.

42 AGÊNCIA GOV. **Lula abre a 79ª Assembleia Geral da ONU. Veja íntegra e principais pontos do discurso**. 24 de setembro de 2024. Disponível em: https://agenciagov.ebc.com.br/noticias/202409/lula-abre-79-assembleia-geral-da-onu-veja-integra-e-principais-pontos-do-discurso Acesso em: 20 out. 2024.

gulação estatal e a investidas do Poder Judiciário contra diretores executivos das *big techs*[43].

5. Conclusão

No Brasil há um avanço significativo no desenvolvimento do marco regulatório de IA com atenção às legislações existentes, como, a LGPD, e à necessidade de atualização constante dessas regulações específicas à luz da jurisprudência e das demandas da sociedade civil. Embora o contexto político e social de cada país deva ser considerado no momento da formulação de abordagens à proteção da integridade da informação via regulação da IA, o Brasil pode ser visto como um caso de referência. Após ataques à democracia, resultando no 8 de janeiro de 2023, houve um concerto entre os poderes executivo, legislativo e judiciário no combate à desinformação.

Cada vez mais os Estados vêm buscando reafirmar sua soberania sobre as grandes empresas de tecnologia. A participação do Brasil nos fóruns internacionais desde 2023 tem enfatizado essa tendência em defesa de governos democráticos e da legitimidade da execução de suas leis, inclusive no espaço digital. Nesse contexto, é de extrema relevância a proposta de uma leitura crítica do termo "integridade da informação" que enfatiza a defesa de um sentido social e coletivo à luz da realidade e dos interesses do Brasil e dos demais países latino-americanos[44].

---

43 No final de agosto de 2024, dias antes da suspensão do "X" no Brasil, o Poder Judiciário Francês ordenou a prisão do diretor executivo do Telegram, Pavel Durov, por acusações de distribuição de material de abuso sexual infantil e uso ilegal de equipamento de criptografia, entre outras. O Telegram tem um histórico de não cumprir ordens judiciais na França. Ver KLONICK, Kate; SCHRAMM, Moritz. "This case has the potential to set precedent for all of the internet". **Verfassungsblog**. 14 de setembro de 2024. Disponível em: https://verfassungsblog.de/this-case-has-the-potential-to-set-precedent-for-all-of-the-internet/ Acesso em: 19 out. 2024.

44 SANTOS, op. cit.

Nessa perspectiva, o Brasil, neste seu momento de volta ao protagonismo internacional, deve pugnar pela construção de um ambiente de comunicação e informação digital, com a atuação de empresas de tecnologia responsivas, que atenda aos anseios das democracias instáveis e desiguais do Sul Global. Com isso, o país pode contribuir efetivamente para o debate global acerca dos riscos e potenciais da IA no contexto de combate à desinformação.

Eleonora Mesquita Ceia · Doutora em Direito pela Universidade de Saarbrücken. Professora Titular de Direito Constitucional do Ibmec-RJ e Professora Adjunta de Teoria do Estado da Faculdade Nacional de Direito da Universidade Federal do Rio de Janeiro (UFRJ). Professora Colaboradora do Programa de Pós-Graduação em Direito da UFRJ.

Fernanda Paes Leme Peyneau Rito · Doutora em Direito pela Universidade do Estado do Rio de Janeiro (UERJ). Professora Titular de Direito Civil do Ibmec-RJ. Coordenadora Acadêmica do Curso de Graduação em Direito do Ibmec-RJ. Professora convidada dos cursos de Extensão e de Pós-Graduação da CEPED/UERJ, EMERJ e da Escola Nacional de Seguros. Presidente da Diretoria Regional do Instituto Brasileiro de Direito Contratual (IBDCont/RJ). Vice-Presidente Executiva da Academia Brasileira de Direito Civil (ABDC).

Computação Quântica: desafios e oportunidades

Franklin de Lima Marquezino

Resumo

A computação quântica é a proposta de controlar sistemas físicos quânticos, como átomos ou fótons, para resolver alguns problemas que são muito difíceis nos computadores clássicos. Embora ainda esteja em estágio experimental, seu potencial revolucionário promete transformar áreas estratégicas da economia global. Este artigo explora o impacto potencial da computação quântica em diversos setores, destacando suas aplicações mais promissoras, como a simulação de sistemas quânticos e a otimização combinatória. O artigo discute os principais desafios tecnológicos e econômicos, incluindo a correção de erros e a escalabilidade dos sistemas quânticos, e também aborda o impacto social e a necessidade de educar a sociedade sobre essa tecnologia emergente.

Abstract

Quantum computing is the proposal to control quantum physical systems, such as atoms or photons, to solve problems that are extremely difficult for classical computers. Although still in an experimental stage, its revolutionary potential promises to transform strategic areas of the global economy. This article explores the potential impact of quantum computing across various sectors, highlighting its most promising applications, such as quantum system simulation and combinatorial op-

timization. It also discusses key technological and economic challenges, including error correction and system scalability, as well as the social impact and need for public education on this emerging technology.

Introdução

A mecânica quântica é uma área da física moderna que surgiu no início do século XX para estudar sistemas em escalas extremamente pequenas, como partículas subatômicas e moléculas, já que a mecânica clássica não funcionava corretamente nessas situações. Sistemas quânticos se comportam de forma muito diferente dos objetos com os quais interagimos cotidianamente, de modo que algumas previsões da mecânica quântica podem causar grande perplexidade. Se lançarmos um dado comum dentro de uma caixa podemos afirmar com convicção, mesmo antes de olhar o resultado, que a face voltada para cima tem um número de um a seis. Se esse dado fosse do tamanho de um átomo, a mecânica quântica prevê que situações mais estranhas poderiam acontecer. Antes de olhar dentro da caixa, o „dado quântico“ poderia existir em um estado como se de alguma forma tivesse várias faces voltadas para cima ao mesmo tempo. Mas ao olharmos dentro da caixa, veríamos somente um dado comum, com um único número voltado para cima. Claro, trata-se apenas de uma metáfora, com suas limitações. No entanto, por mais estranho que um cenário desses possa parecer, o arcabouço matemático da mecânica quântica tem sido extremamente bem sucedido em prever resultados de experimentos com altíssima precisão. Pensando ainda na metáfora anterior, o leitor certamente deve ter diversos questionamentos sobre o que realmente há dentro da caixa e o que ocorre objetivamente ao observarmos seu interior. De fato, discussões acaloradas sobre as interpretações da mecânica quântica vem acontecendo até os dias de hoje, sendo esta uma importante área de estudo da filosofia da ciência.

Muito além de ser um campo fascinante do ponto de vista teórico, a mecânica quântica já vem sendo usada há muitas décadas para aplica-

ções tecnológicas. Por exemplo, os transistores e o *laser* são tecnologias quânticas de primeira geração, que portanto somente foram viáveis a partir da compreensão de fenômenos quânticos. A computação quântica, um dos assuntos tecnológicos mais discutidos nos últimos anos e tema principal deste artigo, é um exemplo típico de tecnologia quântica de segunda geração, por utilizar fenômenos quânticos mais diretamente e de forma mais controlada. Trata-se de um modelo computacional que emprega sistemas físicos quânticos como componentes fundamentais dos computadores, permitindo realizar certos tipos de cálculos de forma muito mais eficiente do que com computadores clássicos. Alguns desses cálculos teriam impactos profundos na sociedade ao serem resolvidos de forma eficiente – eis o motivo pelo qual a computação quântica tem atraído tanta atenção. Por exemplo, cálculos precisos e eficientes em química quântica têm impactos profundos tanto na indústria farmacêutica como na produção de fertilizantes para o agronegócio. A fatoração de inteiros grandes representa uma ameaça concreta para a segurança da informação e obriga a adoção de métodos criptográficos mais seguros que os atuais.

Dado que a computação quântica tem potencial para impactar profundamente tantos setores estratégicos, alguns fatos básicos sobre essa tecnologia precisam ser conhecidos por todos os cidadãos, independentemente de sua área de atuação na sociedade. No entanto, muitas pessoas que desejam aprender sobre computação quântica sentem-se intimidadas pela expectativa de lidar com conceitos muito avançados de física moderna. Em nossa sociedade, a mecânica quântica é reconhecida como um dos tópicos mais difíceis de aprender e inacessível para quem não possui sólida formação em CTEM[1]. Essa visão elitista da ciência é problemática e traz consequências negativas, contribuindo para a proliferação de ideias erradas sobre as tecnologias quânticas. Por isso é importante que a sociedade seja educada sobre a ciência moderna, a fim

1 Ciência, Tecnologia, Engenharia e Matemática.

de compreender o potencial e as limitações da tecnologia, e dessa forma tomar decisões sensatas quanto à alocação de recursos.

Em primeiro lugar, é importante esclarecer que a computação quântica não é capaz de resolver problemas que são impossíveis para computadores clássicos. Há, de fato, problemas matemáticos que são provadamente impossíveis de se resolver mesmo pelos computadores mais sofisticados – são os problemas chamados „incomputáveis". Um exemplo típico é o problema da parada, estudado por Alan Turing, e nem mesmo um computador quântico conseguiria resolvê-lo. Portanto, a primeira distinção importante que devemos fazer é entre eficiência e computabilidade. A promessa da computação quântica é ser mais eficiente, porém não faz sentido prometer a resolução de problemas incomputáveis.

Um segundo mito que precisa ser combatido é de que a computação quântica irá resolver qualquer problema com facilidade, ou que será mais eficiente que a computação clássica em todos os aspectos. Na verdade, nem tudo pode ser resolvido eficientemente na computação quântica. E além disso, muitos problemas para os quais a computação clássica já possui soluções eficientes não podem ser melhorados no mundo quântico. Dessa forma, é esperado que a computação quântica sempre coexista com a computação clássica, e que unidades de processamento quânticas sejam usadas para resolver problemas específicos.

Outro engano comum é pensar que seja trivial desenvolver algoritmos quânticos a partir de ideias conhecidas da computação clássica. A realidade é que a maioria dos algoritmos quânticos são altamente contra-intuitivos e o seu desenvolvimento possui muitas particularidades que requerem habilidades diversas daquelas de desenvolvedores clássicos. Testar um software quântico, por exemplo, é muito mais difícil, pois não se pode observar estados intermediários do cálculo sem causar seu colapso e a perda de propriedades quânticas.

Para obter vantagem a partir de algoritmos quânticos precisamos de hardware quântico, cujo desenvolvimento ainda é um grande desafio tecnológico. Já existem computadores quânticos, porém todos são ainda

muito limitados e sujeitos a erros, de modo que ainda não são capazes de resolver problemas práticos de forma mais eficiente que os clássicos. Alguns desses computadores quânticos podem ser acessados gratuitamente na nuvem, com algumas limitações, sendo boas ferramentas para treinamento e pesquisa acadêmica. No entanto, a maioria dos computadores quânticos atualmente é acessada mediante pagamento por tempo de uso. Também é possível comprar computadores quânticos para uso exclusivo, porém isso ainda requer um altíssimo investimento nos dias de hoje.

Neste artigo, algumas noções essenciais de mecânica quântica e computação quântica são apresentados na Seção 1, sem entrar em detalhes técnicos e sem usar notação matemática avançada. As principais aplicações da computação quântica são apresentadas na Seção 2. Os principais obstáculos para o desenvolvimento da computação quântica são apresentados na Seção 3. Os progressos recentes e as perspectivas de médio e longo prazo, são apresentados na Seção 4. Finalmente, as discussões finais e conclusões são apresentadas na Seção 5.

1. Fundamentos de computação quântica

Na computação digital clássica, a unidade básica de informação é o bit, termo cunhado por Claude Shannon na década de 1940 como abreviação de *binary digit*, ou dígito binário. Portanto, o bit é uma variável que pode assumir a cada instante somente um dentre dois valores possíveis, usualmente denotados por 0 ou 1. É importante observar que o bit não é uma mera idealização matemática, mas pode também possuir uma realização física. Basicamente qualquer sistema físico clássico com dois estados bem definidos e facilmente distinguíveis é apto a representar um bit. Pode-se utilizar para representar os bits 0 e 1, por exemplo, dois níveis de tensão de uma corrente elétrica, ou duas polarizações perpendiculares de um fóton, ou a carga armazenada de um capacitor.

Se substituirmos esses sistemas clássicos por sistemas quânticos com dois níveis de energia bem distinguíveis, de modo que possamos

controlá-los e medi-los, teremos uma realização física para um *bit quântico*, ou abreviadamente *qubit*. Enquanto o bit pode assumir a cada instante somente um valor dentre dois possíveis, o qubit pode existir em um estado que é uma combinação destes dois. Intuitivamente, podemos pensar que o qubit vale 0 e 1 ao mesmo tempo, com certos pesos associados. Chamamos a esse estado de *superposição quântica*.

Ainda de modo intuitivo, podemos considerar o que teríamos ao juntar dois qubits. As superposições possíveis nesse caso envolveriam os estados 00, 01, 10 e 11, com seus respectivos pesos. A propriedade da superposição dá origem ao *paralelismo quântico*. A ideia é que ao efetuarmos uma operação sobre uma superposição de estados, essa operação é aplicada simultaneamente a todos os termos da superposição. Com dois qubits, conseguimos realizar paralelamente operações sobre quatro termos distintos. Com três qubits, o paralelismo atua sobre oito termos. E assim por diante, com crescimento exponencial.

Uma outra consequência muito curiosa do princípio da superposição quântica envolvendo dois ou mais qubits é o *emaranhamento*. Um exemplo de emaranhamento seria a superposição envolvendo dois qubits na qual somente os estados 00 e 11 possuem algum peso. Uma pergunta que podemos fazer nesse caso é como escrever o estado de cada qubit individualmente. A resposta é que não podemos fazê-lo, pois os dois qubits estão muito fortemente correlacionados. Se observamos o primeiro qubit colapsando-o para o estado 0, então nesse caso o segundo também necessariamente terá colapsado para 0. E, da mesma forma, se o primeiro qubit colapsa para o estado 1, então o segundo qubit também colapsa para 1. E curiosamente isso é verdade mesmo que os dois qubits correspondam a partículas quânticas muito distantes entre si – uma na Terra e outra em Marte, digamos. Trata-se de um fenômeno dos mais contra-intuitivos da mecânica quântica e sem paralelos diretos no nosso cotidiano.

Somente o paralelismo quântico e o emaranhamento não são suficientes para garantir ganhos expressivos de desempenho nos computadores quânticos. Um erro comum transmitido com frequência é dizer

que o computador quântico é mais rápido porque tenta todas as soluções possíveis em paralelo. Na verdade, somente com o paralelismo mas sem a *interferência quântica*, não seria possível ter vantagem por meio da computação quântica. A interferência é o efeito que permite a alguns termos de uma superposição serem amplificados enquanto outros são atenuados – de modo semelhante aos padrões de interferência que vemos nas ondas em um lago, ao se lançar pedras sobre o mesmo. Para desenvolver algoritmos quânticos eficientes, além de explorar o paralelismo precisamos também garantir que os termos correspondentes à solução desejada sejam amplificados por meio de interferência construtiva, enquanto os demais termos sejam atenuados por interferência destrutiva.

