

Desdemocratização algorítmica: a erosão da democracia como resultado da plataformização política

Wagner Silveira Rezende ¹

Jessicka Oliveira de Assis ²

Akleis Müller Ferreira Júnior ³

RESUMO

Este estudo analisa as interseções entre a cultura algorítmica, os sistemas de inteligência artificial e a plataformização da atividade parlamentar, destacando suas implicações para a construção dos processos eleitorais enquanto pilares fundamentais da democracia. O problema central da pesquisa consiste em compreender, através de uma revisão bibliográfica, os riscos que a datificação impõe às liberdades individuais, especialmente no que se refere à autodeterminação informativa e aos seus impactos nas dinâmicas sociais contemporâneas. O objetivo da pesquisa é analisar os impactos da plataformização da política sobre a integridade dos processos eleitorais, examinando os riscos da datificação para as liberdades individuais, a reprodução de desigualdades e vieses pelos algoritmos e as estratégias de engajamento político baseadas em campanhas permanentes. O trabalho evidencia o potencial destrutivo dos algoritmos, particularmente na medida em que comprometem os princípios de objetividade, neutralidade e imparcialidade. Ao operarem de maneira opaca, essas tecnologias tendem a reforçar desigualdades estruturais, amplificar vieses, enfraquecer a transparência, e, por conseguinte, impulsionar o surgimento de bolhas informacionais. Nesse contexto, propõe-se uma reflexão sobre como a digitalização dos espaços eleitorais e a lógica das “campanhas permanentes” adotam estratégias comerciais de engajamento, convertendo a comunicação política em uma plataforma voltada à mobilização de

¹ Mestrado (2010) em Ciências Sociais pela UFJF. Doutor em Ciências Sociais (2014) e em Educação (2020) pela UFJF, tem experiência na área de Teoria Social, Sociologia e Antropologia do Direito, Sociologia e Educação, Avaliação Educacional, Retórica e Argumentação. Atualmente, é Professor Adjunto da Faculdade de Direito da UFJF, responsável pela disciplina Sociologia do Direito, membro do corpo docente permanente do Programa de Pós-Graduação em Direito da UFJF e membro do corpo docente permanente do Programa de Pós-Graduação Profissional em Gestão e Avaliação da Educação Pública da UFJF. Diretor do CEAD/UFJF. Fundador, em parceria com o professor Raul Francisco Magalhães, do grupo de pesquisa Polis – Estudos Clássicos. Membro do grupo de pesquisas Direito, Argumentação e Inovação, da Faculdade de Direito da UFJF. Membro da Rede de Estudos sobre Implementação de Políticas Públicas Educacionais – Reippe. Pesquisador associado ao Centro de Políticas Públicas e Avaliação da Educação – CAEd/UFJF, com as linhas Direito e Educação e Avaliação Educacional. <http://lattes.cnpq.br/5372700780542200>

² Mestre em Direito (UFJF/MG). E-mail: jessickaoliveira1996@gmail.com

³ Mestre em Direito (UFJF/MG). E-mail: jessickaoliveira1996@gmail.com.

bases eleitorais nem sempre comprometidas com os valores democráticos.

Palavras-chave: cultura algorítmica; inteligência artificial; plataformação; democracia digital; comunicação política; bolhas informacionais; processos eleitorais

ABSTRACT

This study analyzes the intersections between algorithmic culture, artificial intelligence systems, and the platformization of parliamentary activity, highlighting their implications for the construction of electoral processes as fundamental pillars of democracy. The central problem of the research is to understand, through a bibliographic review, the risks that datafication poses to individual freedoms, especially regarding informational self-determination and its impacts on contemporary social dynamics. The aim of the research is to examine the impacts of the platformization of politics on the integrity of electoral processes, addressing the risks of datafication for individual freedoms, the reproduction of inequalities and biases by algorithms, and the strategies of political engagement based on permanent campaigns. The study reveals the destructive potential of algorithms, particularly as they compromise the principles of objectivity, neutrality, and impartiality. By operating in an opaque manner, these technologies tend to reinforce structural inequalities, amplify biases, weaken transparency, and consequently foster the emergence of informational bubbles. In this context, the work proposes a reflection on how the digitalization of electoral spaces and the logic of “permanent campaigns” adopt commercial engagement strategies, transforming political communication into a platform aimed at mobilizing electoral bases not always committed to democratic values.

Keywords: algorithmic culture; artificial intelligence; platformization; digital democracy; political communication; informational bubbles; electoral processes.

Introdução

Os novos contornos sociais da sociedade em rede transcendem a mera comunicação operacional e se desdobram em relações sociais mediadas por uma economia informacional e global (Castells, 2016). Essa hiperconexão é caracterizada, por um lado, pela abundância de bens, e, por outro, pelo fetichismo da mercadoria (Debord, 1997), fruto da influência recíproca entre indivíduos (Kleinberg; Easley, 2010).

Dessa forma, a publicização do indivíduo por meio de seus dados torna-se, ao mesmo tempo, meio e mensagem da inserção

social (Maffesoli, 2014) e da memória coletiva (Nora, 1987), indexada através da aglomeração de informações sobre comportamentos individuais (Kleinberg; Easley 2010).

O poder preditivo político, social e mercadológico, viabilizado e extraído pela identificação de perfis de consumo, estilos de vida e preferências políticas (Barros, 2021), vem sendo criticado por autores da literatura específica, como Frazão (2019), Lira (2014) e Vieira (2007), por representar um risco às liberdades individuais e à própria democracia.

Compreendendo que os algoritmos são a unidade básica de computação para o tratamento dos dados (Qin; Zeng, 2020) e, a partir de uma metodologia qualitativa de estudo bibliográfico e documental, este estudo pretende relacionar a cultura algorítmica e a nova forma de dominação social da era contemporânea - o poder sobre dados - às recentes manipulações eleitorais engendradas pela reconfiguração política das campanhas partidárias.

Colonialidade digital e cultura algorítmica

É inegável que a contribuição das Tecnologias da Informação e Comunicação (TICs) transformou os contornos sociais da sociedade moderna. No entanto, a gleba social contemporânea não está apenas “em rede”, como definiria Castells (2016). Não se trata apenas da comunicação operacionalizada num novo formato de nós interconectados, mas, mais do que isso, de um novo desdobramento da sociedade do espetáculo de Debord (1997).

Para Debord (1997), o espetáculo seria não apenas um conjunto de imagens, mas uma relação social entre as pessoas, mediatizada por imagens - uma representação divisora de classes, como também defenderia Bourdieu (1979), em “A Distinção: crítica social do julgamento”. Tal representação teria sido engendrada pelo fetichismo da mercadoria e seria caracterizada, como forma-mercadoria, pelo quantitativo.

Dessa forma, tem-se uma sociedade do consumo marcada, de uma lado, pela economia informacional, global e em rede (Castells, 2016), organizada em conexões globais e estruturada a partir de sua capacidade de gerar, processar e aplicar a informação de maneira eficiente; e, de outro, pela cultura de um espetáculo caracterizado pelo fetichismo da abundância da mercadoria.

Ocorre que, quando os indivíduos estão conectados por uma rede, é possível — e muito provável — que passem a influenciar o comportamento e as decisões uns dos outros. Isso ocorre por conta tendência humana ao pertencimento tribal (Maffesoli, 2004) e de forma quase involuntária, por um efeito epistêmico: porque somos mais pensados do que pensamos e porque somos mais agidos do que agimos (Foucault, 2002).

É assim que as denominadas “cascatas de informações” da era informatizada dão origem a uma série de processos sociais nos quais as redes agregam comportamentos individuais, produzindo resultados coletivos (Kleinberg; Easley, 2010, p. 483). Um desses processos — talvez o mais importante e debatido — é o da superexposição.

