ARTIGO

Inteligência artificial e desigualdade social: o impacto do colonialismo digital nas políticas públicas

Letícia Lé Oliveira
leticialeolv@gmail.com

Bacharel pela Faculdade de Direito da Universidade de São Paulo e Pós-Graduanda em Direito Digital pela Fundação Getúlio Vargas.

V. 5 / N. 1 / JULHO DE 2024
PÁGINAS 148 A 167

LETÍCIA LÉ OLIVEIRA

Inteligência artificial e desigualdade social: o impacto do colonialismo digital nas políticas públicas

Palavras-chave
Inteligência Artificial
Colonialismo Digital
Direitos Fundamentais
Políticas Públicas

Resumo
Este artigo tem como objetivo analisar a intersecção entre os direitos fundamentais e a inteligência artificial, com um foco particular no colonialismo digital e na proteção constitucional. Busca-se compreender como as práticas de vigilância e controle de dados por grandes empresas e eventualmente poderes estatais desafiam os princípios constitucionais e os direitos fundamentais, bem como explorar as respostas jurídicas e políticas necessárias para mitigar esses desafios.

V. 5 / N. 1 / JULHO DE 2024
PÁGINAS 148 A 167

Artificial intelligence and social inequality: the impact of digital colonialism on public Policy

Keywords
Artificial Intelligence
Digital Colonialism
Fundamental Rights
Public Policies

Abstract
This article aims to analyze the intersection between fundamental rights and artificial intelligence, with a particular focus on digital colonialism and constitutional protection. It seeks to understand how surveillance practices and data control by large corporations and eventually government powers challenge constitutional principles and fundamental rights, as well as to explore the legal and political responses needed to mitigate these challenges.

1 Introdução

O avanço acelerado da tecnologia, com especial destaque para o campo da inteligência artificial (IA)[1], tem gerado uma série de desafios e oportunidades que impactam diretamente a proteção dos direitos fundamentais. De acordo com Russel e Norwig (2021), entende-se que Inteligência Artificial é

> "o campo de estudo e desenvolvimento de sistemas computacionais capazes de realizar tarefas que normalmente requerem inteligência humana, como reconhecimento de fala, tomada de decisão, tradução de idiomas e percepção visual. A IA pode ser dividida em subcampos específicos, incluindo aprendizado de máquina, processamento de linguagem natural, visão computacional, e robótica, entre outros". (Russel & Norwig, 2021)

A crescente interação entre o mundo digital e o mundo real tem transformado as formas de socialização - econômica e política - demandando uma reavaliação dos conceitos tradicionais de privacidade, liberdade e controle. Nesse contexto, emerge a compreensão da categoria que é conhecida como colonialismo digital, definido por Cassino et al. (2022, p. 17) como uma nova forma de dependência que combina práticas predatórias do colonialismo histórico com métodos abstratos de quantificação computacional.

A proteção dos direitos fundamentais, tais como a privacidade e a dignidade da pessoa humana, enfrenta desafios significativos diante dessa nova realidade digital. A Constituição Federal de 1988, que consagra a dignidade da pessoa humana como um de seus fundamentos, deve também ser reinterpretada e aplicada de modo a proteger os cidadãos contra os abusos potenciais do colonialismo digital. Neste sentido, a promulgação da Lei Geral de Proteção de Dados (LGPD), em 2018, representa um marco importante, estabelecendo diretrizes claras para a coleta, tratamento e armazenamento de dados pessoais[2]. Todavia, a efetividade dessa legislação depende de sua implementação rigorosa e da adaptação contínua às rápidas mudanças tecnológicas.

A discussão aqui proposta será estruturada em quatro seções principais. Na primeira, serão abordados os conceitos de direitos fundamentais na era digital, destacando a evolução da proteção de dados e privacidade como direitos essenciais. Na segunda seção, será explorado o conceito de colonialismo digital e suas implicações, incluindo a análise do capitalismo de vigilância. A terceira seção discutirá os desafios jurídicos e tecnológicos impostos pelo colonialismo digital à proteção dos direitos fundamentais. Finalmente, a quarta seção apresentará propostas de políticas públicas e intervenções legislativas para proteger os direitos na era digital.

Diante da crescente importância da inteligência artificial e da digitalização na sociedade contemporânea, a proteção dos direitos fundamentais torna-se uma questão urgente e complexa.