Uma importante diferença entre computadores clássicos e quânticos é o momento de ler o resultado. A medição na mecânica quântica implica necessariamente um colapso aleatório e irreversível do estado quântico. Devido à forma como se dá a medição em sistemas quânticos, os computadores quânticos são particularmente sensíveis a interferências do ambiente. Por um lado, precisamos controlar o computador de modo que realize o cálculo que desejamos, portanto ele precisa interagir com o meio externo de alguma forma. Por outro lado, essa interação pode agir como uma medição, ainda que involuntária, causando a degradação do estado quântico e consequentemente do cálculo que se desejava realizar. Essa perda das propriedades quânticas chamada de *descoerência* é um dos maiores desafios para construção de computadores quânticos hoje.

Como os computadores quânticos são tão sensíveis, somente conseguiremos extrair todo seu potencial com a ajuda de sistemas que detectem e corrijam erros. A boa notícia é que a teoria para esse tipo de sistema já é bem conhecida há muitos anos, e novos códigos ainda mais avançados vêm sendo desenvolvidos nos últimos anos. No entanto, ainda há pelo menos dois grandes obstáculos para a implementação de uma computação quântica tolerante a falhas. Em primeiro lugar, o número de qubits disponíveis deve ser muito alto para compensar os que

são perdidos devido à necessidade de redundância. Em segundo lugar, a qualidade destes deve ser bem melhor que a atual para que os erros não sejam produzidos mais rapidamente do que podem ser corrigidos.

A discussão nesta seção foi propositalmente informal, dada a restrição de espaço. Para sermos mais formais, deveríamos usar recursos da álgebra linear, que é o ramo da matemática por trás da mecânica quântica e consequentemente da computação quântica. A álgebra linear ocupa-se do estudo de objetos chamados vetores e as operações que podemos realizar entre eles satisfazendo certas propriedades. Nesse formalismo matemático, os qubits são representados por vetores, e se precisarmos juntar vários qubits podemos fazê-lo por meio de uma operação chamada produto tensorial. Os algoritmos quânticos são representados matematicamente por sequências de matrizes que, operadas sobre os vetores de qubits, os vão transformando passo a passo até alcançar a solução para o problema. A medição dos qubits, ou seja, a leitura do resultado, é representada matematicamente por meio de projetores. O profissional que deseja se aprofundar na computação quântica deve buscar uma boa formação matemática, especialmente em álgebra linear.

Para uma introdução mais abrangente sobre os conceitos de computação quântica, o leitor pode consultar o livro de Marquezino, Portugal e Lavor (2019). Para continuar se aprofundando, o leitor pode estudar o livro de Wong (2022), que é mais extenso apesar de ainda adequado como introdução. Ambos os livros introduzem de forma concisa os principais conceitos e notações de álgebra linear.

2. Aplicações da computação quântica

Um erro comum cometido por quem se inicia na computação quântica e que é propagado por notícias exageradas, é a ideia de que computadores quânticos serão capazes de resolver todo tipo de problema exponencialmente mais rápido que os computadores clássicos. Há também quem pense que um algoritmo clássico ficaria automaticamente mais rápido apenas se fosse executado em um computador quântico.

Todas essas ideias são exageradas e não correspondem à realidade. Na verdade, há certos tipos de problemas que os computadores quânticos poderão resolver muito mais rapidamente que os clássicos, enquanto para outros não faria diferença. Por esse motivo, o mais provável é que no futuro computadores clássicos e quânticos co-existam.

Uma analogia é a forma como GPUs[2] não utilizadas hoje em dia como auxiliares para diversos problemas que envolvem cálculos intensos de matrizes. No futuro, é provável que além de GPUs, os centros de computação de alto desempenho lançarão mão também de QPUs[3] para resolver cálculos específicos. Não faz sentido utilizar um equipamento mais caro para resolver problemas com os quais processadores comuns e GPUs já lidam muito bem, então a tendência é que todos esses dispositivos trabalhem juntos nos futuro. Os computadores quânticos somente substituirão os clássicos um dia, se por algum motivo improvável eles se tornarem mais baratos que os clássicos – não necessariamente na sua construção, mas no consumo de energia ou manutenção, por exemplo. Sendo assim, é importante conhecer os tipos de problemas em que os processadores quânticos serão úteis.

A primeira aplicação pensada para a computação quântica foi a simulação de sistemas quânticos, conforme proposto por Feynman (1982). Ele sugeriu que seria mais eficiente usar um computador quântico para simular outros sistemas quânticos, algo que os computadores clássicos encontram extrema dificuldade em fazer. A simulação quântica tem importância central em áreas como o desenvolvimento de fármacos, permitindo a modelagem precisa de interações moleculares que podem levar à criação de novos medicamentos. Além disso, a descoberta de novos nanomateriais com propriedades personalizadas para aplicações tecnológicas é outro campo que pode ser revolucionado por essa tecnologia. Um exemplo prático é a simulação de catalisadores para aumentar a eficiência de processos industriais, como a produção de fer-

2 *Graphical Processing Unit*.

3 *Quantum Processing Unit.*

tilizantes, que consome grandes quantidades de energia. A computação quântica poderá proporcionar enormes economias energéticas e benefícios ambientais significativos.

O primeiro algoritmo quântico com uma aplicação prática muito evidente mesmo para não-especialistas e com grande potencial de impacto na sociedade foi o algoritmo de Shor para fatoração de inteiros, apresentado em 1994. A capacidade de fatorar números inteiros grandes de forma eficiente tem como consequência a obsolescência de diversos métodos criptográficos que utilizamos amplamente para realizar compras na Internet ou para transações bancárias. Portanto, a notícia de que computadores quânticos poderiam decifrar esses códigos secretos causou uma revolução na forma como a computação quântica era vista. O que antes era uma curiosidade científica de físicos teóricos passou a ser tratado como um assunto de alta relevância prática mesmo por quem não era especialista. O algoritmo de Shor requer computadores quânticos tolerantes a falhas, que ainda estão muito distantes da realidade atual, como veremos mais adiante neste artigo. Portanto, os sistemas criptográficos atuais ainda permanecerão seguros por muitos anos. Ainda assim, setores que dependem de altíssima confidencialidade já estão investindo em métodos de criptografia *pós-quânticos*, mais sofisticados, e que permanecerão seguros mesmo quando tivermos computadores quânticos operando de acordo com seu pleno potencial.

Outro desenvolvimento que causou grande impacto na história da computação quântica foi o algoritmo de Grover, em 1996. Esse algoritmo apresentou um ganho de desempenho bem mais modesto que o de Shor, porém para um problema de aplicação muito mais geral. O algoritmo de Grover serve para encontrar um elemento em uma lista não ordenada ou sem uma estrutura. Por exemplo, encontrar uma palavra no dicionário é fácil pois as entradas estão em ordem alfabética. Se não estivessem, teríamos que procurar palavra por palavra, e no pior caso teríamos que consultar o livro inteiro. Com o algoritmo de Grover, o número de consultas é da ordem de raiz quadrada do número de palavras – não é um ganho exponencial como o algoritmo de Shor, mas ainda

assim é interessante. Talvez o resultado não pareça muito impressionante através dessa metáfora, pois dicionários sempre estão em ordem alfabética. No entanto, há muitos problemas práticos que não conseguimos resolver diretamente, mas conseguimos verificar se uma tentativa de solução que nos é apresentada está correta ou não. Podemos resolver esse tipo de problema por tentativa e erro, testando um candidato de cada vez. Essa abordagem é semelhante a procurar uma palavra específica em uma lista desordenada, o que certamente é muito ineficiente. Computadores quânticos, entretanto, podem tirar proveito da superposição de estados e da interferência, e dessa forma encontram a solução para o problema muito mais rapidamente.

A computação quântica tem grande potencial para resolver problemas de otimização combinatória, o que pode trazer benefícios significativos para a indústria. Muitos desses avanços são possíveis graças ao uso de algoritmos híbridos, que combinam o melhor dos computadores quânticos e clássicos. Nessa abordagem, parte dos cálculos ocorre em circuitos quânticos parametrizados, enquanto otimizadores clássicos ajustam esses parâmetros – de modo semelhante ao treinamento de uma rede neural artificial. Esse método permite que os circuitos sejam mais compactos, tornando-os mais adequados para a limitação dos dispositivos quânticos atuais. Além disso, a técnica de *annealing* quântico, que é análoga ao *simulated annealing* da computação clássica, também tem sido aplicada com sucesso em problemas de otimização. Essa técnica é particularmente útil em problemas onde a busca pela solução global ótima precisa navegar por um vasto espaço de soluções, sendo usada em campos como logística, planejamento e finanças.

Uma aplicação importante da computação quântica é a resolução de sistemas lineares de equações, problema recorrente em diversas áreas, desde a física até a economia, e para o qual os algoritmos quânticos oferecem um ganho exponencial de eficiência em relação aos métodos clássicos. No entanto, utilizar esse tipo de algoritmo em computadores quânticos não é tão simples quanto na computação clássica, pois o resultado final é codificado em estados de superposição, impossibilitando

uma medição direta como fazemos em sistemas clássicos. Apesar desse desafio, várias propostas têm sido desenvolvidas para aplicar essa técnica na solução de equações diferenciais, o que abre portas para aplicações em áreas como a simulação da dinâmica de fluidos, onde a precisão e a rapidez na resolução de sistemas lineares são essenciais. Esses avanços mostram o potencial de algoritmos quânticos para resolver problemas matemáticos complexos, possibilitando simulações mais rápidas e precisas em diversas áreas da ciência e da engenharia.

Para uma exposição mais completa e mais técnica das aplicações da computação quântica o leitor pode consultar Dalzell *et al.* (2024). Os leitores que já possuem certa experiência em programação de computadores podem se aprofundar nessas aplicações e até mesmo executá-las em computadores quânticos reais, estudando algum kit de desenvolvimento como o IBM Qiskit (JAVADI-ABHARI *et al.*, 2024).

3. Principais desafios atuais

Apesar de todo o entusiasmo recente em torno da computação quântica, deve-se ter em mente que ainda há grandes desafios a serem superados antes que a computação quântica avance da fase experimental para aplicações comerciais. Conhecer esses desafios é importante para manter as expectativas alinhadas com a realidade.

3.1 Desafios tecnológicos

Um primeiro obstáculo para o avanço da computação quântica ainda é a qualidade dos qubits e a escalabilidade dos sistemas. Os qubits atuais, apesar de terem melhorado recentemente, ainda possuem um nível de ruído elevado. Além disso, a construção de computadores com milhares ou milhões de qubits, que seriam necessários para resolver problemas práticos, ainda é uma meta distante. A dificuldade em controlar muitos qubits de forma estável, sem comprometer a coerência e introduzir erros, impõe limites ao crescimento dos sistemas quânticos.

Soma-se a isso o fato de não termos ainda uma direção clara de implementação física dos qubits. Há muitas propostas diferentes – como supercondutores, armadilhas de íons, átomos neutros, fótons, dentre outros – cada qual com suas vantagens e desvantagens.

Devido à extrema sensibilidade dos qubits ao ambiente externo, até mesmo mínimas interações podem gerar erros que, se não corrigidos, comprometem o resultado final dos cálculos. Diferente da computação clássica, onde bits errôneos podem ser facilmente detectados e corrigidos, a correção de erros em sistemas quânticos é muito mais complexa. No entanto, para atingir todo o potencial da computação quântica é necessário ainda avançar em sistemas de correção de erros até finalmente atingir o marco da computação quântica tolerante a falhas. Apesar de avanços significativos, implementar esses mecanismos em larga escala continua a ser um desafio (CAMPBELL, 2024).

Para mais detalhes sobre os desafios da computação quântica no estágio atual, em que somente temos à disposição computadores com poucos qubits e muito ruído, o leitor pode consultar Bharti *et al.* (2022). Para mais detalhes sobre a construção de computadores quânticos, existe o recente livro de Majidy, Wilson e Laflamme (2024).

3.2. Desafios econômicos

O custo de desenvolvimento e implementação de computadores quânticos é extremamente elevado, o que restringe sua disponibilidade a poucos centros de pesquisa e grandes empresas tecnológicas. A criação de ambientes econômicos que permitam o investimento contínuo nessa área será crucial para que a computação quântica tenha impacto global. Programas de cooperação internacional e incentivos governamentais serão fundamentais para democratizar o acesso à computação quântica e garantir que o progresso tecnológico seja amplamente distribuído.

Países em desenvolvimento como o Brasil estão aproveitando o acesso a plataformas de computação quântica via nuvem, fornecidas por grandes empresas como IBM e Amazon, para avançar na pesquisa

e no desenvolvimento sem a necessidade de construir hardware próprio. Esse modelo de colaboração internacional permite que pesquisadores brasileiros explorem as potencialidades da computação quântica e apliquem algoritmos quânticos a problemas locais. Através de parcerias com empresas globais, o Brasil pode acelerar seu acesso à tecnologia quântica, superando as limitações econômicas e tecnológicas que ainda impedem a construção de computadores quânticos próprios.

Outro obstáculo significativo é a escassez de profissionais capacitados para trabalhar com computação quântica. Apesar de as universidades e centros de pesquisa estarem começando a oferecer mais programas de estudo sobre o tema, o número de especialistas ainda é insuficiente para atender à crescente demanda. Desenvolver um ecossistema de talentos que vá além dos cientistas e engenheiros quânticos, abrangendo também desenvolvedores de software e profissionais de TI capazes de integrar as tecnologias quânticas aos sistemas clássicos, será essencial para que a computação quântica tenha um impacto sustentável a longo prazo.

4. Progressos recentes e perspectivas

Nos últimos anos, a pesquisa em computação quântica avançou significativamente, com vários grupos reivindicando a chamada supremacia quântica – o ponto em que um dispositivo quântico supera até o melhor supercomputador clássico em uma tarefa específica, não necessariamente de interesse prático. O experimento mais notório, apesar de um tanto controverso, foi realizado pela Google em 2019, quando seu processador *Sycamore* completou um cálculo em cerca de 200 segundos, o que de acordo com eles levaria cerca de 10.000 anos usando o supercomputador clássico mais rápido do mundo. No entanto, a IBM contestou essa afirmação, sugerindo que a mesma tarefa poderia ser realizada por um supercomputador clássico em poucos dias, desde que utilizando uma abordagem melhorada. Desde então, outros grupos também realizaram experimentos que alcançaram supremacia quântica, motivando o desenvolvimento de algoritmos clássicos que os superaram. A

supremacia quântica, portanto, ainda é um alvo em movimento. Apesar das controvérsias desses resultados, principalmente devido aos aspectos de marketing envolvidos, eles são importantes por marcarem uma tendência de progresso contínuo da área, demonstrando o potencial da computação quântica em resolver problemas que seriam inviáveis para sistemas clássicos.