A tecnologia pós-moderna e suas mídias sociais, abarcadas por um relacionismo galopante, funcionam principalmente a partir da publicização do indivíduo como forma de inserção social (Amaral, 2016). Para Maffesoli (*apud* Sayuri, 2014), isso acontece porque, nesse novo tipo de sociedade do espetáculo, as mídias sociais são o meio e a mensagem da representação a que se referia Debord (1997).

Neste cenário, de uma sociedade inteira em rede e se superexpondo, surge o denominado superinformacionismo, ou seja, a grande “massa de informações sobre tudo e sobre todos, queiram ou não estar naqueles conjuntos de dados ou informações” (Rulli Junior; Rulli Neto, 2013). Esse fenômeno concretiza a previsão de Lévy (1999) de que a digitalização geral das informações tornaria o ciberespaço o principal canal de comunicação e suporte de memória da humanidade a partir do início do século seguinte.

Esse sistema se retroalimenta, já que, à medida que desaparece a memória tradicional, “nós nos sentimos obrigados a acumular religiosamente vestígios, testemunhos, documentos, imagens, discursos, sinais visíveis do que foi, como se esse dossiê cada vez mais prolífero devesse se tornar prova em não se sabe que tribunal da história” (Nora, 1987, p. 15). O resultado não poderia ser diferente:

Nenhuma época foi tão voluntariamente produtora de arquivos como a nossa, não somente pelo volume que a sociedade moderna espontaneamente produz, não somente pelos meios técnicos de reprodução e de conservação de que dispõe, mas pela superstição e pelo respeito ao vestígio (Nora, 1987, p. 15).

No entanto, para além de tornar o ciberespaço o principal canal de comunicação da era, outro fenômeno é engendrado pelo superinformacionismo: o capitalismo de vigilância (*surveillance capitalism*). Como afirma Dal Bello (2011), “a exposição generalizada da intimidade dá margem a novos modelos de exploração das informações pessoais ali depositadas (à revelia de autorização prévia)”, tornando visibilidade, vigilância, identidade e indexação completamente indiscerníveis.

A extração de capital a partir da gestão de dados — muitas vezes fornecidos gratuitamente por usuários a empresas de tecnologia — é o que define o chamado capitalismo de vigilância (Zuboff, 2021).

Essa extração de valor parte, muitas vezes, de uma operação denominada *data mining*. A mineração de dados, em tradução livre para o português, consiste na descoberta de padrões de relacionamentos significativos entre informações a partir da aplicação de técnicas de análise de dados, como classificação, agrupamento, regressão, análise de associação e mineração de sequências (Han; Pei; Tong, 2022).

Tais informações podem não aparentar utilidade *prima facie*; no entanto, quando retiradas de uma perspectiva unitária — principalmente se pertencentes a uma grande base de dados - as denominadas *Big Datas* —, oferecem potencial preditivo e perfilizador: O agrupamento dos dados pessoais dos usuários com o objetivo de extrair informações detalhadas sobre seus titulares, por exemplo, por exemplo, é uma prática comum no mundo do *Business Analytics*, por ser uma técnica de identificação de padrões de consumo (Bioni, 2019).

As *big techs*, consideradas grandes empresas de tecnologias que, em regime de monopólio, coletam e tratam os dados dos usuários, são conhecidas pela utilização da análise de negócios, já que essa coleta seria capaz, em última instância, de traçar perfis de consumo, estilos de vida, além de preferências pessoais e políticas, influenciando um grande mercado digital (Barros, 2021).

Esse agrupamento de informações é conhecido pela sigla PII (*personally identifiable information*), que significa, em português, informações pessoais identificáveis, ou seja, que podem ser usadas para descobrir a identidade de um indivíduo¹. Na Ciência de

¹ Disponível em: [https://www.ibm.com/br-pt/topics/pii#:~:text=As%20informa%C3%A7%C3%B5es%20pessoalmente%20identific%C3%A1veis%20\(PII,ou%20endere%C3%A7o%20de%20e%20Dmail](https://www.ibm.com/br-pt/topics/pii#:~:text=As%20informa%C3%A7%C3%B5es%20pessoalmente%20identific%C3%A1veis%20(PII,ou%20endere%C3%A7o%20de%20e%20Dmail). Acesso em 10 de dez. de 2023.

Dados, é o metadado que permite tal identificação - vocábulo que significa, por definição própria, um dado que fornece informações sobre outros dados. Apesar de não existir um conceito único que os defina, podem ser compreendidos, segundo a literatura específica majoritária, como “dados sobre dados” (Ventura; De Albuquerque Siebra; Lima, 2013).

Existem diferentes tipos de metadados: os descritivos, que descrevem o conteúdo e contexto dos dados; os estruturais, que descrevem a estrutura ou o relacionamento entre os dados, ou seja, a hierarquia ou organização entre os elementos; os administrativos, que reúnem informações relacionadas à gestão dos dados, como direitos autorais, controle de acesso e política de preservação; e os de preservação, que descrevem informações como o formato de arquivo e estratégias de backup.

Dessa forma, é possível argumentar que os metadados exercem uma função essencial para o gerenciamento e para a eficiência e efetividade na utilização dos dados (Qin; Zeng, 2020).

Essa função, no entanto, somente pode ser operacionalizada a partir da descrição de características essenciais das informações, como formato, conteúdo, estrutura, proveniência e contexto — elementos que também podem ser utilizados para identificar tais dados² (Qin; Zeng 2020, p. 2, tradução da autora).

Não por acaso, autores como Frazão (2019), Lira (2014) e Vieira (2007) alertam para o fato de que esses mecanismos de agrupamento podem representar um risco às liberdades individuais e à própria democracia, já que transformam a conduta num modelo lucrativo de negócio. A possibilidade do cruzamento de dados pessoais, muitas vezes oferecidos pelos próprios usuários, pode, dessa forma, se agigantar como uma ameaça ao direito à privacidade.

É o caso do emblemático episódio ocorrido com a Target, em meados de 2012. A empresa mantinha uma base de dados com padrões de consumo que eram capazes de traçar modelos preditivos. Um exemplo era o evento de uma gravidez, estatisticamente associado à compra de loções sem essência e de suplementos alimentares. A empresa criou uma lista com 25 produtos que uma mulher grávida costuma adquirir e, com base nessas informações,

² “Metadata is data that provide information about other data. It describes essential characteristics of data such as format, content, structure, provenance, and context. Metadata can be used to identify, locate, manage, and preserve data as well as to enhance the access, usability, and interoperability of data”.

era possível estimar uma probabilidade de 0 a 100% — e o estágio da gravidez (em semanas). Essa prática servia para que a loja enviasse cupons de descontos e ofertas personalizadas para as potenciais mães. No entanto, em uma das redes varejistas da marca, em Minneapolis, uma adolescente recebeu um cupom de desconto relacionado à gravidez antes mesmo de saber que estava grávida, o que lhe gerou sérios desconfortos familiares (O guia financeiro, 2019).

Casos como esses, em que cadastros e inscrições “gratuitas” dão acesso a determinados benefícios — como é o caso de informar algum dado pessoal para obter descontos em farmácias ou acesso ao Wi-Fi de lugares públicos - deram ensejo à criação da expressão “Se você não está pagando pelo produto, você é o produto” (O Dilema das Redes, recurso online), disseminando o entendimento de que o próprio dado constitui o valor do bem.

O grande imbróglio existente nessa seara é que raramente o consumidor é informado sobre a utilização ou a forma de tratamento que será dada àquela informação, motivo pelo qual a faculdade de o sujeito construir sua própria esfera particular, exercendo o controle sobre suas próprias informações, torna-se objeto sujeito à tutela do direito contemporâneo à privacidade (Rodotà, 2018).