A metodologia deste artigo adota uma abordagem mista que combina análise teórica e empírica para uma compreensão aprofundada do impacto da inteligência artificial (IA) e do colonialismo digital sobre direitos fundamentais. A análise teórica será fundamentada na literatura acadêmica existente sobre proteção de dados, discriminação algorítmica e vigilância digital, integrando conceitos e debates presentes nas áreas de direito e políticas públicas. Serão incorporados dados empíricos sobre violações de privacidade e casos de discriminação algorítmica, extraídos de relatórios, estudos de ONGs e instituições de pesquisa, bem como um estudo comparativo entre diferentes países que implementaram regulamentações de proteção de dados.

Desse modo, este estudo pretende contribuir para o debate acadêmico e jurídico sobre como o Direito pode responder de forma eficaz a esses novos desafios, promovendo um desenvolvimento tecnológico que respeite e proteja os direitos humanos.

1. A inclusão da proteção de dados e privacidade como direitos fundamentais.

A proteção de dados pessoais emergiu como uma questão central no século XXI, impulsionada pelo crescimento exponencial da coleta, armazenamento e processamento de dados pelas empresas e governos. Este fenômeno, frequentemente descrito como a "era dos dados", trouxe à tona preocupações significativas sobre privacidade, segurança e autonomia individual. Mayer-Schönberger e Cukier (2013) destacam que a capacidade de coletar e analisar grandes volumes de dados transformou diversos aspectos da sociedade, desde negócios até políticas públicas.

O reconhecimento da proteção de dados como um direito fundamental tem implicações profundas para a estruturação das interações sociais e econômicas. A legislação de proteção de dados, como a GDPR e a LGPD, busca criar um equilíbrio entre a necessidade de inovação tecnológica e a proteção dos direitos individuais. Ao garantir que os dados pessoais sejam tratados de maneira ética e transparente, essas leis não apenas protegem a privacidade, mas também promovem um ambiente de confiança que é essencial para o desenvolvimento econômico e social.

A privacidade, tradicionalmente entendida como o direito de estar só, passou por uma transformação significativa com o advento da era digital. A definição clássica de privacidade, conhecida como “o direito de ser deixado em paz”, articulada por Warren and Brandeis (1890) e baseada na ideia de que a privacidade é um direito essencial à dignidade e ao bem-estar individual, sendo fundamental para proteger a integridade moral e psicológica das pessoas, não é mais suficiente para abordar as complexidades introduzidas pela tecnologia moderna. Na era digital, a privacidade envolve não apenas a proteção contra intrusões físicas, mas também a proteção contra a coleta e uso indevido de informações pessoais.

Zuboff (2019) argumenta que a privacidade deve ser contextualizada em um mundo onde os dados pessoais são constantemente coletados, analisados e monetizados por empresas de tecnologia. Ela introduz o conceito de "capitalismo de vigilância", no qual o comportamento humano é transformado em dados que são utilizados para prever e influenciar futuras ações. Zuboff (2019) destaca ainda que essa prática cria formas de poder e controle, onde as empresas detêm vastas quantidades de informações sobre os indivíduos, muitas vezes sem o seu conhecimento ou consentimento. Este novo paradigma exige uma reavaliação das normas jurídicas de privacidade para proteger os indivíduos contra a exploração e manipulação de seus dados pessoais.

A proteção de dados e a privacidade não são apenas elementos essenciais para a dignidade e a liberdade dos indivíduos, mas também fundamentais para a autonomia pessoal. Segundo Rodotà et al. (2008), a proteção de dados é uma condição indispensável para a realização da dignidade humana na sociedade contemporânea. Este reconhecimento da proteção de dados como um direito fundamental tem implicações profundas e necessárias para a estruturação das interações sociais e econômicas. Ao garantir que os dados pessoais sejam tratados de maneira ética e transparente, essas leis não apenas protegem a privacidade, mas também promovem um ambiente de confiança

que é essencial para o desenvolvimento econômico e social.

Neste sentido, a dignidade humana, como princípio fundamental, está intrinsecamente ligada à proteção da privacidade e dos dados pessoais. A vigilância e a coleta indiscriminada de dados podem levar à manipulação e ao controle das escolhas individuais, comprometendo a liberdade e a autonomia. Portanto, proteger os dados pessoais é proteger a capacidade dos indivíduos de tomar decisões livres e informadas sobre suas próprias vidas.