Apesar dos grandes desafios tecnológicos ainda existentes, a produção de computadores quânticos têm acelerado não somente em quantidade, mas também em qualidade. Diversas empresas têm estabelecido *roadmaps* ousados para o desenvolvimento de hardware quântico e os têm cumprido razoavelmente bem até aqui, com progressos significativos. Uma parceria entre os finlandeses VTT e IQM tem sido muito bem sucedida, tendo atingido recentemente a marca de 30 computadores quânticos produzidos e a capacidade de produzir até 20 computadores por ano. A Quantinuum espera ter computadores quânticos universais e tolerantes a falhas até 2030, e possui um histórico recente de muitos marcos importantes de desenvolvimento atingidos, inclusive na área de códigos de correção de erros. A IBM planeja entregar já em 2029 computadores quânticos de 200 qubits, com correção de erros, e capacidade de executar um total de 100 milhões de operações.[4]

Portanto, a computação quântica tem um enorme potencial econômico. Jean-François *et al.* (2024), do Boston Consulting Group, projetam que a computação quântica poderá gerar entre US$ 450 bilhões e US$ 850 bilhões em valor econômico, com um mercado na faixa de US$ 90 bilhões a US$ 170 bilhões até 2040. Valores semelhantes também são previstos pelo *Quantum Technology Monitor 2024* de McKinsey & Company[5], que inclui na análise outras tecnologias quânticas correlacionadas, como comunicação e sensores quânticos. Os investimentos

4 O *roadmap* completo está disponível em https://www.ibm.com/roadmaps/quantum/2024/. Acesso em 21 de outubro de 2024.

5 Disponível em https://www.mckinsey.com/featured-insights/the-rise-of-quantum-computing. Acesso em 21 de outubro de 2024.

públicos no setor têm sido bastante elevados em países como China, Alemanha, Reino Unido e Estados Unidos da América.

5. Considerações finais

Em conclusão, a computação quântica apresenta um potencial transformador em várias áreas estratégicas, incluindo a saúde, segurança da informação, finanças, logística e otimização de processos industriais. Aplicações como a simulação de sistemas quânticos e o desenvolvimento de novos fármacos demonstram o alcance dessa tecnologia, que pode impactar desde a produção de fertilizantes até a indústria farmacêutica. Embora os recentes avanços sejam promissores, é crucial alinhar as expectativas à realidade. A computação quântica não substituirá os sistemas clássicos; em vez disso, coexistirá com eles, fornecendo soluções específicas para alguns problemas. Além disso, os computadores quânticos ainda enfrentam desafios tecnológicos significativos, como a correção de erros, a estabilidade dos qubits e a escalabilidade dos sistemas. Somente quando esses obstáculos forem superados poderemos atingir todo seu potencial.

Também é essencial destacar o papel das considerações políticas e sociais no avanço dessa tecnologia. Uma vez que a computação quântica pode impactar profundamente tantos setores estratégicos para uma nação, não é prudente manter o país em alta dependência de soluções estrangeiras. Os investimentos do Brasil no setor ainda são baixos, tanto no setor público quanto no privado. Finalmente, é importante destacar que além de pesquisa e desenvolvimento, é essencial investir também na formação de profissionais qualificados para garantir que os benefícios dessa tecnologia sejam plenamente alcançados.

Referências

BHARTI, Kishor; CERVERA-LIERTA, Alba; KYAW, Thi Ha; *et al*. Noisy intermediate-scale quantum (NISQ) algorithms. **Reviews of Modern Physics**, v. 94, n. 1, p. 015004, 2022.

CAMPBELL, Earl. A series of fast-paced advances in Quantum Error Correction. **Nature Reviews Physics**, v. 6, n. 3, p. 160–161, 2024.

DALZELL, Alexander M.; MCARDLE, Sam; BERTA, Mario; *et al*. Quantum algorithms: A survey of applications and end-to-end complexities. 2023. Disponível em: <http://arxiv.org/abs/2310.03011>. Acesso em: 10 outubro 2024.

FEYNMAN, Richard P. Simulating physics with computers. **International Journal of Theoretical Physics**, v. 21, n. 6, p. 467–488, 1982.

JAVADI-ABHARI, Ali; TREINISH, Matthew; KRSULICH, Kevin; *et al*. Quantum computing with Qiskit. 2024. Disponível em: <http://arxiv.org/abs/2405.08810>. Acesso em: 10 outubro 2024.

JEAN-FRANÇOIS, Bobier; MATT, Langione; CASSIA, Naudet-Baulieu; *et al*. **The Long-Term Forecast for Quantum Computing Still Looks Bright**. BCG Global. Disponível em: <https://on.bcg.com/3ye4ey2>. Acesso em: 18 outubro 2024.

MAJIDY, Shayan; WILSON, Christopher; LAFLAMME, Raymond. **Building Quantum Computers: A Practical Introduction**. Cambridge: Cambridge University Press, 2024.

MARQUEZINO, Franklin de Lima; PORTUGAL, Renato; LAVOR, Carlile. **A Primer on Quantum Computing**. 1. ed. [s.l.]: Springer, 2019.

WONG, Thomas G. **Introduction to classical and quantum computing**. Omaha, Nebraska: Rooted Grove, 2022.

Franklin de Lima Marquezino · Bacharel em Ciência da Computação pela Universidade Católica de Petrópolis (UCP). Mestre e Doutor em Modelagem Computacional pelo Laboratório Nacional de Computação Científica (LNCC). Professor Associado da Universidade Federal do Rio de Janeiro (UFRJ), atuando no Núcleo Multidisciplinar de Pesquisa em Computação (NUMPEX-Comp) do Campus Duque de Caxias Prof. Geraldo Cidade, e no Programa de Engenharia de Sistemas e Computação (PESC) do Instituto Alberto Luiz Coimbra de Pós-Graduação e Pesquisa de Engenharia (COPPE). Em 2011, sua tese de doutorado sobre Computação Quântica recebeu o Prêmio CAPES como melhor tese do Brasil na Área Interdisciplinar. Em 2024 foi Pesquisador Visitante no Centre for Quantum Computer Science da Universidade da Letônia. É membro do corpo editorial do periódico Theoretical Computer Science (TCS-C: Theory of Natural Computing).

A urgência da regulação das plataformas digitais

Rosemary Segurado

Resumo

O debate sobre a regulação das plataformas digitais é urgente, considerando a importância da proteção de dados, desinformação, privacidade, transparência, entre outros temas.

Abstract

The debate on regulating of digital platforms is urgent, considering the importance of data protection, disinformation, privacy, transparency, among other issues.

As plataformas desempenham um papel significativo na contemporaneidade considerando que através delas circulam os fluxos informacionais com os mais variados conteúdos e formatos. Temas como proteção de dados, desinformação, privacidade, transparência, monitoramento de conteúdos, entre outros são centrais na elaboração da regulação.

As legislações europeia e brasileira sobre proteção de dados, respectivamente o Regulamento Geral de Proteção de Dados (GDPR) e a Lei Geral de Proteção de Dados visam garantir que os dados pessoais dos usuários sejam tratados com segurança e que as plataformas sejam mais

transparentes sobre suas práticas de operação, algoritmos e políticas de conteúdo.

A responsabilidade sobre os conteúdos por parte das plataformas tem sido debate cada vez mais importante, colocando o estabelecimento de critérios claros e transparentes para que a moderação de conteúdos não seja prejudicial ou incorra em práticas ilegais.

O debate em torno da regulação em âmbito global tem se realizado em um contexto polarizado entre a autorregulação corporativa e a autorregulação autoritária e, nesse sentido, atores e organizações da sociedade civil buscam a realização de um debate capaz de construir uma regulação democrática que seja capaz de proteger os direitos humanos, garantindo que a população possa exercer seus direitos e liberdades individuais e coletivas.

As corporações de tecnologia ocupam um lugar cada vez mais importante nas dinâmicas sociais, políticas e econômicas. Através do processo de extração e modulação de dados pessoais, as plataformas digitais lucram com os dados adquiridos a partir dos rastros digitais, disponibilizados pelos indivíduos por meio da navegação cotidiana nas redes. Esses rastros se tornaram moedas valiosas para as Big Techs, empresas, governos e atores políticos.

Morozov (2018) afirma que a lógica do capitalismo centrado em dados, que ele denomina capitalismo dadocêntrico, transforma tudo em ativo rentável, desde nossos relacionamentos pessoais, a vida familiar, as férias, o sono, preferências alimentares etc. O big data pressupõe que cada indivíduo passa a ser concebido como um conjunto de dados que são considerados fundamentais para o capitalismo, tendo em vista a capacidade de predizer e modular o comportamento humano possibilitando tanto diversas formas de acumulação de riquezas para empresas quanto um conjunto de mudanças no campo da política e das relações sociais que passam a utilizar essas tecnologias intensamente.

Esse processo se intensifica à medida que as plataformas e aplicativos gratuitos passam a atuar em regiões com elevados níveis de pobreza em que a impossibilidade de adquirir conexões pagas de internet é su-

prida pelo acesso a serviços sem custo como facebook, whatsapp e instagran. É consenso entre pesquisadores que quando a aplicação é gratuita, os indivíduos entram na equação com seus dados disponibilizados a partir dos rastros digitais. É exatamente nesse campo que atua o data mining ou mineração de dados, processo que analisa grandes conjuntos de dados na busca de padrões, correlações com o objetivo de monetizar as experiências e dados pessoais, além de configurar diretrizes para uma nova ordem social e política.

Plataformas são infraestruturas digitais que permitem a interação de dois ou mais grupos e se posicionam como intermediários (POELL, T., NIEBORG, D., VAN DIJCK, 2020), tendo a capacidade de reunir diferentes usuários desde clientes a anunciantes, prestadores de serviços, entre outros. Os aplicativos de transporte privados urbanos são responsáveis por conectar passageiros a motoristas, os aplicativos de aluguéis de imóveis conectam proprietários a usuários, esse caráter intermediário é característico de uma parte significativa da economia informacional. A operação é aparentemente simples: a plataforma fornece a infraestrutura básica para mediar pessoas, grupos diferentes, porém diferentemente dos negócios tradicionais, aqui os dados são fundamentais e essa é a chave de vantagem em relação aos negócios tradicionais. Essa dinâmica confere grande poder às plataformas e faz com que se torne em um poderoso bloco que articula interesses mercantis opacos, lobistas e políticos com claros projetos de dominação.

> definimos plataformas como infraestruturas digitais (re)programáveis que facilitam e moldam interações personalizadas entre usuários finais e complementadores, organizadas por meio de coleta sistemática, processamento algorítmico, monetização e circulação de dados. Nossa definição é um aceno para os estudos de software, apontando para a natureza programável e orientada por dados das infraestruturas das plataformas, reconhecendo os *insights* da perspectiva dos estudos de negócios, incluindo os principais *stakeholders* ou "lados" nos mercados de plataforma: os usuários finais e os complementadores (POELL, T., NIEBORG, D., VAN DIJCK, 2020, p. 4)

As plataformas imprimem novo modelo de negócios adequado a um capitalismo voltado para a exploração econômica dos dados. Significa dizer que são um novo conjunto de tecnologias e modelos organizacionais e, o mais importante, representam um novo regime de acumulação capitalista (SRNICEK, 2017). Por isso, as empresas de tecnologias, as Big Techs, têm grande interesse no debate sobre regulação e atua justamente no sentido de bloquear qualquer conjunto de regras que possa gerar impacto em seu modelo de negócios. "as principais empresas de plataformas surgiram como os 'equivalentes modernos dos monopólios ferroviários, telefônicos e de serviços elétricos do final dos séculos XIX e XX'" (PLANTIN et al., 2018, p. 307).

A exploração econômica dos dados ocupa lugar de destaque nas formas de produzir riquezas no capitalismo contemporâneo sob a égide do neoliberalismo, ou seja, diferentes regimes de produção e acumulação de riquezas. Dito isso, os dados são os insumos básicos da produção e apresentam novas formas de competição e tendência à monopolização. Nesse sentido, as plataformas possuem grande poder na organização dos mercados em que atuam e acabam obtendo vantagens na definição das regras e do sistema de geração de valor.

É importante destacar que no século XXI, os dados passaram a ser matéria-prima fundamental e entramos na era do capitalismo centrado os dados. Não se trata de uma novidade que o sistema use dados para desenvolver sua estratégia de atuação, mas é importante ressaltar que a tecnologia se torna o grande diferencial nesse novo modelo de negócios. A expansão da internet e, consequentemente, a dependência do digital está transformando as relações produtivas.

Os dados extraídos das atividades cotidianas dos usuários nas redes digitais dependem de imensa infraestrutura com capacidade para detectar, registrar e analisar todo e qualquer tipo de fluxo informacional nas redes. É o que Zuboff (2021) denomina capitalismo de vigilância, considerado como uma nova ordem econômica baseada na vigilância, ou seja, uma forma intencional e fundamental para o processo de acumulação de capital no século XXI.

> Em vez de permitir novas formas contratuais, esses arranjos descrevem o surgimento de uma nova arquitetura universal que existe em algum lugar entre a natureza e Deus, batizada por mim de **Big Other**. Essa nova arquitetura configura-se como um ubíquo regime institucional em rede que registra, modifica e mercantiliza a experiência cotidiana, desde o uso de um eletrodoméstico até seus próprios corpos, da comunicação ao pensamento, tudo com vista a estabelecer novos caminhos para a monetização e o lucro. O **Big Other** é o poder soberano de um futuro próximo que aniquila a liberdade alcançada pelo Estado de Direito. É um novo regime de fatos independentes e independentemente controlados que suplanta a necessidade de contratos, de governança e o dinamismo de uma democracia de mercado. O **Big other** é a encarnação, no século XXI, do texto eletrônico que aspira abranger e revelar os amplos fatos imanentes de comportamentos econômicos, sociais, físicos e biológicos. Os processos institucionais que constituem a arquitetura do **Big Other** podem ser imaginados como a instância imaterial (...) que ganha vida na transparência didática da mediação por computador (ZUBOFF, 2021, p. 44).

Zuboff afirma que o maior paradoxo da atualidade é a retórica que busca convencer os indivíduos que a privacidade é algo privado, ou seja, que temos condições de decidir quais as informações pessoais damos às big techs e os usuários possuem o poder de controlar esse intercâmbio. Para a autora, a privacidade é questão pública e não privada e os riscos de renunciarmos a ela pode gerar impactos nas dimensões sociais, políticas e econômicas.