Para além do problema da falta de autodeterminação informativa, os titulares do que se tornaram os ativos mais valiosos do mundo - os dados - passaram a ser bombardeados por infinitivos tipos de ataques arquitetados para roubar a mercadoria mais preciosa do novo modelo econômico. As consequências são catastróficas: *ransomware*, *phishing*, *backdoor*, *cryptojacking*, *spoofing*, *man-in-the-middle* (MitM), *denial of service* (DoS), *direct memory access* (DMA), *decoy*, *zero-day*³ e tantas outras técnicas de cibercrime trouxeram consigo as maiores polêmicas de vazamento e roubo de dados para a construção de perfis psicográficos, além de

³ O *ransomware* é um tipo de prática que se utiliza de um *malware* - um software malicioso - para manter dados reféns até que seu titular concorde em pagar um resgate ao invasor; é também conhecido como sequestro de dados. O *phishing* é um tipo de estelionato: o criminoso dá golpes, através de engenharia social, para obter dados do titular. *Backdoor* significa, em tradução livre, “porta dos fundos” e é uma forma de contornar a segurança do sistema para ter acesso ao controle geral de dados e informações. O *cryptojacking* é um ataque a dispositivos com o fim de fazer mineração de criptomoedas. O *spoofing* é um ataque cibernético que consiste na falsificação de endereços para que o invasor possa se passar pelo usuário e ter acesso às suas informações. O *Man-in-the-middle* (em tradução livre, “homem no meio”) ocorre quando um hacker - ou invasor - se insere entre os meios de comunicação de um usuário para interceptar seus dados. O *DoS* é um ataque que faz com que determinado sistema fique indisponível enquanto os invasores têm acesso aos dados daquele diretório. O *DMA* é um ataque de acesso direto à memória do sistema. O *decoy* é o ataque realizado através de um programa legítimo hackeado, fazendo com que o usuário entre no “programa espelho” com seus dados reais. O *zero-day* (em tradução livre, “dia zero”) é um ataque a partir das falhas de seguranças (ou *bugs*) de aplicações recém-lançadas (Fortinet, 2022).

diversos escândalos envolvendo a disseminação de *fake news* e a falta de transparência e *accountability* no que se refere ao tratamento de dados e metadados.

Levantamentos de empresas que se dedicam ao estudo da cibercultura e do gênero criminal inerente a essa seara — o cibercrime — apontam para um aumento drástico dessa modalidade criminal no cenário nacional nos últimos anos (G1, 2021). A Central Nacional de Denúncias de Crimes Cibernéticos, uma parceria da ONG “Safernet” Brasil com o Ministério Público Federal (MPF), divulgou dados que demonstram que o total de cibercrimes cometidos no ano de 2020 (156.692) foi o maior da série histórica desde o início do levantamento, em 2014, sendo, ainda, o dobro do total do ano de 2019.

Em 2021, os números não foram mais animadores: nos primeiros oito meses do ano, o Brasil registrou um aumento de 23% nos casos de cibercrimes em comparação ao mesmo período do ano anterior (Fórum Konferencia @Casa Kaspersky, 2021). Além de liderar os rankings de *ransomware* e *phishing*, o país registrou, nesse período, 481 milhões de tentativas de infecção — o equivalente a 1.395 tentativas por minuto (Olhar digital, 2021). Órgãos públicos e cidadãos mostraram-se igualmente frágeis à crescente tendência dos ataques.

Na esteira do aumento exponencial de cibercrimes, estão os vazamentos de dados pessoais sensíveis, aliados ou não à disseminação de notícias falsas (*fakes news*). Em 2013, ocorreu o vazamento de dados — inclusive bancários — de mais de 152 milhões de nomes e senhas, além de 2,8 milhões de números de cartões de crédito de usuários da empresa Adobe, bem como o vazamento de pelo menos 40 milhões de dados de cartões e 70 milhões de outros dados de clientes da franquia Target. Em 2014, a Home Depot teve cerca de 56 milhões de números de cartões de créditos roubados. Em 2016, a Uber registrou o vazamento dos dados de mais de 57 milhões de usuários — dentre eles, 196 mil brasileiros.

No ano seguinte, 2017, o vazamento de mais de 1,4 bilhão de nomes de usuários e senhas de sites como Netflix, LinkedIn, MySpace, Last.Fm e YouPorn foram expostos, além da disseminação do *ransomware* WannaCry, que infectou mais de 230 mil sistemas. Em 2021, ocorreu o vazamento de 8.4 bilhões de senhas de usuários da rede social RockYou (Araújo, 2020; Rodrigues, 2021).

Um dos vazamentos de dados pessoais que ganhou mais repercussão foi o do Facebook, em 2019, no qual mais de 87 milhões de usuários — dentre eles, mais de 443 mil brasileiros — tiveram seus dados pessoais publicados gratuitamente em fóruns hackers. Informações incluindo nome, endereço, número de telefone, data de nascimento e e-mail foram obtidas a partir de uma ferramenta então existente, à época, na rede social, que permitia importar os dados dos usuários e associá-los, criando metadados.

O caso do vazamento dessa plataforma é considerado como um dos mais chocantes também pela acusação de conexão do Facebook com a eleição de Donald Trump, em 2016, quando a empresa Cambridge Analytica coletou e tratou dados da rede social com o objetivo de manipular eleitores e influenciar os resultados eleitorais norte-americanos (Senha Segura, 2021).

Não por acaso, diante de tantas controvérsias, a literatura especializada passou a utilizar os termos colonialismo digital e ditadura de dados para se referir à nova forma de dominação na era da tecnologia: o poder sobre os dados (Siqueira, 2019).

Essa nova forma de imperialismo está intrinsecamente relacionada ao poder de dominação advindo da falta de autodeterminação informativa no âmbito do maior valor econômico da contemporaneidade: os dados. O conceito de financeirização-dataficação algorítmica (Dardot; Laval, 2016) parte do entendimento de que o extrativismo de dados pessoais na era moderna não configura mera coleta de informações, mas sim extração de recursos (Srnicsek, 2016), já que o processo de documentação, filtragem, extração e acúmulo dos dados caracteriza o novo padrão sistêmico de geração de riqueza e, conseqüentemente, da modernização do capital (Murdock, 2018).

Todo esse processamento somente é possível a partir da unidade básica da computação: o algoritmo (Van Dijck; Poell; De Wall, 2018).

Algoritmos de destruição em massa: Uma ameaça à democracia

Alguns autores, diante dessa nova era tecnológica, passaram a cunhar o termo “Quarta Revolução Industrial” ou “Revolução 4.0”. O termo se refere, segundo Klaus Schwab (2019), à “combinação

de fatores estruturais (excesso de endividamento e envelhecimento das sociedades) e sistêmicos (a introdução da plataforma e das economias sob demanda, a crescente relevância da diminuição dos custos marginais etc.)” que reescreveu os livros de economia.

Essa revolução industrial, como todas as anteriores, deveria apontar para uma melhoria na eficiência e na produtividade dos processos. No entanto, sua principal característica é demarcada pela presença de conceitos tecnológicos que têm potencial para um crescimento econômico sem precedentes (Schwab, 2019). No entanto, como apresentado, esse não é o único potencial da alteração produzida pela Quarta Revolução.

Dentre as novas definições do ciberambiente — ou ciberespaço —, entendido como o “novo espaço de comunicação proporcionado pela interconexão mundial de computadores e das memórias dos computadores” (Lévy, 2010), a matemática, cientista de dados e escritora Cathy O’Neil, chama atenção, em seu livro *Algoritmos de Destruição em Massa* (2021), para o potencial destrutivo desse novo paradigma.