A coleta massiva de dados realizada por empresas como Google, Amazon, Facebook, Apple e Microsof, Gafam, acrônimo de gigantes da Web, gera o processo conhecido como dataficação, ou seja, tudo se transforma em dados pelas operações realizadas pelas tecnologias digitais. Importante ressaltar que esse tipo captação impacta profundamente na privacidade dos usuários. Morozov (2018) se refere ao dataísmo como uma espécie de religião das plataformas e do capitalismo contemporâneo, considerando a profunda mudança de vida na era digi-

tal. Nesse sentido, internet e smartphones são as principais ferramentas dessa era e é exatamente por meio delas que ocorre a extração massiva dos dados dos indivíduos. A tecnologia digital é um emaranhado de geopolítica global, das finanças globais, e o consumismo desenfreado gera um processo de grande apropriação corporativa até mesmo da nossa intimidade.

As tecnologias informacionais trazem novas formas de organização, mas também de exploração e os mercados emergentes dessa dinâmica apresentam novas formas de exploração da força de trabalho e também das formas de acumulação de riquezas. Significa dizer que é necessário o uso de sensores para o processo de captura e um sistema de armazenamento massivo, os data centers que podem ser físicos ou na nuvem, portanto, não se trata apenas de bases imateriais, à medida que consomem grande volume de eletricidade em âmbito global.

Os algoritmos desempenham um papel central nessa lógica pela capacidade de identificar publicações que devem ser entregues para grande número de pessoas e as que devem ser recebidas por público menor. Trata-se de dispositivos que monitoram sistemas e pessoas continuamente e desconhecemos seu funcionamento. Nesse sentido, é possível afirmar que os algoritmos são opacos, sabe-se como um dado entra no sistema e como ele sai, mas o processo de transformação, de processamento dos dados no interior desses sistemas é desconhecido. Pasquale (2015) faz analogia de algoritmo à caixa-preta, pelo fato das plataformas esconderem os procedimentos de coleta e análise de dados e esse processo garante às empresas um papel de muito destaque, tendo em vista que definem a reputação de clientes com base nessa forma obscura.

Cabe lembrar que os dados não são utilizados apenas para as atividades econômicas, para a expansão do modelo de negócios das plataformas. Ao pensarmos na dinâmica neoliberal devemos entender que os dados são utilizados em processos de dominação em outros moldes, agora colonizando os dados.

Para Avelino

> O colonialismo digital pode ser analisado a partir da prática de aprisionamento tecnológico no ecossistema digital de dispositivos eletrônicos, protocolos de rede, infraestrutura de computação em nuvem, linguagens de máquina e programação. Esse ecossistema é a via que permite à Internet realizar comunicação, transferência e processamento de dados pessoais, sistemas e serviços (...). O colonialismo digital permitiu ao capitalismo exercer seu regime de poder, que pode ser comparado às experiências de colonialidade elaboradas por Anibal Quijano (1992), fundado a ideia de desenvolvimento que determina padrões econômicos, morais e epistemológicos (AVELINO, 2023, p.106-107).

Ao pensarmos que inicialmente a internet se desenvolve como uma rede descentralizada pensada com um funcionamento sem controle governamental ou de corporações para que manter um ambiente livre, mas que aos poucos vai sendo tomada por uma proliferação de tecnologias para intensificar padrões de rastreamento e de controle, transformando essa lógica inicial e produzindo impactos políticos e sociais, tais como o aumento crescente de desinformação, discursos de ódio, teorias da conspiração, entre outros fatores que estão corroendo a dinâmica democrática em vários países e abrindo caminho para governos autocráticos.

Além disso, verifica-se que o colonialismo digital além de capturar o conhecimento através da extração da produção intelectual e científica, aprisiona os processos de criação e busca um amplo processo de privatização da cultura, da produção científica etc.

Para enfrentar o colonialismo e a apropriação indevida dos dados é preciso pensar na autonomia tecnológica, é fundamental pensarmos em formas de regular a ação das plataformas, mas também de desenvolvermos infraestruturas digitais soberanas para garantir que haja, efetivamente, uma tecnodiversidade (YUI, 2020).

> é possível – mas somente se antes reconquistarmos a soberania popular sobre a tecnologia? Sim, é possível – mas somente se antes reconquistar-

> mos a soberania sobre a economia e a política. Se a maioria de nós acredita em algum tipo de "fim da história" – sem disposição ou capacidade para questionar a possibilidade de uma alternativa do mercado na vida social -, então não resta de fato nenhuma esperança; quaisquer que fossem os novos valores contidos na internet, eles acabariam esmagados pela força da subjetividade neoliberal (MOROZOV, 2018, p. 25).

Cabe ressaltar que o processo de conquista da soberania digital ocorrerá se houver enfrentamento à lógica do capitalismo dadocêntrico e esse processo será possível se a sociedade civil for capaz de transformar em luta política, um movimento tecnopolítico capaz de organizar a luta pela soberania das infraestruturas sociotécnicas que tire o país do patamar de meros " consumidores de produtos e serviços criados por sistemas automatizados a partir do tratamento de dados extraídos de nossa população" (AMADEU, 2024).

PL 2630/20 – Lei Brasileira de Liberdade, Responsabilidade e Transparência Digital na Internet

O projeto de lei PL 2630/20 – Lei Brasileira de Liberdade, Responsabilidade e Transparência Digital na Internet, apoiado pela Coalização Direitos da Rede, frente composta por mais de 50 organizações da sociedade civil, defende a urgência na aprovação do projeto por entender que se trata de uma agenda essencial à democracia. Se aprovada a lei se aplicará a redes sociais, ferramentas de busca, serviços de mensageria instantânea e provedores de aplicações que oferecem conteúdo sob demanda.

O projeto propõe a criação de regras básicas para a moderação de conteúdos nas redes sociais, possibilitando a remoção, restrição de circulação ou sinalização de conteúdos e contas considerados impróprios ou ilegais. A lei cria mecanismos que dotam as empresas de maior transparência em seu funcionamento e também definem que sejam co-responsáveis pelos danos causados por conteúdos que circulam nas redes.

Um dos pontos da transparência é que os termos de uso das plataformas sejam disponibilizados de forma clara e objetivo, deixando claro às usuárias e usuários o que é proibido e o que fica permitido e deve deixar indicados os potenciais riscos de uso da rede e a faixa etária a que se destina.

Cabe ressaltar que além a transparência exigida às plataformas também se aplica aos algoritmos, deixando explicitadas as formas de funcionamento e os parâmetros para a recomendação de conteúdos. Com a aprovação da lei, as plataformas serão obrigadas a elaborarem relatórios de transparência semestralmente, prazo que pode ser diminuído caso haja algum motivo de interesse público, como por exemplo em caso de calamidade ou em períodos eleitorais. Os relatórios devem proteger a identidade das usuárias e usuários e informar os procedimentos utilizados pelas plataformas para as ações adotadas. O cumprimento dessas regras e obrigações deverá ser realizar auditórias externas e independentes que avaliação o cumprimento das regras estabelecidas e os impactos na moderação de conteúdos e dos algoritmos.

Nesse sentido a lei aborda o dever das plataformas de notificarem os usuários quando compartilhem conteúdos potencialmente ilegais e, caso decida fazer a moderação de algum tipo de publicação deverá informar o usuário e explicitar os motivos adotados para essa prática.

No que diz respeito à transparência, a proposta de lei define que as empresas devem divulgar de forma clara os seus termos de uso, deixando o usuário ciente do que é proibido e quais os potenciais riscos de uso da rede.

A transparência deve ser estendida aos algoritmos, considerando que só se conhecem os inputs e os outputs, o dado que entra e a informação que sai dos sistemas, mas não se sabe as formas de processado adotadas, aquilo que Pasquale (2015) denomina caixa-preta.

As plataformas devem deixar claro as recomendações de conteúdos exibidas aos usuários, no atual funcionamento da rede, essas informações são bastante opacas. Para que seja possível acompanhar o cumprimento das regras, caso a lei seja aprovada, está previsto que sejam realizadas auditorias externas e independentes para avaliarem a eficiência do

cumprimento das obrigações e os impactos da moderação de conteúdos e dos algoritmos.

O PL 2630/20 passou por processo intenso de debates com organizações da sociedade civil e é fruto da reflexão sobre a urgência de se adotar medidas regulatórias capazes de tornar a atuação das big techs mais transparentes, além de tentar impedir que as redes digitais sejam mais um espaço de aprofundamento das inúmeras desigualdades existentes na sociedade.

Referências

AVELINO, Rodolfo, **Colonialismo digital – tecnologias de rastreamento online e a economia informacional**, São Paulo: Alameda, 2023.

MACHADO, Sidnei, ZANONI, Alexandre P. (Orgs.), **O trabalho controlado por plataformas digitais:dimensões, perfis e direitos**, UFPR – Clínica Direito do Trabalho: Curitiba, 2022.

MOROZOV, Evgeny, **Big Tech: A ascensão dos dados e a morte da política,** São Paulo: Ubu, 2018.

PASQUALE, Frank, **The Black Box Society – The secret algorithms that control money and information,** Massachusetts: Harvard University Press, 2015.

PLANTIN, J.-C.; LAGOZE, C.; EDWARDS, P. N.; SANDVIG, C. 2018. Infrastructure studies meet platform studies in the age of Google and Facebook. New Media & Society, *20* (1), 293–310.

POELL, T., NIEBORG, D., VAN DIJCK, J. Plataformização in **Revista Fronteiras – estudos midiáticos**, in Vol. 22 Nº 1 – janeiro/abril 2020.

SILVEIRA, Sergio Amadeu da, Soberania Digital in: h**ttps://aterraeredonda.com.br/soberania-digital/** acesso em 08.11.2024.

SRNICEK, Nick, **Platform Capitalism**, Cambridge: Harvard Polity Press, 2017.

YUI, Huk, **Tecnodiversidade**, São Paulo: Ubu, 2020.

ZUBOFF, Shoshana, **A era do capitalismo de vigilância – a luta por um futuro humano na nova fronteira do poder,** 1ª. ed., Rio de Janeiro: Intrínseca, 2021.

Rosemary Segurado · Cientista Política, Profa. do Programa de Pós-graduação em Ciências Sociais da PUC/SP e pesquisadora do NEAMP (Núcleo de estudos em arte, mídia e política da PUCSP).

Ética e Inteligência Artificial: desafios na modulação e regulação dos algoritmos

Irineu Francisco Barreto Junior

Resumo

Este artigo examina os dilemas éticos e os desafios regulatórios associados à crescente utilização de algoritmos no contexto da Sociedade da Informação, com ênfase no papel da inteligência artificial, no capitalismo de vigilância e na consequente invasão da privacidade. Assinala que, conforme os algoritmos se tornam mais sofisticados, a opacidade dos processos informáticos e a automação de decisões tradicionalmente humanas levantam preocupações sobre a transparência e a accountability dessas tecnologias. O estudo discute como a interação entre IA e big data cria modelos que impactam diretamente a vida dos indivíduos, ao mesmo tempo em que desafiam os marcos regulatórios existentes, especialmente em relação à proteção da privacidade e dos direitos fundamentais. A análise propõe a adoção de medidas que não impeçam o avanço tecnológico, resguardem a dignidade humana e assegurem um equilíbrio entre inovação e direitos fundamentais. Conclui-se que, para garantir o uso ético e responsável da IA, é necessário um arcabouço regulatório policêntrico, capaz de proteger as liberdades individuais sem sacrificar a eficiência tecnológica.

Abstract

This paper examines the ethical dilemmas and regulatory challenges posed by the increasing use of algorithms in the context of the Information Society, with a focus on the role of artificial intelligence in surveillance capitalism and the resulting invasion of privacy. It highlights that, as algorithms become more sophisticated, the opacity of computational processes and the automation of traditionally human decisions raise concerns about transparency and accountability. The study explores how the interaction between AI and big data creates models that directly affect individuals' lives, while also challenging existing regulatory frameworks, particularly regarding privacy and fundamental rights. The analysis advocates for measures that protect human dignity and balance innovation with fundamental rights, without hindering technological progress. It concludes that a polycentric regulatory framework is necessary to ensure the ethical and responsible use of AI, safeguarding individual liberties without compromising technological efficiency.

Introdução

A inteligência artificial (IA) desponta como um dos esteios centrais da transformação digital, suscitando reflexões profundas e inadiáveis acerca de suas implicações tecnológicas, sociais e éticas. Com o progresso contínuo dos algoritmos, que se mostram cada vez mais sofisticados e abrangentes, emergem desafios incontornáveis para sua regulação sobretudo no que concerne à economia de dados e à proteção dos direitos fundamentais à privacidade e à intimidade. O avanço exponencial de técnicas de aprendizado de máquina e de análise de grandes volumes de dados (*Big Data*) não apenas catalisa a eficiência econômica, mas inaugura novas e complexas fronteiras no campo da automação de processos decisórios, até então reservados ao intelecto humano.

Todavia, o caráter opaco e insondável que permeia muitas das decisões algorítmicas impõem, de maneira inexorável, uma pauta ética que

não pode ser negligenciada. Isso se torna ainda mais preocupante à luz do fato de que tais sistemas são capazes de replicar padrões de comportamento humano sem, contudo, estarem ancorados em qualquer tipo de consciência ou responsabilidade moral. Neste cenário, o presente estudo se propõe a examinar os dilemas éticos e os desafios regulatórios impostos pelos algoritmos, à luz da chamada Sociedade da Informação.

Nesse sentido, busca analisar o papel da inteligência artificial no contexto do capitalismo de vigilância e suas implicações na invasão da privacidade. A investigação detém-se nas questões inerentes à opacidade dos processos algorítmicos, bem como nos impactos dessa tecnologia sobre a formulação de modelos decisórios que afetam, de modo direto e profundo, a vida dos indivíduos. A crescente complexidade na interação entre inteligência artificial e grandes volumes de dados pessoais exige, portanto, uma revisão crítica e apurada das estruturas regulatórias existentes, além da necessária elaboração de novos paradigmas éticos, aptos a mitigar os riscos inerentes à *era dos algoritmos*.

1. Inteligência Artificial e o Capitalismo de Vigilância

Inteligência artificial é a nomenclatura pela qual se convencionou chamar a tecnologia informática desenvolvida com o intuito de oferecer soluções para perguntas humanas, com crescente probabilidade estatística de acerto, questões cujas respostas exigem a simulação da capacidade humana de raciocinar, perceber, tomar decisões e resolver problemas. A nomenclatura *Inteligência Artificial* não é propriamente nova. Originalmente foi aplicada a processos de automação e robótica desenvolvidos desde a segunda metade do século XX. Conforme conceitua Harasim (2015, p. 74): "Inteligência Artificial é uma área da Ciência da Computação que busca fazer os computadores pensarem e se comportarem como seres humanos."