A autora afirma, em sua obra, com base também em sua experiência profissional e pessoal, que o processamento contínuo de dados obtidos de redes sociais e sites de e-commerce vem enfocando cada vez mais os seres humanos:

Matemáticos e estatísticos estavam estudando os nossos desejos, movimentações e poder de compra. Eles previam nossa credibilidade e calculavam nosso potencial enquanto estudantes, trabalhadores, amantes e criminosos. Esta era a economia do Big Data, os imensos volumes de dados, e ela prometia ganhos espetaculares. Um programa de computador poderia vasculhar milhares de currículos ou pedidos de empréstimo em um segundo ou dois e ordená-los em listas impecáveis, com os candidatos mais promissores no topo. Isso não apenas economizava tempo, mas também era vendido como algo imparcial e objetivo. Afinal, não envolvia humanos preconceituosos cavoucando resmas de papel, apenas máquinas processando números frios. Por volta de 2010, a matemática impunha-se como nunca nas questões humanas, e o público, amplamente, a saudava (O’Neil, 2021, p. 6).

A alcunha “algoritmos de destruição em massa” ou “armas de destruição matemática” (ADM) foi criada pela autora para caracterizar situações em que, sob o manto da imparcialidade, objetividade

e neutralidade matemática, algoritmos de policiamento preditivo acentuam desigualdades e injustiças.

Os algoritmos podem ser compreendidos, dentro da lógica computacional, como conjuntos de passos finitos e organizados que, quando executados, resolvem um determinado problema (Manzano, 2000). Para resolver determinado problema, é comum que a ciência de dados utilize uma representação abstrata de um sistema real ou conceitual, a fim de compreender seu comportamento e prever seu desempenho (O'Neil, 2021). Essa representação abstrata, normalmente pautada em dados de um histórico, é denominada modelo.

A aprendizagem de máquina, ou *machine learning*, constitui o subcampo da inteligência artificial que se concentra em desenvolver algoritmos e modelos capazes de aprender a partir de dados, ou seja,

O *machine learning* envolve o uso de algoritmos que permitem que um sistema faça previsões ou decisões com base em dados, sem essas previsões ou decisões que precisam ser explicitamente programadas. Em vez disso, os algoritmos são projetados para encontrar padrões nos dados e ajustar seus parâmetros para melhorar sua capacidade de fazer previsões ou decisões (Géron, 2022).

Os algoritmos, portanto, treinam um modelo de aprendizagem de máquina com base em um conjunto de dados, para que esse modelo possa ser usado para fazer previsões ou tomar decisões sobre novos dados. Estes são modelos preditivos porque analisam dados de um histórico e calculam o posicionamento com maior probabilidade de sucesso (O'Neil, 2021)

Os algoritmos mais comuns para o treinamento da aprendizagem de máquina são o aprendizado por reforço, o não supervisionado, o semi-supervisionado e o supervisionado (Brazdil; Gama, 2010).

No algoritmo de aprendizado por reforço, o objetivo é maximizar as recompensas totais ao longo do tempo, e o modelo é treinado para tomar ações a partir de um feedback em tempo real de recompensa ou penalidade. A aprendizagem por reforço tem aplicações em jogos de computador, como é o caso da IA *AlphaGo*,

desenvolvida pela *Google DeepMind*, que usa esse modelo de aprendizagem para jogar o jogo de tabuleiro *Go* (Brazdil; Gama, 2010).

Já no algoritmo de aprendizagem não supervisionado, não há dados rotulados e o modelo é treinado a partir do agrupamento dos dados em *clusters*, identificando relações entre estes. A aprendizagem não supervisionada possui aplicações em reconhecimento de imagens, classificação de documentos e recomendação de conteúdo em redes sociais (Brazdil; Gama, 2010).

Por fim, no algoritmo de aprendizagem supervisionada, os dados de entrada são rotulados com uma resposta correta, e o modelo é treinado a partir de um conjunto de dados de treinamento rotulados para prever a resposta para novos dados de entrada ainda não rotulados. Apesar de poder ser utilizado em outras categorias de aprendizagem de máquina, uma das técnicas mais conhecidas do aprendizado supervisionado é o *deep learning*, um “conjunto de técnicas de aprendizado de máquina baseadas em redes neurais profundas, que são capazes de aprender representações complexas dos dados de entrada”. Essas técnicas se diferenciam das redes neurais tradicionais por apresentarem arquiteturas mais profundas e com camadas especializadas na extração de características relevantes dos dados; normalmente, são utilizadas para tarefas como reconhecimento de voz, visão computacional, processamento de linguagem natural, entre outras (Silva; Spatti, 2017).

Existe, ainda, um modelo híbrido e mais moderno de aprendizagem semi-supervisionada, que trabalha com poucos exemplos rotulados na entrada e que não será examinado profundamente neste trabalho, por conta do recorte do estudo (Matsubara, 2004).

Na atualidade, esses modelos parecem ser os que mais se aproximam do conceito de inteligência artificial, considerada a expressão mais avançada e tecnológica da unidade básica de computação na modernidade.

Uma das referências mais prestigiadas na ciência de dados acerca do conceito de inteligência artificial, o livro *Artificial Intelligence: A Modern Approach*, de Stuart Russell e Peter Norvig, publicado em 1995 e atualizado em 2021, descreve a IA como “o ramo da ciência da computação que se preocupa com a criação de máquinas que podem executar tarefas que exigem inteligência humana” (Russell,

2021), como o reconhecimento de fala, a compreensão da linguagem natural, o aprendizado e a tomada de decisão.

Mais recentemente, surgiu um sub ramo da IA denominado Inteligência Computacional, cujo objeto são os mecanismos adaptativos que permitem um comportamento inteligente da máquina em ambientes complexos. Tais mecanismos são pautados em paradigmas da capacidade humana, como o de aprender, generalizar, abstrair, descobrir e associar (Salomão, 2021).

Não por acaso, o teste de Turing, concebido por Alan Turing em 1950, avaliava que uma máquina poderia ser considerada inteligente se pudesse fingir ser humana com sucesso para um observador experiente. O teste funcionava através de um teletipo (para evitar exigir que a máquina imitasse a aparência ou a voz do humano envolvido) e o observador deveria interagir com a máquina e com o humano, a fim de distingui-los (Turing, 2009).

O *deep learning* é concebido a partir de unidades básicas de processamento capazes de imitar o comportamento do cérebro humano, como o são os neurônios artificiais - capazes de receber informações de outras unidades, processá-las e transmitir um resultado para outras unidades — e as redes neurais artificiais, sistemas de unidades interconectadas capazes de aprender e se adaptar a partir de determinado *input* (dados de entrada) para reconhecer padrões ou resolver problemas de classificação (Mcculloch; Pitts, 1943). Por isso, podem ser considerados os modelos que, na contemporaneidade, melhor representam a máquina inteligente de Turing.

No mundo moderno, o que era entendido como um agente inteligente analítico vem se tornando, cada vez mais, um agente inteligente generativo. Ou seja, se antes a IA era utilizada para tarefas de análise preditiva e reconhecimento de imagem e fala, hoje é aplicada à criação de novos elementos. Num momento anterior, a humanidade conheceu a utilização da IA para tarefas específicas, como o processamento de linguagem natural (PLN), ação voltada para a compreensão, interpretação e manipulação da linguagem humana, ou para a mineração de textos, ação voltada para a busca de termos relevantes ou de padrões em grandes volumes de dados. Na contemporaneidade, a IA é capaz de criar vídeos, áudios, imagens e quaisquer outras mídias digitais (Guidi; Timpone, 2023).

Esses avanços tecnológicos permitiram a criação, pelas IAs, de conteúdos hiper-realistas e que deixam poucos ou quase nenhum vestígio de manipulação (Chawla, 2019): são os denominados *deep-fakes*, mídias que, ao mesclar, combinar, substituir e sobrepor outras mídias, criam conteúdos que parecem autênticos (Alexandrou; Mara, 2018). E, apesar de espalhar esse tipo de mídia falsa (criando as *fake news*) seja fácil, corrigir esse registro é extremamente difícil (De Keersmaecker; Roets, 2017).