> O termo foi cunhado em 1956 por John McCarthy no *Massachusetts Institute of Technology* (MIT). Esta área da ciência tem sido tratada como

> ficção científica pela grande maioria das pessoas para as quais IA, robôs, androides e outras formas de inteligência avançada eram coisa de cinema e livros de ficção. Nos últimos anos, os aspectos ficcionais da IA estão desaparecendo ao tempo em que cientistas e o público compreendem os incríveis avanços que estão sendo feitos pela Ciência da Computação no campo da IA e os investimentos vultosos que estão sendo feitos no estudo, replicação e substituição do cérebro humano (HARASIM, 2015, p. 74).

Contemporaneamente, o modelo de IA passou a ser associado à capacidade informática de oferecer respostas para perguntas humanas, com crescente probabilidade estatística de acerto, questões cujas respostas exigem a simulação da capacidade humana de raciocinar, perceber, tomar decisões e resolver problemas. Essas perguntas são decodificadas na forma de programações informáticas denominadas a*lgoritmos*, que podem ser imaginadas como sequencias de linhas de códigos e repletas de complexos cálculos matemáticos. Na definição de Marvin Minsky, pioneiro da inteligência artificial (*apud* TEIXEIRA, 2015, p. 19), essa tecnologia pode ser compreendida como a "ciência de construir máquinas capazes de fazer operações que, habitualmente, requerem inteligência humana. Recentemente, o Conselho da União Europeia editou o *Artificial intelligence Act*[1], que define essa tecnologia como sistema baseado em máquina, projetado para operar com níveis variados de autonomia e que pode exibir adaptabilidade após o lançamento, e que, para objetivos explícitos ou implícitos, infere, a partir dos *inputs* recebidos, como gerar *outputs*, previsões, classificações, conteúdo, recomendações ou decisões que podem influenciar ambientes físicos ou virtuais.

Ao longo do século XXI as pesquisas em inteligência artificial retomam a vitalidade com a proposta de replicar artificialmente a mente

1 Council of the European Union. Artificial Intelligence Act: Council and Parliament strike a deal on the first rules for AI in the world. Disponível em: https://www.consilium.europa.eu/en/press/press-releases/2023/12/09/artificial-intelligence-act-council-and-parliament-strike-a-deal-on-the-first-worldwide-rules-for-ai/. Acesso em: 19. Set. 2024.

humana (TEIXEIRA, 2015, p. 22), com novas estratégias voltadas às aplicações que se alimentam de volumes exponenciais de dados e alcançam novos campos do conhecimento humano, como neurociência, neurobiologia, genética, nanotecnologia e robótica.

Inteligência Artificial pressupõe a programação de a*lgoritmos*, sequências de linhas de códigos repletas de complexos cálculos matemáticos. Na medida em que a revolução tecnológica propicia a digitalização de quantidades de dados que crescem de forma exponencial, os *algoritmos* se tornam cada vez mais poderosos, pois possuem a capacidade de aprender através de exemplos (*Machine Learnig*) e, dessa forma, realiza uma *simulação da compreensão humana*. Na medida em que a revolução tecnológica propicia a digitalização de quantidades de dados, cujos volumes crescem de forma exponencial, os *algoritmos* se tornam cada vez mais poderosos, pois possuem a capacidade de aprender através de exemplos. Não é possível, assim, dissociar inteligência artificial e os algoritmos de programação que, efetivamente, a fazem produzir efeitos no mundo natural.

No livro *Weapons of Math Destruction* (Armas de Destruição Matemática), Cathy O'Neil (2020, p. 19-35), aborda aspectos importantes relacionados aos algoritmos, ao afirmar que modelos matemáticos são o motor de nossa economia digital. Com base nessa premissa a autora formula dois *insights* – "que podem surpreender legiões de pessoas que veem as máquinas como simplesmente "neutras":

> 1) Aplicações baseadas em matemática e que empoderam a Economia de Dados são baseadas em escolhas feitas por seres humanos falíveis.
> 2) esses modelos matemáticos são opacos, e seu trabalho é invisível para todos, exceto os cardeais em suas áreas: matemáticos e cientistas computacionais. Seus vereditos são imunes a disputas ou apelos, mesmo quando errados ou nocivos (O'NEIL, 2020, p. 19-35).

Inteligência Artificial não significa, portanto, autonomia das máquinas na tomada de decisões ou exercício de uma ilimitada discriciona-

riedade informática. Com base na inteligência artificial, programadores informáticos, que recentemente passaram a ser chamados de *cientistas de dados,* propiciam a interação entre os usuários/clientes das aplicações por eles desenvolvidas e equipamentos/dispositivos com elevada capacidade computacional de armazenagem e processamento de dados. Com base na programação, a IA é capaz de estabelecer a relação estatística entre palavras, traduzindo-a e tornando-a inteligível na linguagem computacional e, nas aplicações de inteligência artificial generativa, devolvendo-a em linguagem natural. Esses e outros desafios da regulação algorítmica serão abordados na próxima unidade desse artigo.

2. Desafios Éticos e Tecnológicos na Regulação dos Algoritmos

Antes de tratar da necessidade de limites éticos para as aplicações de inteligência artificial (IA), é imperativo compreender e esmiuçar os principais aspectos do funcionamento tecnológicos dessa programação informática. Suas aplicações atingem novos patamares de desenvolvimento tecnológico que, que por sua vez, impulsionam a substituição da mão de obra humana pelo trabalho de máquinas. Esse processo não é recente. Desde meados do século XVII, inovações tecnológicas têm substituído o trabalho do homem na realização de atividades braçais, mecânicas ou repetitivas. Mais recentemente, a partir do término do século XX, a tecnologia passa a substituir atividades antes realizadas pelo intelecto humano. Abramovay (2024, *on-line*) assinala que "a maior ameaça ligada à Inteligência Artificial (AI) deriva do fato de que as máquinas conseguem mimetizar nossos padrões de comportamento ético, mas, por definição, não podem e jamais poderão se dotar de consciência ética."

A revolução tecnológica ocorrida nos meios de comunicação, desde meados da década de 1990, deu origem a uma nova era denominada *Sociedade da Informação*. A sua principal característica é a geração e propagação de informações, advindas de qualquer lugar do mundo,

em tempo quase que real e de forma inédita na história da tecnologia. Denota-se que a *informação é o centro gravitacional* desta nova era ou, em outras palavras, é possível afirmar que ela possui valor comercial (BARRETO JUNIOR, 2015, p. 100-127). Nesse contexto, a inteligência artificial pode ser conceituada como "a aplicação de técnicas ou teorias cujo objetivo é utilizar máquinas para reproduzir a inteligência humana".

A falta de inteligibilidade dos algoritmos, que forma a estrutura cognitiva da inteligência artificial merece destaque, torna indecifrável para leigos e, como destaca O'Neil (2020, p. 8), são representações computacionais de formulações humanas, desde logo falíveis e voltadas a oferecer respostas para questões eminentemente humanas. Em razão disso faz todo o sentido abordar a necessidade de submeter a IA ao debate sobre o teor ético de sua formulação. Daí o conceito de *Armas de Destruição Matemática* (WMDs), de O'Neil, ou, em suas palavras, "modelos matemáticos destrutivos que estão acelerando um terremoto social." Sua obra detalha como "modelos matemáticos destrutivos microgerenciam vastas faixas da economia real, da publicidade ao sistema prisional, sem falar do sistema financeiro e dos efeitos posteriores à interminável crise de 2008." Afirma ainda que "os modelos matemáticos são *essencialmente opacos, não responsáveis*; e miram acima de toda "otimização" das massas consumidoras" e "os sistemas são construídos para devorar mais e mais dados, e afinar suas análises de modo a despejar neles [nos sistemas] mais e mais capacidade de gerar valor (O'NEIL, 2020, p. 13)."

A economia algorítmica inaugura um novo estágio de desenvolvimento econômico denominado *sociedade de plataforma,* cujo cerne é formado pelo tráfego social e econômico, cada vez mais capilarizado, dentro de um ecossistema global de redes *online* formatadas por algoritmos e alimentado por dados. Dentro do referido modelo de negócios, "a informação em si não é o que alavanca eficiência na atividade empresarial, mas o seu processamento-organização a ser transformado em um conhecimento aplicado" (BIONI, 2022a, p. 38). Em posse dessas informações sobre os usuários, as empresas de tecnologia têm uma minuciosa segmentação do perfil do indivíduo, tanto em relação às questões

objetivas, como às subjetivas, sem ciência do sujeito quanto ao destino da coleta de dados pessoais.

Sob essa perspectiva, tem-se o chamado Capitalismo de Vigilância (ZUBOFF, 2020, p. 153) novo modelo econômico informacional cujos objetivos são prever e modificar o comportamento humano. Esse novo estágio de desenvolvimento econômico resulta da revolução tecnológica ocorrida nos meios de comunicação, desde meados da década de 1990, originária da nova era denominada Sociedade da Informação. A sua principal característica é a geração e propagação de informações, advindas de qualquer lugar do mundo, em tempo quase que real e de forma inédita na história da tecnologia.

Além da coleta dos dados pessoais, os algoritmos das *Big Techs* coletam e tratam dados das interações realizadas online, processos de captura, análise e utilização de informações psíquicas e emocionais extraídas dos registros disseminados em plataformas digitais. É por meio da economia psíquica que o modelo de negócios das plataformas triunfa, utilizando matrizes preditivas e *captológicas* (técnicas de persuasão e retenção do usuário endossam o mecanismo de vigilância trazendo mais uma camada de controle), sugerindo realização de tratamento indevido de dados sensíveis para fins econômicos, que evidenciam as estruturas do capitalismo de dados que utilizam de suas ferramentas em prol da monetização algorítmica, em detrimento da transparência e da autodeterminação informativa.

Apenas precisar e prever o comportamento do usuário não foi suficiente para as empresas líderes do Capitalismo de Vigilância, e mais eficiente do que prever com precisão as atitudes dos usuários conectados, é mantê-los engajados nas plataformas por meio da matriz *captológica*. Nir Eyal (2020, p. 147), designer comportamental aclamado pelo Vale do Silício, em sua obra *Hooked*, discute "como construir produtos e serviços que modulam hábitos humanos por meio da utilização das plataformas e alcançar, assim, o maior engajamento do usuário no ambiente online". No contexto tecnológico – ambiente onde há excesso de estímulos e que o tempo é finito, a atenção dos indivíduos é disputada pelas

plataformas digitais. O foco na formação de hábitos aditivos é importante, se os algoritmos se alimentam de dados, necessitam que o usuário esteja conectado o maior tempo possível – perpetrando um ciclo de influência de comportamento e captura massiva da atenção dos usuários.

Dessa forma, a constatação de que a IA realiza uma *simulação da compreensão humana* é imprescindível na abordagem da necessidade de imperativos éticos na sua aplicação. Outro aspecto característico do tratamento informático de dados, por meio da inteligência artificial, reside na compreensão de que essa técnica é consubstanciada na aplicação de sofisticadas tecnologias de coleta, processamento e análise estatística de grandes massas de dados, comumente denominadas como *Big Data*[2]. Essa técnica foi possível com o desenvolvimento de equipamentos com elevada capacidade de armazenagem, processamento e aplicações capazes de tratar bilhões de registros em servidores físicos e virtuais (denominada armazenagem de nuvem – *Cloud*) com o intuito de obter a resposta almejada. Quanto maior o volume de dados analisados, há uma tendência de aumento da acurácia estatística de acerto da resposta algorítmica. Em suma, *eleva-se a chance estatística da IA oferecer a resposta correta ao problema formulado pelos cientistas de dados*, que traduziram as questões humanas em linguagem computacional. Com a inteligência artificial generativa cada usuário se torna um cientista de dados em potencial, o que exige a disseminação do conhecimento sobre o uso adequado e limitações dessa tecnologia.

A sucessiva formulação de novas perguntas (ou novos *prompts*) coopera com a "*calibragem estatística*" da resposta formulada pela IA impulsionando um círculo virtuoso: *quanto maior a quantidade de dados processados, maior é a probabilidade estatística de acerto da resposta ofe-*

2 "*Big Data* é a tecnologia capaz de processar e analisar estatisticamente qualquer tipo e volume de dados – estruturados ou não – como textos, áudios, vídeos, cliques, registros, imagens e outros. *Big Data* é mais do que apenas uma questão de tamanho: é uma oportunidade de descobrir insights em novos tipos de dados e conteúdo, para tornar o seu negócio mais ágil. " In: Cukier; Mayer-Schönberger, 2012, p. 45.

recida pela inteligência artificial. É necessário realizar uma diferenciação entre *Inteligência Artificial* e *Machine Learning,* a denominada aprendizagem de máquina. Nessa última tecnologia, programas informáticos possuem a capacidade de tornarem-se mais inteligentes ou aprenderem com exemplos, como permite supor sua nomenclatura, processo que se desenrola no âmbito do processamento de dados algorítmico.

Maranhão (2024, *on-line*) comenta sobre essas tecnologias que "técnicas de processamento" de linguagens naturais e *Machine Learning* são treinados a partir de um corpus de dados relevantes, sobre os quais são construídas ontologias, que representem as relações semânticas entre os termos e conceitos empregados. Na sua percepção, uma vez treinados, esses sistemas podem interagir com textos aos quais ainda não foram expostos, generalizando os conceitos representados nas ontologias e as interações entre eles. Essas interações formam a base lógica de aplicação da Inteligência Artificial. Em decorrência da estreita dependência tecnológica no emprego da IA, uma das grandes preocupações éticas decorrentes do emprego dessa tecnologia está no fato de que tais sistemas podem desenvolver correlações baseadas em abordagens meramente vazias de sentido humano e, a partir delas, propiciar a tomada de decisões cujo fundamento ético é de difícil apreensão.

Algoritmos representam um dos ativos mais valiosos na era da informação como mercadoria, como insumo para geração de valores. A inteligência artificial permite o desenvolvimento de *algoritmos inteligentes*, que aprendem com a própria experiência e passam a selecionar autonomamente as variáveis que considera mais adequadas para solucionar o problema proposto.

3. Opacidade na aplicação de dados pessoais em Inteligência Artificial

O raciocínio lógico, até aqui exposto, aponta para questão significativa e cuja abordagem é imprescindível na perspectiva dos limites éticos da Inteligência Artificial: essa enorme massa de dados que ali-

menta a IA é originária – em substancial medida –de dados pessoais dos usuários da internet. Yves Alexandre de Montjoye (2024, *on-line*) afirma que o primeiro obstáculo na aplicação tecnológica dos algoritmos é garantir a privacidade dos indivíduos:

> Como os algoritmos têm acesso a dados provenientes de um número crescente de fontes, mesmo se esses dados são anônimos, a partir de seu cruzamento e combinação seria possível inferir algumas características sobre uma pessoa em particular, ainda que essa informação nunca tenha sido divulgada pelo indivíduo. Felizmente, medidas podem ser tomadas para minimizar ou eliminar o impacto sobre a privacidade, tais como a agregação de dados anônimos. O desenvolvimento de algoritmos para a tomada de decisões com base em dados reflete a busca da objetividade e da aspiração de decidir baseando-se em evidências de modo a eliminar – ou pelo menos minimizar – a discriminação, a corrupção, a injustiça ou a ineficiência das quais, infelizmente, as decisões humanas não escapam (MONTJOYE, 2024, *on-line*).