Assim, quando a mimetização da atividade nervosa, não mais como um processo metabólico, mas como um circuito de neurônios interagindo como uma rede lógica de interruptores, passa a ser tratada pelos métodos da lógica simbólica, e a atividade nervosa envolvida nos processos de percepção, memória e raciocínio passa a ser descrita por um cálculo algébrico⁴, surge, para além de um questionamento filosófico acerca da natureza da consciência e da distinção entre mente e cérebro, uma preocupação com o futuro da humanidade.

Isso porque, diante da escalada dos modelos de aprendizagem de máquina, não basta a aplicação de um teste unilateral para a aferição de inteligência. Ou seja, um teste como o de Turing deve ser considerado também parcial: uma máquina que passa no teste deve ser considerada inteligente, mas uma máquina ainda poderia ser considerada inteligente sem saber o suficiente sobre humanos para imitá-los. Há que se considerar um debate acerca das restrições do conhecimento do observador sobre a IA, porque “algumas pessoas são facilmente conduzidas a acreditar que um programa bastante estúpido é inteligente” (McCarthy, 2007, tradução da autora).

Warren McCulloch e Walter Pitts, ainda em 1943, já previam o nascimento desse e de outros possíveis embates envolvendo a criação de um modelo de inteligência capaz de imitar o comportamento da inteligência humana. A despeito das posteriores sucessivas criações cinematográficas distópicas envolvendo a IA, tais questionamentos seguem orbitando a temática sem um consenso definitivo no mundo contemporâneo.

Uma das principais preocupações com o rápido desenvolvimento dos modelos inteligentes diz respeito aos riscos existenciais da IA

⁴ “We shall show that all nervous activity, when it is not mere metabolism, is resolvable into circuits of interacting neurons which are themselves logical networks of switches, exciting and inhibiting each other. These circuits can be treated by the methods of symbolic logic, and therefore the nervous activity involved in the processes of perception, memory and reasoning can be described by an algebraic calculus” (McCulloch; Pitts, 1943, s/p).

para a humanidade. Segundo O’Neil (2021), com o fenômeno da Internet,

[...] pessoas de todo o mundo têm produzido quadrilhões de palavras sobre nossas vidas e trabalhos, amizades e forma como compramos. Ao fazê-lo, construímos de modo involuntário a mais vasta coletânea de treinamento para máquinas de linguagem natural. Conforme trocamos papel por e-mail e redes sociais, as máquinas podiam estudar nossas palavras, compará-las com outras, e deduzir algo sobre seu contexto. O progresso tem sido rápido e dramático. Esses avanços em linguagem natural abriram um filão de possibilidades para os anunciantes. Os programas “sabem” o que uma palavra significa, ao menos o bastante para associá-la com certos comportamentos e resultados, ao menos parte das vezes. Impulsionados em parte por esse crescente domínio da língua, os anunciantes podem sondar padrões mais profundos. Um programa de publicidade pode começar com os detalhes mais comuns de demografia e geografia. Mas no curso de semanas e meses ele começa a aprender os padrões das pessoas em que está mirando e fazer previsões acerca de seus próximos passos. Passa a conhecê-las. E se for um programa predatório, afere suas fraquezas e vulnerabilidades e persegue o caminho mais eficiente para explorá-las (O’Neil, 2021, p. 74).

O monstruoso poder auferido pelas *Big Techs* passa a ser sensível na democracia quando há comprovações científicas de que postagens influenciam o comportamento de voto das pessoas: apesar de geralmente serem utilizados para os lucros dessas empresas, os dados passam a ser utilizados na política, já que cabe às políticas governamentais regulamentar os titãs da tecnologia (O’Neil, 2021).

Nesse ponto, o *machine learning*, que “faz com que a máquina aprenda certas funções a ponto de conseguir agir sem a interferência humana”, quando evolui para o *deep learning* e para a criação de redes neurais artificiais, torna-se um poderoso artifício, pois é considerado uma tecnologia pautada numa racionalidade formal e probabilística, capaz de realizar escolhas mais eficientes, objetivas e imparciais do que as humanas, sujeitas a falhas de enviesamento (Nunes, 2018).

Ocorre, no entanto, que tal alegada neutralidade vem se mostrando apenas aparente, já que a literatura específica diagnosticou que o algoritmo herda todo o conteúdo de seu humano-criador,

inclusive o preconceito (Frazão, 2018), como apontam os célebres exemplos de enviesamento algorítmico.

No caso COMPAS (*Correctional Offender Management Profiling for Alternative Sanctions*), por exemplo, o algoritmo de Perfil de Gerenciamento Corretivo de Infratores para Sanções Alternativas, elaborado pela empresa Northpointe (atual Equivant) e utilizado nos EUA para auxiliar juízes em suas decisões, apresentou enviesamento racial. O modelo avaliava a probabilidade de reincidência dos réus e, após investigação jornalística, verificou-se que pessoas negras classificadas como de alto risco de reincidência não voltavam a cometer crimes; enquanto pessoas brancas classificadas como de baixo risco reincidiam (Vieira, 2019).

Outro episódio célebre envolvendo vieses algorítmicos diz respeito aos anúncios de emprego da empresa Google. Um estudo empírico sobre carreiras em STEM (Ciência, Tecnologia, Engenharia e Matemática), pautado na criação de anúncios fictícios de posições de emprego e na atribuição aleatória a perfis de usuários masculinos ou femininos, identificou que, quando os anúncios foram direcionados a usuários com base em informações demográficas, houve uma tendência de exibir os anúncios de carreira em STEM para um público predominantemente masculino. Além disso, os custos dos anúncios voltados para mulheres eram maiores, por conta de uma menor taxa de cliques (Lambrecht; Tucker, 2019).

Para além das críticas à pretensa neutralidade algorítmica, há também questionamentos quanto aos processos envolvidos nesse tipo de tecnologia. Uma das questões mais controversas dos modelos de redes neurais artificiais, nessa toada, é a inócua tentativa de regular suas operações algorítmicas dirigidas por dados. Diferentemente de outras tecnologias, o modelo de aprendizado profundo demonstra a impossibilidade de explicação dos procedimentos realizados por seu sistema algorítmico, que age conforme a estrutura de dados que obtém. Essa impossibilidade, denominada na Ciência de Dados “inescrutabilidade do sistema”, significa que as operações realizadas nas camadas das redes neurais não podem ser plenamente compreendidas (Silveira, 2020).

Em outros tipos de aprendizagem de máquina, como nos algoritmos de árvores de decisão, regressão linear ou regressão logística, isso não ocorre, já que as regras para a escolha de determinado resultado são evidentes: é possível descobrir matematicamente

quais nós de uma rede neural profunda foram ativados, mas não as operações realizadas pelos neurônios que modelaram o resultado (Tiwari; Tiwari; Tiwari, 2018, p. 8).

Já existem propostas para a criação de um modelo dotado de inteligência artificial explicável - o que ficou conhecido como XAI (Explainable Artificial Intelligence), ou seja, uma tecnologia cujas previsões possam ser qualitativamente interpretáveis ou explicáveis pelo próprio agente inteligente (Ribeiro *et al.*, 2018). Para além dessa proposta, alguns cientistas da computação defendem que todo algoritmo pode ser compreendido a partir da estrutura de dados que o acompanha (Seaver, 2019).

O antropólogo Nick Seaver (2019), no entanto, afirma que a transparência não é a solução. Modelos de aprendizagem profunda são tão complexos que se tornam uma caixa-preta inviolável, tanto por conta do volume de dados que os alimenta quanto em razão do número de pessoas envolvidas em seu desenvolvimento. Tais fatores engendrariam um nível de enredamento que constitui um óbice à previsão do comportamento e dos resultados do modelo (Seaver, 2019).

O problema da inescrutabilidade e da opacidade algorítmica não apenas reforça o argumento da falsa neutralidade dos algoritmos, como também traz à tona o imbróglio da responsabilização jurídica:

Quem deve ser responsabilizado quando um robô, software ou dispositivo executado por algoritmos de redes neurais artificiais discrimina pessoas ou segmentos sociais, cria acidentes ou gera resultados injustos, ofensivos e até letais? Os seus desenvolvedores, analistas e pessoas envolvidas na sua modelagem? A corporação que o comercializa? A empresa ou o governo que o adotou? E a pergunta derradeira é se podemos responsabilizar alguém por algo que tem suas decisões geradas de um modo impossível de rastrear e, portanto, de compreender e explicar (Silveira, 2020, p. 91).

A responsabilização algorítmica é frequentemente encontrada na literatura especializada sob o termo *accountability*, que não possui tradução exata em português, em razão da própria ausência do conceito na sociedade. Por esse motivo é comum o uso do termo em seu idioma original. Segundo Campos (1990), o conceito de

accountability envolve, de um lado, a delegação de uma responsabilidade e, de outro lado, a gestão dos recursos delegados, gerando, uma obrigação de prestação de contas por parte daquele que exerce a referida gestão.

Todos esses imbróglis, advindos do avanço exponencial dos algoritmos, impulsionado pela ascensão das redes sociais e pela capacidade massiva de armazenamento de dados, engendram, para além de uma reconfiguração técnica e uma nova forma de comunicação e a interação social, um profundo impacto no âmbito político.

Plataformização e mídias sociais: a erosão da esfera pública eleitoral

Sérgio Amadeu (2019) elabora que a organização e a distribuição de conteúdos e anúncios nos *feeds* de notícias, notadamente pelo algoritmo Edgerank, responsável por classificar as interações, foram cruciais para o progresso das plataformas digitais. Essa dinâmica resulta em uma distribuição acelerada de informações, mediada por filtros ordenados e probabilísticos. O que, à primeira vista, pode parecer uma oportunidade de personalização de vendas no mercado, sob a ótica de Jodi Dean (2010), revela-se como uma capitalização dos meios comunicativos, em que as interações são mediadas por algoritmos de direcionamento de consumo baseados em preferências.

Nesse contexto, Joana Machado (2021) propõe que as plataformas digitais não se limitam a veicular conteúdo, mas são projetadas para formar redes em torno de ideias específicas. Isso ocorre por meio de conteúdos produzidos por indivíduos, que são subsequentemente agrupados por algoritmos operando sob uma lógica de maximização de preferências, a partir da qual esses conteúdos são distribuídos. Tal lógica assegura que determinados conteúdos sejam promovidos e alcancem grupos específicos com maior propensão ao engajamento. Essa visibilidade gerenciada por preferências reforça crenças preexistentes, instruindo a repercussão de certos assuntos e aproximando públicos por interesses comuns, o que inevitavelmente ocasiona a formação de "bolhas informacionais" (Machado, 2021).

Essa nova configuração do processo comunicacional ganhou particular destaque no meio político, onde seus efeitos são mais agudos para a saúde democrática. Antônio Barros *et al.* (2021), em sua pesquisa "Presença parlamentar nas mídias sociais", demonstram que a possibilidade de gerar identificação com pautas e a distribuição interativa reconfiguraram a atividade parlamentar. Assim, é possível afirmar que houve uma transição da tradicional campanha mediada pelo partido e suas diretrizes, veiculadas nas mídias convencionais, para "campanhas permanentes" produzidas pelos próprios agentes políticos, que se comunicam com suas bases a partir de uma mediação algorítmica que reforça os ideais políticos customizados (Barros, 2021).

Os impactos dessa transformação na esfera eleitoral são inegáveis. Uma pesquisa de opinião divulgada pelo DataSenado (2018) revelou que 45% dos entrevistados declararam ter decidido seu voto com base em informações obtidas em redes sociais. Além disso, o levantamento apontou que 79% dos participantes utilizam plataformas como WhatsApp como principal fonte de notícias, enquanto 50% manifestaram recorrer à televisão como canal informativo habitual. Essa pesquisa evidencia o recrudescimento da lógica de transferência de influência dos meios de comunicação tradicionais para as plataformas digitais, revelando uma "convolução entre o antigo e o novo" ao reafirmar o papel central das redes na formação da opinião pública.

No contexto político, portanto, essa dinâmica manifesta-se diretamente na forma como a lógica da representação se articula, engendrando uma prática cada vez mais mediada algorítmicamente e refletindo as intenções e estratégias adotadas pelos parlamentares. Desse modo, a premissa fundamental de que a democracia se realiza por meio de um processo representativo, sustentado em eleições livres, participação ampla e liberdade de escolha, mostra-se crescentemente tensionada pelas novas dinâmicas comunicacionais mediadas por algoritmos.

Sociólogos digitais, como Deborah Lupton (2014), Noortje Marres (2017) e Neil Selwyn (2019), têm alertado para as implicações dessa plataformização política, que permite a customização e o direcionamento de informações, não raramente falsas, a eleitores. Lupton (2014) discute como a coleta e análise de dados nas plataformas alteram as relações sociais e o modo como o indivíduo é

compreendido, ao passo que Marres (2017) foca na forma como as redes digitais se tornam infraestruturas para a ação social. Já para Sara Selwyn (2019), a sociologia digital deve ir além da análise de dados, investigando as lógicas algorítmicas que moldam as interações. Fato é que a literatura especializada contemporânea aponta para a capacidade dos algoritmos de criar bolhas informacionais e de reforçar vieses preexistentes, levando à polarização e à manipulação da opinião pública, o que, consequentemente, mina a autonomia do eleitor e a integridade do processo eleitoral.

Esses pontos são corroborados pelas preocupações de autores como Enrica Amaturro e Biagio Aragona (2019), que questionam a epistemologia do digital e o uso de *big data* na pesquisa social, e Mark Carrigan (2014), que propõe uma agenda para a sociologia digital focada nos impactos sociais.

Além disso, o manifesto da Ciência Social Computacional (Conte *et al.*, 2012) e as discussões sobre sociologia digital em obras como *Digital Sociologies* (Daniels; Gregory; Cottom, 2016) e *Digital Anthropology* (Horst; Miller, 2012) aprofundam a compreensão de como essas novas configurações tecnológicas transformam o tecido social e, em particular, as dinâmicas políticas e eleitorais. O risco, como aponta Elias (2008), é o da individualização excessiva que, mediada por algoritmos, fragmenta a esfera pública e dificulta a construção de um consenso democrático.

Considerações finais

A imersão na era digital reconfigurou profundamente a sociedade, transformando-a em um complexo ecossistema interconectado onde a comunicação e as relações sociais são inseparáveis das plataformas digitais. Nesse novo modelo, a exploração de dados pessoais, muitas vezes fornecidos gratuitamente, alimenta a mineração de dados e a criação de perfis detalhados, que são utilizados para o exercício de um poder sem precedentes, capaz de influenciar não apenas o consumo, mas também as preferências políticas dos cidadãos.

Os riscos inerentes a essa transformação são multifacetados e impactam diretamente as liberdades individuais e a própria democracia, já que a coleta e o cruzamento de dados pessoais, não raramente exemplificados por escândalos recentes, evidenciam a

fragilidade do direito à privacidade e a falta de autodeterminação informativa. Esses eventos expõem não apenas vulnerabilidades de segurança, mas também o potencial de manipulação de eleitores e a disseminação de *fake news*, comprometendo a integridade dos processos democráticos.