A proteção da privacidade torna-se cada vez mais desafiadora na Sociedade da Informação. Perdeu-se, com a tecnologia, a possibilidade de assegurar a diferença entre *pessoa identificada e identificável*. A dicotomia entre dados anônimos (sigilosos) e dados pessoais identificáveis não é mais viável em decorrência do aparato tecnológico e das técnicas de *linkage* de bancos de dados, além do georreferenciamento. Conforme exposto por Bioni (2022b, p. 34), desenvolve-se a necessidade de formulação de um novo conceito de privacidade associado a uma liberdade positiva – não mais negativa, que se refere ao controle da aplicação das informações pessoais a ser exercido pelo dono desses dados, ou seja, a assunção da *autodeterminação informacional* quanto à aplicação dos dados pessoais.

Reside na possibilidade, daquele que cede os dados, de exercitar o controle sobre a captação (coleta), tratamento aos quais são submetidos seus registros pessoais e tomar conhecimento das aplicações aos quais

serão submetidos. Ainda conforme Bioni (2022b, pa.34), a revolução tecnológica das últimas décadas impõe novos e grandiosos desafios para a privacidade e proteção dos dados pessoais que alimentam as máquinas e algoritmos de inteligência artificial. A privacidade historicamente foi associada a uma liberdade negativa, ao direito de não mostrar algo, de não expor, esconder, cobrir. A privacidade, portanto, não parece mais executável em tempos de economia alimentada pela coleta, tratamento e geração de valor a partir de dados pessoais disseminados pela internet.

No intuito de mitigar essa vigilância extrema e para que se possa desenvolver um ecossistema de confiança para as sociedades e economias baseadas em dados é imprescindível respeitar as *legítimas expectativas dos usuários* (BIONI, 2022b, p. 40) quando são levados a ceder seus dados pessoais em troca das aplicações e serviços. Essas iniciativas são necessárias para preservar direitos muito caros na tradição liberal contemporânea, os direitos de proteção do indivíduo contra a violabilidade da sua intimidade pelo Estado e agora pelo Mercado. Para Maranhão (2024, *on-line*), "como os dados processados podem ser enviesados, as decisões automáticas decorrentes podem interferir em direitos individuais, sem que o programa ou os desenvolvedores consigam sequer apresentar justificativas humanamente compreensíveis sobre quais foram as razões de sua decisão." Dessa forma, para Maranhão, "além da preocupação de a Inteligência Artificial poder extrair o conhecimento por trás de decisões baseadas em algoritmos complexos envolvendo aprendizado de máquina, existe a preocupação jurídica com a regulação e garantia dos direitos daqueles que são afetados por tais decisões (MARANHÃO, 2024, *on-line*)."

Foi possível expor, portanto, nessas duas unidades do artigo, como a Inteligência Artificial processa grandes volumes de dados para oferecer respostas e predizer o comportamento humano. E que parcela significativa do insumo usado em suas aplicações é originária de dados pessoais de usuários de Internet. Foram perpassados aspectos éticos que são mitigados ou relativizados, principalmente na incapacidade tecnológica de estabelecer freios para suas aplicações, o que é inerente, e da opacidade dos mecanismos de captação e tratamento de dados pessoais.

Considerações finais

Diante do exposto, resta evidente que a crescente inserção da inteligência artificial em diferentes esferas da vida social e econômica exige uma reflexão profunda sobre os seus impactos éticos e jurídicos. A evolução vertiginosa das tecnologias digitais, por meio do desenvolvimento de algoritmos cada vez mais complexos e autônomos, desafia os marcos regulatórios vigentes e impõe ao legislador e ao intérprete da norma a tarefa de reavaliar os conceitos tradicionais de privacidade, autodeterminação informativa e responsabilidade.

A inteligência artificial, ao atuar como agente decisório em situações que afetam diretamente a vida e os direitos fundamentais dos cidadãos, demanda a imposição de limites éticos claros e precisos. A opacidade inerente aos algoritmos e a capacidade das máquinas de processar volumes incomensuráveis de dados pessoais devem ser contrabalançadas por um sistema jurídico que assegure a transparência e a accountability no uso dessas tecnologias. É inaceitável que decisões automatizadas, muitas vezes invisíveis ao olho humano, perpetuem desigualdades e consolidem discriminações estruturais.

Além disso, cabe ao Estado, na qualidade de guardião dos direitos e garantias fundamentais, promover um ambiente regulatório que não apenas estimule a inovação tecnológica, mas também proteja a dignidade da pessoa humana contra os abusos que podem emergir do capitalismo de vigilância. Urge que as instâncias democráticas, em conjunto com a sociedade civil, estabeleçam um arcabouço normativo robusto, capaz de garantir que a revolução digital sirva ao bem comum, sem sacrificar as liberdades individuais no altar da eficiência tecnológica.

Neste sentido, é imperativo que o debate sobre a inteligência artificial, em suas múltiplas facetas, não se restrinja aos círculos acadêmicos ou ao âmbito das grandes corporações tecnológicas, com vistas à construção de um consenso social que assegure o uso ético e responsável dessas ferramentas. Somente assim será possível construir um futuro em que a tecnologia sirva como instrumento de promoção da justiça e

do desenvolvimento humano, e não como veículo de exclusão e vigilância desmedida.

Referências

ABRAMOVAY, Ricardo. Inteligência artificial pode trazer desemprego e fim da privacidade. **Jornal Folha de S. Paulo**, 02 de abril de 2017. Caderno Ilustríssima. Disponível em: http://www1.folha.uol.com.br/ilustrissima/2017/04/1871569-inteligencia-artificial-pode-trazer-desemprego-e-fim-da-privacidade.shtml. Acesso em: 23. set. 2024.

BARRETO JUNIOR, Irineu Francisco; MOLINA, Fernanda Zampieri. Capitalismo de plataforma: a ameaça ao direito à autodeterminação informativa na Sociedade da Informação. **Revista Brasileira de Estudos Políticos**, Belo Horizonte, n. 125, pp. 243-278, jul./dez. 2022.

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

BARRETO JUNIOR, Irineu Francisco; VENTURI JUNIOR, Gustavo. Inteligência Artificial e seus efeitos na Sociedade da Informação. *In*: LISBOA, Roberto Senise (Org.). **O Direito na Sociedade da Informação V.4**. São Paulo: Almedina, 2020.

BIONI, Bruno Ricardo. **Proteção de Dados Pessoais:** a função e os limites do consentimento. 3. Ed. Rio de Janeiro: Forense, 2022a.

BIONI, Bruno Ricardo. **Regulação e proteção de dados pessoais:** O princípio da accountability. Rio de Janeiro: GEN; Forense, 2022b.

CUKIER, Kenneth; MAYER-SCHÖNBERGER, Viktor. **Big Data – Como Extrair Volume, Variedade, Velocidade e Valor da Avalanche de Informação Cotidiana**. Rio de Janeiro: Campus, 2012.

EYAL, Nir. **(ENGAJADO):** Como construir produtos e serviços formadores de hábitos. São Paulo, Alfacon, 2020.

HARASIM, Linda. Educação online e as implicações da inteligência artificial **Revista da FAEEBA** – Educação e Contemporaneidade, Salvador, v. 24, n. 44, p. 25-39, jul./dez. 2015.

MARANHÃO, Juliana. **A pesquisa em inteligência artificial e Direito no Brasil**. Disponível em: https://www.conjur.com.br/2017-dez-09/juliano-maranhao-pesquisa-inteligencia-artificial-direito-pais. Acesso em: 23. set. 2024.

MONTJOYE, Yves Alexandre de. **Big Data':** antídoto contra a corrupção? Disponível em: https://brasil.elpais.com/brasil/2017/03/24/ciencia/1490358953_071638.html. Acesso em: 23. set. 2024.

O'NEIL, Cathy. **Armas de Destruição em Massa:** como o Big Data aumenta a desigualdade e ameaça a democracia. Santo André, SP: Editora Rua do Sabão: 2020.

TEIXEIRA, João de Freitas. **O cérebro e o robô:** inteligência artificial, biotecnologia e a nova ética. Coleção Ethos. São Paulo: Paulus, 2015.

ZUBOFF, Shoshana. **A Era do Capitalismo de Vigilância:** A luta por um futuro humano na fronteira do poder. Rio de Janeiro: Intrínseca, 2020.

Irineu Francisco Barreto Junior • Pós-Doutor em Sociologia pela Faculdade de Filosofia, Letras e Ciências Humanas (FFLCH), da Universidade de São Paulo – USP. Doutor em Ciências Sociais pela Pontifícia Universidade Católica de São Paulo – PUC-SP. Professor do Programa de Mestrado em Direito da Sociedade da Informação e do Curso de Graduação em Direito do Centro Universitário das Faculdades Metropolitanas Unidas (FMU-SP). Analista de Pesquisas da Fundação Seade – SP. Pesquisador do Centro de Ciências de Dados para Estatísticas Públicas. Membro da Comissão de Direito Constitucional da OAB-SP. neubarreto@hotmail.com

Internet das Coisas, inovação e desafios: oportunidades, riscos e o papel do Estado em sociedades datificadas

Sivaldo Pereira da Silva
Vivian Peron

Resumo

A expansão da Internet das Coisas (IoT), com infraestrutura de sensores e dispositivos conectados que absorvem e processam dados, tem transformado espaços físicos em fontes de produção e captação informação. Neste cenário, o principal objetivo deste artigo é caracterizar como sistemas de IoT são uma forma inovadora de datificação da vida que abre oportunidades e riscos, apontando qual do papel do Estado nesse fenômeno emergente. Constatou-se que o Estado tem diante de si desafios significativos para criar normas que equilibrem proteção de direitos e estímulo à inovação neste campo, além de garantir infraestrutura tecnológica necessária. Modelos regulatórios multissetoriais são recomendados para lidar com as tensões entre o potencial transformador da IoT e os riscos de ampliação de ataques, vigilância e controle.

Abstract

The expansion of the Internet of Things (IoT), with its infrastructure of sensors and connected devices that capture and process data, has transformed physical spaces into sources of information production and collection. In this context, the primary objective of this article is to charac-

terize how IoT systems represent an innovative form of life datification that creates both opportunities and risks, highlighting the role of the State in this emerging phenomenon. It was found that the State faces significant challenges in creating regulations that balance the protection of rights with the promotion of innovation in this field, in addition to ensuring the necessary technological infrastructure. Multisectoral regulatory models are recommended to address the tensions between the transformative potential of IoT and the risks of increased attacks, surveillance, and control.

1. Introdução

Um dos pilares das inovações tecnológicas deste século é o exponencial aumento da produção e disponibilização de dados. Este fenômeno está intimamente ligado ao processo de *datificação* da vida, marcado pela difusão de aparelhos conectados que passaram a compor o ecossistema social e o tecido cultural contemporâneo. Isso vem se consolidando através do alargamento gradual de infraestruturas e microestruturas interligadas, composta por camadas físicas e lógicas. Capilarizadas no cotidiano, as pontas desse sistema são aquilo que nos é mais visível, apresentando-se na forma de dispositivos sociotécnicos como celulares, aplicativos, computadores, câmeras, wi-fi e conexões 5G.

A Internet das Coisas (Internet of Things – IoT) consiste na expansão deste cenário. Implica em um substancial fortalecimento da infraestrutura de *datificação* através da presença intensificada de máquinas e objetos conectados. Nestas primeiras décadas do século XXI isso está em fase de florescimento e a sua evolução ampliará enormemente a capacidade humana de compreender o mundo e, por consequência, de agir sobre este. Não apenas sobre o mundo natural, mas também sobre a vida social e, em última instância, permitirá compreender mais sobre o indivíduo enquanto unidade comportamental integrado a modelos estatísticos descritivos e preditivo avançados.

Muito mais que o exemplo banal de uma geladeira capaz de se conectar com os produtos e avisar quando algum deles está prestes a acabar, o que concretamente é relevante na concepção de Internet das Coisas é a sua capacidade de *datificar* o mundo. O que importa não é o que a geladeira faz, mas o que a geladeira apreende em termos de informação e aprende com nosso comportamento e como essa informação é processada, utilizada e, principalmente, como isso nos é devolvido. O que faz a geladeira parecer inteligente é a sua capacidade em se comunicar como se estivesse no mesmo nível cognitivo e emocional que o nosso e, para isso, requer captar dados, abrir-se sensitivamente para tal.

Não por acaso, um dos elementos centrais da IoT são os sensores. Onde estão? O que captam? Como armazenam e processam dados? Quais dados? Para quais finalidades? E quem são seus detentores? Sobretudo, o uso em larga escala de sensores é capaz de captar um amplo leque de informação e converter espaços físicos antes vazios em câmaras de produção de dados. Como isso pode significar um ganho de conhecimento com impactos positivos, ajudando a melhorar e baratear processos, prevendo catástrofe, otimizando serviços públicos, agilizando a resolução de crises, tornando a vida mais confortável etc. Ao mesmo tempo, é preciso discutir como o funcionamento desta infraestrutura pode também ampliar violações de direitos, inviabilizar a noção de privacidade e criar problemas de segurança pública.

Tendo como premissa que o processo de *datificação* é uma força vital que se assemelha ao *Zeitgeist* do século XXI e significa um salto epistemológico importante, considera-se necessário debater seus rumos, estabelecer seus princípios e limites. Pressupõe-se, nestes termos, que tal fenômeno requer a ação direta do Estado por implicar no manuseio de recursos estratégicos (dados) com potencial benefício público e, ao mesmo tempo, por ampliar o leque de ameças à segurança pública ou violação de direitos individuais e coletivos. Diante disso, o principal objetivo deste artigo é caracterizar como sistemas de IoT são uma forma inovadora de *datificação* da vida que abre oportunidades e riscos, apontando qual do papel do Estado nesse fenômeno emergente.

Assim, artigo segue dividido em três seções subsequentes.Primeiramente, será configurado um quadro conceitual e prático sobre o que é e como funciona IoT, apontando para os tipos de inovação e oportunidades que este fenômeno implica. Na seção seguinte, serão identificadas as fragilidades inerentes aos dispositivos e sistemas de IoT, seus problemas e riscos, sobretudo no tocante à violação de direitos e segurança. Por fim, a última seção será dedicada a configurar o papel do Estado no estabelecimento políticas digitais promissoras capazes de lidar com as oportunidades e riscos gerados por estes sistemas.