Quando a reconfiguração da comunicação política permite a formação de bolhas informacionais e a capitalização das interações em prol de ideologias, a ditadura de dados se torna especialmente agravada pela possibilidade de controle algorítmico da visibilidade e da capacidade de reforço de crenças preexistentes. Por isso, a transição das campanhas partidárias tradicionais para campanhas permanentes customizadas, aliada ao uso massivo de plataformas digitais como fonte primária de informação eleitoral, demonstra uma erosão da deliberação democrática e da autonomia do eleitor, já que o controle algorítmico da visibilidade e o reforço de crenças preexistentes comprometem a formação de uma esfera pública plural e informada.

É nesse contexto que os algoritmos *de destruição em massa* levantam preocupações sobre a autonomia humana, pois a mediação algorítmica na representação política permite a disseminação direcionada de *fake news* e a manipulação da opinião pública, minando a liberdade de escolha e a integridade do processo eleitoral. Por esse motivo, é imperativo que os legisladores e a sociedade civil compreendam a dimensão dos riscos da cultura algorítmica e trabalhem para desenvolver mecanismos robustos de regulamentação, transparência e responsabilização, a fim de salvaguardar a democracia na era digital.

REFERÊNCIAS

- AMARAL, Rogério do. **Exposição privada nas redes sociais: uma análise sobre o Facebook na sociedade contemporânea**. Tese (Doutorado). UNESP, FCT, 2016.
- AMATURO, Enrica; ARAGONA, Biagio. **Per un'epistemologia del digitale: note sull'uso di big data e computazione nella ricerca sociale**. Quaderni di Sociologia, v. 81, n. 81–LXIII, p. 71–90, 1 dez. 2019.
- BARROS, Frederico Kern Ferreira. **Fake News, legislação simbólica e a proteção dos direitos fundamentais e da personalidade digital**. In.: OMMATI, José Emílio Medauar (org.). *Escritos de direitos fundamentais*. Belo Horizonte: Conhecimento Editora, <https://www.google.com/search?q=2021>.
- ARAÚJO, Franciele Cassimiro de; ROSSI, Jackeline Magrin. **A evolução dos ataques cibernéticos**. Americana, 2020.
- BARROS, Antonio Teixeira de; BERNARDES, Cristiane Brum; FARIA, Cristiano Ferri Soares de; BUSANELLO, Elisabete. **Presença parlamentar nas mídias sociais: a estruturação dos mandatos digitais na Câmara dos Deputados**. Revista de Informação Legislativa: RIL, Brasília, DF, v. 58, n. 232, p. 57-86, out./dez. 2021. Disponível em: https://www12.senado.leg.br/ril/edicoes/58/232/ril_v58_n232_p57
- BARROS, Frederico Kern Ferreira. **Fake News, legislação simbólica e a proteção dos direitos fundamentais e da personalidade digital**. In.: OMMATI, José Emílio Medauar (org.). *Escritos de direitos fundamentais*. Belo Horizonte: Conhecimento Editora, 2021.
- BIONI, Bruno. **Proteção de Dados Pessoais: a função e os limites do consentimento**. Rio de Janeiro: Forense, 2019.
- BOURDIEU, Pierre. **A distinção**. São Paulo: Edusp, 2007.
- CAMPOS, Ana Maria. **Accountability: quando poderemos traduzi-la para o português?** Revista de Administração Pública. Rio de Janeiro, FGV, 24(2):30-50, fev./abr. 1990.
- CARRIGAN, Mark. **An Agenda for Digital Sociology**. The Sociological Imagination. [S.l.: s.n.]. Disponível em: <http://sociologicalimagination.org/archives/16568>. Acesso em: 13 abr. 2015., 30 dez. 2014.

CASTELLS, Manuel. *A sociedade em rede. Revista e ampliada*. Tradução de Roneide Majer. São Paulo: Paz e Terra, 2016.

CHAWLA, Ronit. Deepfakes: How a pervert shook the world. *International Journal of Advance Research and Development*, v. 4, n. 6, p. 4-8, 2019.

DAL BELLO, Cíntia. Visibilidade, vigilância, identidade e indexação: a questão da privacidade nas redes sociais digitais. *Logos*, v. 18, n. 1, 2011.

DANIELS, Jessie; GREGORY, Karen; COTTOM, Tressie McMillan (Org.). *Digital Sociologies*. Reprint edition ed. [S.l.]: Policy Press, 2016.

DEAN, J. *Communicative capitalism: Circulation and the foreclosure of politics*. *Cultural Politics*, v. 1, n. 1, p. 51-74, 2005.

DEBORD, Guy. *A sociedade do espetáculo*. Rio de Janeiro: Contraponto, 1997.

ELIAS, Norbert. *Sociologia do conhecimento: novas perspectivas*. *Sociedade e Estado*, v. 23, n. 3, 2008. Disponível em: <http://periodicos.unb.br/index.php/estado/article/view/3395>. Acesso em: 28 mar. 2017.

FOUCAULT, Michel. *Arqueologia do saber*. 6 ed. Rio de Janeiro: Forense Universitária, 2002.

FRAZÃO, Ana. *Algoritmos e inteligência artificial*. Jota, 2018.

FRAZÃO, Ana. *Fundamentos da proteção dos dados pessoais: Noções introdutórias para a compreensão da importância da Lei Geral de Proteção de Dados*. *Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito Brasileiro*, v. 1, p. 23-52, 2019.

G1. *Denúncias de crimes cometidos pela internet mais que dobram em 2020*. G1, 2021. Disponível em: <https://g1.globo.com/economia/tecnologia/noticia/2021/02/09/numero-de-denuncias-de-crimes-cometidos-pela-internet-mais-que-dobra-em-2020.ghtml>. Acesso em: 11 de set. de 2022.

GÉRON, Aurélien. *Hands-on machine learning with Scikit-Learn, Keras, and TensorFlow*. O'Reilly Media, Inc., 2022.

- GUIDI, TIMPONE; GUIDI, Michel. **Explorando a Mudança de Cenário da IA**. Da IA Analítica à IA Generativa, p. 2023-05, 2023.
- HAN, Jiawei; PEI, Jian; TONG, Hanghang. **Data mining: concepts and techniques**. Morgan Kaufmann, 2022.
- HORST, Heather A.; MILLER, Daniel. **Digital Anthropology**. [S.l.]: Bloomsbury Academic, <https://www.google.com/search?q=2012>.
- JÚNIOR, Antonio Rulli; NETO, Antonio Rulli. **Direito ao Esquecimento e o Superinformacionismo**: apontamentos no direito brasileiro dentro do contexto de sociedade da informação. Revista ESMAT, v. 5, n. 6, p. 11-30, 2013.
- KASPERSKY. **Ciberataques crescem 23% no Brasil em 2021**. Kaspersky, 2021. Disponível em: <https://www.kaspersky.com.br/blog/panorama-ciberameacas-brasil-2021-pesquisa/18020/>. Acesso em: 11 de set. de 2022.
- KLEINBERG, J.; EASLEY, D. **Networks, Crowds, and Markets: Reasoning about a Highly Connected World**. Cambridge: University Press, 2010.
- LAMBRECHT, Anja; TUCKER, Catherine. **Algorithmic bias? An empirical study of apparent gender-based discrimination in the display of STEM career ads**. Management science, v. 65, n. 7, p. 2966-2981, 2019.
- LAVAL, Christian; DARDOT, Pierre. **A nova razão do mundo: ensaio sobre a sociedade neoliberal**. São Paulo: Boitempo, 2016.
- LÉVY, P. **Cibercultura**. São Paulo: Editora 34, 1999.
- LIRA, L. de A. **Lei Carolina Dieckmann: (in) eficácia da proteção dos direitos fundamentais à intimidade e à vida privada em face da pena cominada aos delitos informáticos**. Brasília, DF: Conteúdo Jurídico, 2014.
- LOURENÇO, Gabriel D. **Cibercrimes no Brasil crescem em 23% em 2021, aponta pesquisa**. Olhar Digital, 2022. Disponível em: <https://olhardigital.com.br/2021/08/31/seguranca/cibercrime-brasil-2021/>. Acesso em: 11 de set. de 2022.
- LUPTON, Deborah. **Digital Sociology**. [S.l.]: Routledge, 2014. Disponível em: [link suspeito removido]. Acesso em: 19 ago. 2018

- MACHADO, Joana; TOLEDO, Larissa Fonseca. **Plataformas digitais e discurso de ódio entre liberalismo e constitucionalismo digital: uma análise do modelo regulatório do PL 2360/2020**. *International Journal of Digital Law*, Belo Horizonte, v. 5, n. 3, p. 67-93, 2025. DOI: 10.47975/digital.law.vol.5.n.3.machado. Disponível em: <https://journal.nuped.com.br/index.php/revista/article/view/1286>. Acesso em: 8 jun. 2025.
- MAFFESOLI, M. **Perspectivas tribais ou a mudança do paradigma social**. *Revista FAMECOS*, Porto Alegre, n. 23, abr. 2004.
- MANZANO, José Augusto NG; DE OLIVEIRA, Jayr Figueiredo. **Algoritmos lógica para desenvolvimento de programação de computadores**. Saraiva Educação SA, 2000.
- MARAS, Marie-Helen; ALEXANDROU, Alex. **Determining authenticity of video evidence in the age of artificial intelligence and in the wake of Deepfake videos**. *The International Journal of Evidence & Proof*, v. 23, n. 3, p. 255-262, 2019.
- MARRES, Noortje. **Digital Sociology**. Malden, MA: Polity Press, 2017.
- MATSUBARA, Edson Takashi. **O algoritmo de aprendizado semi-supervisionado co-training e sua aplicação na rotulação de documentos**. 2004. Tese de Doutorado. Universidade de São Paulo.
- MCCARTHY, John. **What is artificial intelligence**. 2007.
- MCCULLOCH, Warren S.; PITTS, Walter. **A logical calculus of the ideas immanent in nervous activity**. *The bulletin of mathematical biophysics*, v. 5, p. 115-133, 1943.
- MURDOCK, Graham. **Media materialities: For a moral economy of machines**. *Journal of Communication*, v. 68, n. 2, p. 359-368, 2018.
- NORA, Pierre. **Les Lieux de Mémoire**. Paris: Gallimard, 1987.
- NUNES, Ana Carolina de Assis. **Entre redes neurais naturais e artificiais: estudo antropológico sobre humanidade e inteligência artificial em algumas revistas brasileiras**. Dissertação de Mestrado. Universidade Federal de Goiás, Faculdade de Ciências Sociais, Programa de Pós-Graduação em Antropologia Social.

- O DILEMA DAS REDES.** Netflix, 2020. Documentário disponível em: <https://www.netflix.com>. Acesso em 11 de set. de 2022.
- O GUIA FINANCEIRO.** Big Data: Como a Target descobriu uma gravidez antes da família?. O Guia Financeiro, 2019. Disponível em <https://www.oguiafinanceiro.com.br/textos/big-data-como-a-target-descobriu-uma-gravidez-antes-da-propria-familia/>. Acesso em 11 de set. de 2022.
- O'NEIL, Cathy.** Algoritmos de destruição em massa. Editora Rua do Sabão, 2021.
- QIN, Jian; ZENG, Marcia Lei.** Metadata. American Library Association, 2020.
- RIBEIRO, Marco Tulio; SINGH, Sameer; GUESTRIN, Carlos.** "Why should i trust you?" *Explaining the predictions of any classifier*. In: *Proceedings of the 22nd ACM SIGKDD international conference on knowledge discovery and data mining*. 2016. p. 1135-1144.
- RODOTÀ, Stefano et al.** A vida na sociedade da vigilância: a privacidade hoje. In: *A vida na sociedade da vigilância: a privacidade hoje*, 2008.
- ROETS, Arne et al.** 'Fake news': *Incorrect, but hard to correct. The role of cognitive ability on the impact of false information on social impressions*. *Intelligence*, v. 65, p. 107-110, 2017.
- RUSSELL, Stuart J.** *Artificial intelligence a modern approach*. Pearson Education, Inc., 2021.
- SAYURI, Juliana.** Retratos de uma juventude. Estadão, 2014. Disponível em: <http://www.estadao.com.br/noticias/geral,retrato-de-umajuventude,1167792>. Acesso em: 11 de set. de 2022.
- SCHWAB, Klaus.** *A quarta revolução industrial*. Edipro, 2019.
- SEAYER, N.** Knowing Algorithms. In: VERTESI, J.; RIBES, D. (Eds.). *DigitalSTS: A Field Guide for Science & Technology Studies*. Princeton: Princeton University Press, 2019.
- SELWYN, Neil.** *What Is Digital Sociology?* Cambridge: Polity Press, 2019.

SENADO FEDERAL. Redes sociais influenciam voto de 45% da população, indica pesquisa do DataSenado. Senado Notícias, 12 dez. 2019. Disponível em: <<https://www12.senado.leg.br/noticias/materias/2019/12/12/redes-sociais-influenciam-voto-de-45-da-populacao-indica-pesquisa-do-datasenado>>. Acesso em: 07 fev. 2025.

SILVA, Ivan Nunes da; SPATTI, Danilo Hernane. Redes Neurais Artificiais: Teoria e Aplicações em Inteligência Computacional. 2ª ed. São Paulo: Blucher, 2017.

SILVEIRA, Sergio Amadeu. Discursos sobre regulação e governança algorítmica. Estudos de sociologia, v. 25, n. 48, 2020.

SILVEIRA, Sérgio Amadeu. Democracia e os códigos invisíveis: como os algoritmos estão modulando comportamentos e escolhas políticas. 1. São Paulo: Edições SESC-SP, 2019.

SILVEIRA, Sérgio Amadeu. Responsabilidade algorítmica, personalidade eletrônica e democracia. Revista Eletrônica Internacional de Economia Política da Informação, da Comunicação e da Cultura, v. 22, n. 2, p. 83-96, 2020.

SIQUEIRA, Alessandra Cristina de Mendonça. O Colonialismo Digital Como Nova Forma de Imperialismo na Sociedade em Rede. Revista do Mestrado em Direito da UFS, V.8, N.01, p. 29 – 50, Jan-Jun/2019, ISSN 2237-2040, 2019.

SRNICEK, N. Platform Capitalism. New York: John Wiley & Sons, 2016.

TIWARI, Tanya; TIWARI, Tanuj; TIWARI, S. How Artificial Intelligence, Machine Learning and Deep Learning are Radically Different? International Journal of Advanced Research in Computer Science and Software Engineering, v. 8, n. 2, p. 1-9, mar. 2018. ISSN 2277128X. Disponível em: <http://ijarcsse.com/index.php/ijarcsse/article/view/569>. Acesso em: 07 set. 2019.

TURING, Alan M. Computing machinery and intelligence. Springer Netherlands, 2009.

VAN DIJCK, José; POELL, Thomas; DE WAAL, Martijn. The platform society: Public values in a connective world. Oxford university press, 2018.

VENTURA, Katia Santiago; DE ALBUQUERQUE SIEBRA, Sandra; LIMA, Marcos Galindo. A visão sistêmica na efetivação da Lei de Acesso à Informação: o caso da Universidade Federal de Pernambuco. UFPE, 2013.

VIEIRA, Leonardo Marques. A problemática da inteligência artificial e dos vieses algorítmicos: caso COMPAS. In: Brazilian Technology Symposium. 2019.

VIEIRA, Tatiana Malta. O direito à privacidade na sociedade da informação: efetividade desse direito fundamental diante dos avanços da tecnologia da informação. Porto Alegre: Sergio Fabris, 2007.

ZUBOFF, Shoshana. A era do capitalismo de vigilância. Editora Intrínseca, 2021.