2. Internet das Coisas: inovação, infraestrutura e funcionamento

Para compreendermos de modo mais consistente como funcionam a IoT convém, primeiramente, fazermos um paralelo com a Internet convencional, tal como a conhecemos e apontar diferenças. A Internet nasce incialmente como uma pequena rede de computadores de médio porte; ampliou-se posteriormente deixando de ser restrita e ao incluir computadores pessoais; e expandiu-se ainda mais ao incorporar aparelhos computacionais portáteis (como *smartphones, tablets* e afins) conectados por protocolos comuns através do qual se trafega conteúdos multimidias gerados por indivíduos ou organizações.

A Internet das Coisas (IoT) parte deste mesmo modelo básico de máquinas conectadas trafegando informação em rede, porém com três inovações importantes: (1) aquilo que é conectado passa a ser também todos os tipos de máquinas e outros objetos; (2) o fluxo de informação e comunicação deixa de ser centrado em indivíduos e organizações e passa a incorporar outras máquinas e objetos que se comportam como entes ativos formando um ecossistema de informação híbrido; (3) e, por fim, o que é colocado em rede vai aquém e além de conteúdo multimídia como texto, som ou imagem. Aquém porque boa parte dos dados de *input* que trafegam em IoT são unidades extremamente básicas e primárias de informação que buscam representar o mundo a partir de seus

indicadores mínimos. E vai além porque esta captação de dados ganha a escala de milhões e bilhões de *Gi`gabits* com amplitude e granulação, conseguindo assim descrever eventos em detalhes e desenvolver modelos estatísticos robustos.

Neste sentido, quando falamos de IoT estamos falando de uma rede microestruturas e infraestruturas que captam e processam quantidades inéditas e volumosas de informação capazes de potencializar o conhecimento sobre o mundo. Esta cadeia é extremamente relevante pois nos ajuda a vislumbrar na prática como os sistemas de IoT operam; como se caracterizam; onde estão suas fragilidades e como podem ser inovadoras. Portanto, quando falamos de IoT não devemos pensar no objeto ou no aparelho conectado e sim na cadeia de dispositivos e infraestrutura que conectam esse aparelho.

Muitos autores se propõem a explicar o funcionamento da IoT a partir da concepção de camadas (ATTIA, 2019; MISHRA; PAUL, 2020; SHACKELFORD, 2020; GREENGARD, 2021; KOPETZ; STEINER, 2022; CHIARA, 2022). Para efeito deste artigo e levando em conta essas diversas contribuições, consideramos útil explicar tais camadas nomeando-as por tipos de ação assumida, posicionada na cadeia de *datificação* dos sistemas de IoT. Neste sentido, podemos identificar seis camadas fundamentais: (1) Captação; (2) Leitura; (3) Conexão; (5) Transporte; (6) Armazenamento e (7) Processamento.

As primeiras camadas dos sistemas de IoT são aquelas nas quais residem os elementos mais originais e que carregam o sentido de inovação das coisas conectadas. A camada de captação é composta por sensores e *tags* e se configuram como um sistema de entrada de dados possibilitando a primeira ação de *datificação*: a identificação. Para produzir conhecimento sobre algo (e eventualmente ter poder sobre isso) precisamos identificá-lo, minimamente. Neste processo, os elementos de identificação dos objetos podem ser *tags* que não são máquinas e não funcionam com base energética, mas tem a função primordial de servir como marcador acoplado ao objeto que será mapeado e conectado por leitores. Podem ser também sensores que operam com alguma

forma de energia subjacente, sendo ativos no processo de comunicação ao emitir sinais para outros objetos ou sensores em seu raio de atuação. Por exemplo, etiquetas de RFID são dispositivos de identificação que contêm um código eletrônico associado a um objeto físico. Estas etiquetas podem ser passivas ou ativas. Os RFIDs passivos não possuem fonte de energia própria e são acionadas por campo elétrico emitido por um leitor RFID. Já as etiquetas ativas são microdispositivos com fonte de energia própria, que permite ações mais avançadas, transmitindo sinais a distâncias maiores e integrando sensores (TZAFESTAS, 2018; KOPETZ; STEINER, 2022).

Geralmente, os sensores são estruturas extremamente simplificadas e por isso operam com baixíssimos níveis energéticos. Seja através de *tags* ou sensores, a identificação é apenas a primeira etapa deste processo de datificação. A segunda camada é responsável pela leitura. Os leitores são instrumentos voltados para perceber e registrar dados de embutidos *tags* ou emitidos por sensores (RDIF, *blue tooth*). Os leitores rastreiam, mapeiam, captam e decodificam dados brutos e primários. Na prática, são estruturas que operam nesta cadeia recebendo e organizando os fluxos de dados em primeira instância. Na terceira camada, temos os conectores que são infraestruturas de comunicação sem fio que possibilitam o rápido fluxo desses dados coletados para um primeiro estágio de armazenamento e processamento em estações mais próximas. São as redes sem fio como wif-fi, 4G, 5G e 6G. Na quarta e quinta camada os dados atingem a infraestrutura de transporte de longa distância da internet constituída por *backhauls* e *backbones*, marinhos e terrestres (SILVA; BIONDI, 2012; TANCZER et al, 2019; YOO, 2019) além de *datacenters* na camada de armazenamento e processamento onde operam computação em nuvem ou *edge computing* (computação de borda).

Na prática, toda a infraestrutura de IoT e suas camadas fortalecem uma de computação ubíqua onde tudo pode ser registrado e analisado ampliando enormemente a capacidade de conhecer eventos. Do ponto de vista da inovação de processos, isso traz, naturalmente, diversos benefícios que podemos sintetizar nos seguintes termos:

a) Monitoramento – Sistemas de IoT transformam ambientes e objetos antes inertes em valores estatísticos ou, visto por outro ângulo, como entes que produzem dados. Isso permite um robusto sistema de acompanhamento de processos, *insights* em tempo real e, em última instância, maior controle.

b) Operacionalização – A IoT permite melhor eficiência no funcionamento de máquinas. sistemas de objetos e sistemas de ações humanas. Sobretudo por que produzem informações que permitem tornar operações menos susceptíveis a erros cujo resultado é uma melhoria no desempenho de sistemas existentes, mas também novas características incluindo algumas que ainda inexistentes (GREENGARD, 2021). Neste sentido, para Kopetz e Steiner (2022) isso significa forças inovadoras que influenciam a criação de novos mercados e a produtividade em diversos setores:

> We distinguish between *technology push* and *technology pull* forces. The *technology push forces* see in the IoT the possibility of vast new markets for novel ICT products and services, while the *technology pull forces* see the potential of the IoT to increase the productivity in many sectors of the economy (KOPETZ; STEINER, 2022, p. 325)

c) Impactos econômicos – Esse monitoramento constante aliado à otimização operacional tem um efeito econômico relevante uma vez que possibilita melhor utilização de recursos evitando perdas bem como prejuízos decorrentes do mal funcionamento de sistemas e máquinas (NICOLESCU et al, 2018; MAGRANI, 2018; ATTIA, 2019; VOULGARIDIS et al. 2022). Isso não está apenas restrito a grandes organizações:

> The Internet contributes to increased productivity in large companies and it is even more important for small and medium-sized enterprises and start-ups. There was a survey involving 4,800 SMEs in 12 countries. And it was found that the enterprises using Internet technology,

> increased revenue twice as fast as businesses with minimal use of the Internet of Things. These results can be applied to all economy sectors (KARLOV et al 2019, p. 8).

d) Intensificação da Automação – IoT facilita a automação de várias tarefas diárias, conectando dispositivos que podem trabalhar em conjunto sem a necessidade de intervenção manual. Isso tem uma relação direta com o desenvolvimento de sistemas de Inteligência Artificial atuando em diversos setores e de forma localizada:

Cada vez mais dispositivos digitais são capazes de processar tarefas localmente. Os dados são transmitidos a partir de sensores em um dispositivo, como um robô ou veículo autônomo. Enquanto o sistema de IA de borda realiza os cálculos, ele armazena os resultados no próprio dispositivo. Em alguns casos, esses dados podem ser enviados para a nuvem. Esse modelo permite que os dispositivos operem de forma mais rápida, inteligente e com menor consumo de energia. Isso muda radicalmente o modo como as máquinas autônomas funcionam e prolonga a vida útil das baterias dos sensores por anos (GREENGARD, 2021, p. 40)[4]

e) Prevenção e mitigação – Sistemas de IoT têm implicações diretas na predição e tratamento de problemas que envolvem saúde pública, emergências sociais ou catástrofes. Diversos sensores estão sendo desenvolvidos e testados para conectar o corpo humano em tempo real e produzir informações biológicas que serão fundamentais para prevenção e tratamento de doenças. Dispositivos interconectados criam uma nova fronteira para a interação entre medicina e paciente. A expressão Internet of Body (IoB) enfatiza este campo emergente (LEENES et al 2018). Para além do corpo, sensores encravados no meio ambiente criam redes de proteção e mitigação de eventos ambientes com potencial dano coletivo (SHACKELFORD, 2020).

4 Tradução própria do original em inglês.

Como vimos, do ponto de vista histórico, significa falarmos em um potencial *turn point* epistemológico. Do ponto de vista sociotécnico, implica em pensarmos em uma ampliação da infraestrutura e do aparato de vigilância e *dataveillance* (DIJCK, 2014). Por isso, qualquer conceito mais consistente de IoT deve se ater ao caráter de rede massiva de sensores embutidos nas coisas, nos ambientes e nas práticas culturais e toda a sua cadeia de transporte e processamento de dados em larga escala e suas conequências.

3. Fragilidades, problemas e riscos

Sistemas de IoT tendem a ser ubíquos atuando na captação massiva de dados e possibilitando o gerenciamento de bens e serviços de bilhões de usuários. Por isso, o fluxo de dados precisa ser constante e confiável e suas falhas podem ter um largo espectro de consequências que vão desde inconvenientes mais simples até impactos mais graves, com possibilidade de colocar vidas em risco (GREENGARD, 2021; SHACKELFORD, 2020; TZAFESTAS, 2018). Na prática, dispositivos de IoT são bem mais vulneráveis a ataques justamente por serem, na ponta, extremamente simplificados, operando com baixíssimo nível energético, e, por isso, com baixa capacidade de operar recursos de segurança. Paralelamente a isso, há a questão da escala de introdução dos dispositivos de IoT no cotidiano (SHACKELFORD, 2020). Com o crescente uso de IoT em diversas atividades humanas, envolvendo serviços e produtos utilizados por grande volume de pessoas, a conjunção entre vulnerabilidade a ataque e impacto demográfico se torna um problema especialmente importante. Se por um lado um ataque cibernético em dispositivos tradicionais tem um efeito individual e isolado (por exemplo, em um computador, ou celular), por outro lado, um ataque a uma rede de dispositivos de IoT pode ser especialmente crítico pois operam em uma escala muito maior cuja dimensão é coletiva.

Neste sentido cada uma das camadas da cadeia dos sistemas de IoT podem sofrer diferentes tipos de ataques. Podemos aglutinar os riscos

quanto à segurança de sistemas de IoT em 4 categorias mais relevantes: (a) ataques de funcionamento; (b) ataques de comunicação; (c) ataques de identificação; (d) ataques de invasão. Convém sintetizar como cada tipo de problemas de segurança se caracterizam e seus efeitos.

Os ataques de funcionamento são aqueles que visam inviabilizar a operação do dispositivo, tornando-o inativo. Um bom exemplo são os chamados "ataque de privação de sono" (*sleep deprivation attack*). O objetivo é inviabilizar energeticamente o funcionamento de dispositivos de uma rede impedindo-os de economizar energia, tendo em vista se caráter diminuto especialmente na camada de captação. Os dispositivos são assim programados para "hibernar" e assim economizar recursos energéticos. Este tipo de ataque impede que haja essas pausas mantendo -os continuamente ativos, o que resulta em um rápido esgotamento da energia e, consequentemente, no seu desligamento (KHAN; SALAH, 2018).

No caso de ataques de comunicação, a ação se dá na camada de transporte de dados nas redes sem fio. Um exemplo é o ataque baseada em interferência de sinal de rádio (*Jamming Adversaries*) quando um agente emite sinais clandestinos de rádio bombardeando os equipamentos que passam a ficar sobrecarregados impedindo-os de se comunicar com outros artefatos regulares da rede. No nível mais básico pode degradar o fluxo de comunicação tornando o transporte de dados mais lento. No nível mais alto, pode impedir a comunicação bloqueando o transporte de dados, isolando sensores e dispositivos da rede (MISHRA; PAUL, 2020).

Já os ataques de identificação estão baseados em uma importante característica dos sistemas de IoT que é o reconhecimento de objetos como entes únicos assumindo determinados papeis na rede. Um bom exemplo são os denominados ataques *Sybil* quando um invasor insere na rede identidades falsas de objetos ou sensores, possibilitando-o assim de controlar a inserção de dados e assumir o fluxo de informação, manipulando-o. Em um cenário industrial, por exemplo, um invasor poderia inserir identidades falsas em uma rede de sensores, produzindo dados incorretos sobre temperatura e umidade e fazendo com que as máqui-

nas funcionem a partir de parâmetros distorcidos e inexistentes (KHAN e SALAH, 2018). Ataques de identificação também podem ocorrer no nível físico, por exemplo, ao se vincular um objeto falsificado a uma etiqueta legítima quebrando assim o vínculo entre objeto físico e seu representante digital (KOPETZ; STEINER, 2022).

Quanto aos ataques de captura estes ocorrem quando objetos da rede se tornam porta de entrada para que usuários não autorizados tenham acesso aos dados armazenados ou transportados, quebrando a privacidade do sistema. Invasores podem usar *scripts* maliciosos ou *sniffers* para capturar a ID de uma sessão e, assim, assumir o controle da sessão. Com isso, obtêm acesso não autorizado ao servidor, podendo explorar informações privadas (MISHRA; PAUL, 2020). Além disso, as interfaces de aplicativos que conectam dispositivos IoT (incluindo *middlewares*) são particularmente simplificadas devido à própria estrutura do *hardware* nos quais são baseadas, o que impossibilita a instalação de sistemas mais robustos de segurança tornando esses dispositivos mais susceptíveis a invasões.

4. IoT, datificação e o papel do Estado

O estabelecimento de objetos conectados agindo em larga escala em ambientes físicos e sociais, formando uma intensa rede de coleta de dados ubíqua, significa não apenas um maior aporte de conhecimento e controle sobre o mundo, mas sobretudo, a ampliação do processo de *datificação* da vida através do qual tudo passa a ser monitorado, medido e controlado através do intenso fluxo de diferentes tipos de dados. Se por um lado temos um grande potencial na implantação de sistemas de IoT capazes de gerar avanços significativos na performance de diversas atividades, com horizonte de novos serviços, produtos e produção de conhecimento capaz de prevenir e propor soluções, por outro lado, a proliferação de objetos conectados podem ser tornar parte do cotidiano e ampliar os problemas de segurança e privacidade, criando novas formas de violação e colocando sistemas, bens públicos e vidas em risco.

Neste cenário, o Estado enfrenta grandes desafios regulatórios e de governança devido às características inovadoras inerentes a esse processo de *datificação* gerado pela intensificação dos dispositivos de IoT. Primeiramente, trata-se de um setor expansivo de rápida evolução e transversal. Qualquer regulação ou política pública precisa levar em conta essa velocidade, diversidade e amplitude, que coloca normas em constante tensão para lidar com diferentes contextos de usos. Segundo, essa diversidade setorial tende a gerar uma fragmentação normativa capazes de dificultar o estabelecimento de padrões universais de segurança e privacidade e estabelecer ações unificadas contra problemas de larga escala. Terceiro, a proliferação de dispositivos conectados requer interoperabilidade e isso só pode ser definido a partir de normas comuns, cabendo ao Estado consolidá-las, levando em conta os diferentes interesses dos diferentes *players* nas diversas camadas da cadeia de IoT. Quarto, há uma clara tensão entre violação de direitos e inovação técnica na qual especialistas, organizações civis e ativistas reivindicam legislações mais protetivas contra o poder e a ubiquidade destas estruturas e, do outro lado, setores econômicos reivindicam regulação menos densa sob o argumento de que o excesso de normas pode gerar inibição do potencial inovador do setor. Quinto, as estruturas regulatórias existentes muitas vezes não são adequadas para lidar com os desafios específicos da IoT, como identificadores únicos, redes distribuídas, coleta massiva de dados sem consentimento individualizado. Sexto, para funcionar, IoT pressupõe não apenas microestruturas de sensores mas infraestruturas de transporte (como *backbones, backauls*, 5G, 6G), de tráfego (como Pontos de Troca de Tráfego – TTs) e de armazenamento de dados (como *datacenters*) que tendem a se constituir como um gargalo para muitos países devido à forte dependência tecnológica.

Todos esses desafios requerem amplos esforços em diversas frentes exigindo que o Estado opere diferentes papeis concomitantes: como regulador na definição de regras e padrões deontológicos; como indutor no fomento à criação de infraestruturas e *expertise* técnica; e como protetor de direitos baseado em princípios de interesse público.

Em seu papel de regulador o Estado precisa estabelecer limites e normas de conformidade quanto à segurança que dispositivos de IoT devem sustentar. Neste sentido, o conceito de "privacidade por *design*" é um bom exemplo de como o Estado pode agir introjetando normas de proteção por natureza replicáveis que acompanhe a escala dos sistemas de IoT. Ou seja, uma forma de gerar efeitos transversais para lidar com a ubiquidade dos dispositivos de IoT, garantindo que carreguem mecanismos anti-violação. Uma outra dimensão neste papel é garantir a interoperabilidade entre dispositivos de diferentes fabricantes e garantir que esses padrões sejam abertos e pactuados. Este elemento regulador é essencial pois viabiliza que um ecossistema robusto floresça com diversidade de dispositivos operando de forma intercambiável, evitando oligopólios ou monopólios econômicos, incentivando potenciais inovações técnicas.

Como indutor, o Estado tem como principal papel garantir a existência de uma infraestrutura capaz de suportar e fazer funcionar sistemas de IoT. O volume de dados processados está em expansão com a conexão de mais dispositivos e o surgimento de sistemas de IA. Para suportar tais demandas, é necessário que haja toda uma infraestrutura de base que requer grandes investimentos (VINUEZA-MARTÍNEZ, 2018; FANOU, et al., 2020). Principalmente porque sistemas de IoT funcionam mediante a existência de nuvens de dados. Embora a expressão "nuvem" possa soar abstrata, trata-se de uma metáfora para a conjunção de infraestrutura materiais e lógicas de transporte, armazenamento e processamento de dados de longa distância e curta distância. "As nuvens são cruciais para a IoT porque, entre outras coisas, fornecem um ambiente altamente escalável para armazenamento de dados [...] " (GREENGARD, 2021, p. 74).

Isso também envolve políticas públicas que promovem a integração da IoT em infraestruturas locais como cidades inteligentes e seus equipamentos. Ao mesmo tempo que precisa fomentar infraestruturas, o Estado também precisa olhar para as microestruturas pois nelas estão boa parte dos problemas de segurança que envolvem IoT. O problema da escala aliado à busca por diminuição dos custos desses dispositivos requer que o Estado crie mecanismos para subsidiar e fomentar o de-

senvolvimento de inovações de segurança, capazes de lidar com o problema do custo que isso envolve e ao mesmo tempo solucionar que aumente a segurança da rede.

Por fim, o papel de proteção de direitos requer não apenas um Estado forte mas também um ecossistema de governança ativo e representativo. Neste caminho, ações de regulação tradicional, mesclada com mecanismos de corregulação e principalmente modelos de governança multissetorial (que incorpora institucionalmente diversos segmentos sociais como governo, organizações sociais, empresas, pesquisadores, especialistas etc.) são mecanismos adequados para lidar com as complexidades e os desafios específicos da IoT (Weber, 2013; Jacobs, 2020a. 2020b). Para isso, entes reguladores devem ser estabelecidos com capacidade de *enforcenment* e capacidade técnica para auditar e monitorar as ações destas redes em sua expansão.

Considerações finais

Este artigo discutiu como IoT é hoje um fenômeno com forte viés inovador quanto à ampliação dos processos de *datificação* da vida, criando oportunidades e riscos. Primeiramente, observou-se que sistemas de IoT são redes que constituídas por camadas que envolvem captação, leitura, conexão, transporte, armazenamento e processamento de dados, funcionando através de microestruturas e infraestruturas capazes de potencializar o conhecimento sobre o mundo. Isso permite monitoramento detalhado, operacionalização eficiente e automação de processos, reduzindo erros e aumentando o desempenho de sistemas. A IoT também traz impactos econômicos relevantes ao elevar a produtividade e diminuir custo. Amplia a criação e manutenção de sistemas de Inteligência Artificial (IA) e permite a prevenção e mitigação de crises e emergências coletivas.

Se por um lado, a Internet das Coisas pode significar um salto epistemológico e técnico relevante neste século, também implica em problemas decorrente de suas próprias características disruptivas. Cada ca-

mada pode trazer diferentes tipos de ações maliciosas como (a) ataques de funcionamento; (b) ataques de comunicação; (c) ataques de identificação e (d) ataques de captura. Tais riscos exigem a necessidade de medidas de segurança mais rigorosas pois trata-se de ataques que podem gerar danos em larga escala.

Nesse contexto, o Estado tem desafios complexos para criar normas que acompanhem a velocidade de evolução do setor, evitando a fragmentação normativa e garantindo interoperabilidade. Além disso, é necessário lidar com tensões entre proteção de direitos e inovação, estabelecendo modelos regulatórios multissetoriais capazes de lidar com esta dualidade.

A infraestrutura de suporte à IoT, incluindo sensores, redes e armazenamento de dados, representa outro desafio, especialmente para países com histórico de dependência tecnológica. Como indutor, o Estado deve incentivar e investir em infraestrutura de transporte e armazenamento de dados, tanto no nível local quanto nacional, visando a soberania do interesse público neste campo.

Embora haja em diversos países planos estratégicos e alguma regulação incipiente que versa sobre IoT, ainda não há um marco regulatório sistêmico capaz de lidar com as diversas camadas e dimensões do problema. Para os próximos anos, é preciso compreender que sistemas de IoT significam ampliação do conhecimento sobre o mundo e isso também implica em maior controle e poder. Cabe ao Estado direcionar essas forças inovadoras, fazendo com que o salto epistemológico propiciado por estas novas formas de produção de conhecimento se convertam em benefícios coletivos, ao invés da ampliação da vigilância e concentração de poder típico do processo de plataformização.

Referências

ATTIA, Tarek M. Challenges and Opportunities in the Future Applications of IoT Technology. **2nd Europe – Middle East – North African Regional Conference of the International Telecommunications Society (ITS):** Leveraging Technologies For Growth, Aswan, Egypt, 18th-21st February, 2019, International Telecommunications Society (ITS), Calgary, 2019.

CHIARA, Pier Giorgio. The IoT and the new EU cybersecurity regulatory landscape. **International Review of Law, Computers & Technology**, v. 36, n. 2, p. 118-137, 2022.

DIJCK, José van . 2014. Datafication, dataism and dataveillance: Big Data between scientific paradigm and ideology. **Surveillance & Society** 12 (2), p. 197-208, 2014.

FANOU, R. et al.. Unintended Consequences: Effects of Submarine Cable Deployment on Internet Routing. In: Sperotto, A., Dainotti, A., Stiller, B. (Org.) Passive and Active Measurement. PAM 2020. **Lecture Notes in Computer Science**, vol 12048. Cham: Springer, 2020.

GREENGARD, Samuel**. The Internet of Things**. Revised and updated edition. Cambridge: The MIT Press, 2021.

JACOBS, Naomi et al. Governance and Accountability in Internet of Things (IoT) Networks. In: YATES, Simeon J.; RICE, Ronald E. (Org.). **The Oxford Handbook of Digital Technology and Society**. Oxford: Oxford University Press, 2020b.

JACOBS, Naomi et al. Who trusts in the smart city? Transparency, governance, and the Internet of Things. **Data & Policy**, v. 2, 2020a.

KARLOV, Dmitriy et al. The implementation of the IoT concept in the post-industrial economy. **Revista Espacios**, v. 40, n. 38, p. 1-11, 2019.

KHAN, Minhaj Ahmad; SALAH, Khaled. IoT security: Review, blockchain solutions, and open challenges. **Future Generation Computer Systems**, v. 78, p. 964-979, 2018.

KOPETZ, Herman ; STEINER, Wilfried., W. Internet of Things. In: KOPETZ, H. ; STEINER, W. **Real-Time Systems. Springer**, Cham, 2022, p. 325-340.

LEENES, Ronald et al (Org.). **Data protection and privacy**: the internet of bodies. Portland: Hart Publishing, 2018.

MAGRANI, Eduardo. **A internet das coisas**. Rio de Janeiro: FGV Editora, 2018.

MISHRA, Saumya; PAUL, Aditi. A critical analysis of attack detection schemes in IoT and open challenges. In: IEEE **International Conference on Computing, Power and Communication Technologies (GUCON),** Greater Noida, India. Anais, 2020.

NICOLESCU, R. et al. Mapping the Values of IoT. J**ournal of Information Technology**, 33 (4), 345-360, 2018.

SHACKELFORD, Scott J. **The internet of things:** what everyone needs to know. Nova York: Oxford University Press, 2020.

SILVA, Sivaldo Pereira da; BIONDI, Antonio (Org.). **Caminhos para a universalização da internet banda larga:** experiências internacionais e desafios brasileiros. 1. ed. São Paulo: Intervozes, 2012.

TANCZER, L. M. et al. The United Kingdom's Emerging Internet of Things (IoT) Policy Landscape. In R. Ellis & V.Mohan (Org.). **Rewired:** Cybersecurity Governance. Hoboken: Wiley, 2019.

TZAFESTAS, Spyros G. Ethics and law in the Internet of Things world. **Smart Cities**, v. 1, p. 98-120, 2018.

VINUEZA-MARTÍNEZ, Jorge et al. A study of the Internet and connectivity in South American countries to 2017: An analytical perspective. **Revista Espacios**, v. 39, n. 16, p. 6, 2018.

VOULGARIDIS, Konstantinos et al. IoT and digital circular economy: Principles, applications, and challenges, **Computer Networks**, 219, 2022.

WEBER, Rolf H. Internet of things – Governance quo vadis? **Computer Law & Security Review,** v. 29, n. 4, p. 341-347, 2013.

YOO, C. S. . The Emerging Internet of Things: Opportunities and Challenges for Privacy and Security. In **Governing Cyberspace during a Crisis in Trust**: An essay series on the economic potential – and vulnerability – of transformative technologies and cyber security. Centre for International Governance Innovation, p. 41–44, 2019.

Sivaldo Pereira da Silva · Professor da Faculdade de Comunicação (FAC) e do Programa de Pós-Graduação em Comunicação da Universidade de Brasília (UnB). PhD em Comunicação e Cultura Contemporâneas pela Universidade Federal da Bahia (UFBa), com estágio doutoral na University of Washington (EUA). Possui pós-doutorado no Centro de Estudos Avançados em Democracia Digital e Governo Eletrônico (CEA-DD), UFBa. Foi pesquisador visitante no Instituto de Pesquisa Econômica Aplicada (IPEA); consultor da UNESCO e professor visitante na Technische Universität Dortmund (Alemanha). É fundador e coordenador do grupo de pesquisa Centro de Estudos em Comunicação, Tecnologia e Política (CTPol) e pesquisador do Instituto Nacional de Ciência e Tecnologia em Democracia Digital (INCT-DD).

Vivian Peron · Doutora em Relações Internacionais pela Universidade de Brasília (UnB), com estágio doutoral no Massachusetts Institute of Technology (MIT), nos EUA. Mestrado em Comunicação Social pela Universidade Federal de Minas Gerais (UFMG). Tem pós-doutorado em Relações Internacionais pela Universidade de Brasília (UnB) e pós-Doutorado em Sociologia pela Universidade Federal de São Paulo (Unifesp). Foi pesquisadora no IPEA , consultora da UNESCO e professora no Departamento de Ciência Política e Relações Internacionais do Centro Universitário do Distrito Federal (UDF). Atualmente é coordenadora de Articulação Federativa do Laboratório de Cultura Digital (LabCD), projeto em parceria do Ministério da Cultura (MinC) e Universidade Federal do Paraná (UFPR), onde desenvolve pesquisa de pós-doutorado sobre estratégicas de comunicação e cultura digitais na implementação de políticas públicas governamentais.

A Fundação Konrad Adenauer é uma fundação política da República Federal da Alemanha que, naquele país e no plano internacional, vem trabalhando em prol dos direitos humanos, da democracia representativa, do Estado de Direito, da economia social de mercado, da justiça social e do desenvolvimento sustentável.

Os principais campos de atuação da Fundação Konrad Adenauer são a formação política, o desenvolvimento de pesquisas aplicadas, o incentivo à participação política e social e a colaboração com as organizações civis e os meios de comunicação.

A Fundação Konrad Adenauer está no Brasil desde 1969 e atualmente realiza seu programa de cooperação internacional por meio da Representação no Brasil, no Rio de Janeiro, trabalhando em iniciativas próprias e em cooperação com parceiros locais. Com suas publicações, a Fundação Konrad Adenauer pretende contribuir para a ampliação do debate público sobre temas de importância nacional e internacional.

Os *Cadernos Adenauer* versam sobre temas de interesse público, relacionados ao desenvolvimento de uma sociedade democrática.

Privilegiam-se artigos que abarcam temas variados nos campos da política, da situação social, da economia, das relações internacionais e do direito.

As opiniões externadas nas contribuições desta série são de exclusiva responsabilidade de seus autores.

KONRAD ADENAUER STIFTUNG

adenauer-brasil@kas.de
www.kas.de/brasil