A implementação de regulamentações como a GDPR e a LGPD apresenta tanto desafios quanto oportunidades no campo dos direitos fundamentais. Por um lado, essas leis impõem novas responsabilidades e custos às organizações que coletam e processam dados pessoais. As empresas devem investir em sistemas de compliance, treinamento de funcionários e infraestrutura tecnológica para assegurar a conformidade com as normas de proteção de dados. Além disso, a aplicação extraterritorial dessas leis, como é o caso da GDPR, cria complexidades adicionais para as organizações que operam em múltiplas jurisdições.

Os desafios também incluem a necessidade de adaptar rapidamente as regulamentações às novas tecnologias. A Inteligência Artificial (IA), a Internet das Coisas (IoT) e o big data trazem novos riscos e oportunidades para a proteção de dados. A IA, por exemplo, tem sido usada para analisar grandes volumes de dados e fazer previsões ou decisões automatizadas, o que levanta questões significativas sobre transparência, responsabilidade e vieses. Segundo Crawford (2021), os sistemas de IA operam frequentemente com opacidade, dificultando a compreensão de seus critérios de decisão e introduzindo vieses que refletem as limitações dos dados usados para treinamento, o que pode resultar em discriminação e injustiça algorítmica (Crawford, 2021, p. 215). Complementarmente, Obermeyer et al. (2019) destacam que algoritmos de IA, especialmente em setores críticos como saúde e finanças, têm reproduzido preconceitos presentes nos dados históricos, exacerbando desigualdades e afetando desproporcionalmente grupos vulneráveis (Obermeyer et. al, 2019, p. 447-453).

Já a Internet das Coisas (IoT), com dispositivos conectados que coletam dados em tempo real, aumenta exponencialmente a quantidade de dados disponíveis e o risco de violações de privacidade. De acordo com Zuboff (2019), a coleta contínua de dados por dispositivos IoT alimenta o que ela chama de "capitalismo de vigilância," onde a privacidade dos indivíduos é comprometida para sustentar modelos de negócio baseados na exploração de dados pessoais (Zuboff, 2019, p. 340). Esses dispositivos, como observa Greengard (2020), geram novos desafios de segurança e privacidade, pois muitas vezes carecem de proteções robustas contra invasões, colocando os dados dos usuários em constante vulnerabilidade (Greengard, 2020, p. 56).

Por outro lado, essas regulamentações oferecem uma oportunidade para fortalecer a confiança dos consumidores e promover práticas comerciais mais éticas e transparentes. A proteção de dados eficaz pode ser um diferencial competitivo para as empresas, atraindo clientes que valorizam a privacidade e a segurança de suas informações pessoais. Além disso e principalmente: a proteção de dados contribui para a construção de um ambiente digital mais seguro e confiável, incentivando a inovação e o desenvolvimento econômico sustentável.

Um dos principais desafios na proteção de dados é garantir a conformidade em um ambiente globalizado, onde os dados frequentemente atravessam fronteiras nacionais. A cooperação internacional é essencial para abordar questões transfronteiriças de privacidade e segurança de dados. A criação de frameworks internacionais e a harmonização de normas de proteção de dados podem facilitar a cooperação e a coordenação entre diferentes jurisdições,

promovendo uma abordagem mais coerente e eficaz para a proteção de dados.

A literatura destaca que a proteção de dados e a privacidade não são apenas questões de conformidade regulatória, mas também de ética e responsabilidade social. Autores como Nissenbaum (2009), defendem que a privacidade deve ser vista como um bem social que contribui para a integridade e coesão das comunidades. Nissenbaum (2009) argumenta que a privacidade contextualizada, onde os dados são tratados de acordo com as normas sociais e expectativas do contexto específico, é fundamental para garantir que a proteção de dados seja eficaz e respeite os valores sociais.

Em uma análise comparativa, é possível observar que a implementação de legislações de proteção de dados na América Latina é uma área que tem visto avanços significativos nas últimas décadas, refletindo a crescente conscientização sobre a importância da privacidade e segurança dos dados. No entanto, cada país da região tem adotado abordagens distintas, influenciadas por contextos políticos, econômicos e sociais únicos, além de enfrentar o desafio adicional do colonialismo digital.

Na Colômbia, a proteção de dados pessoais é garantida pela Constituição Política do país, que reconhece o direito de cada cidadão de conhecer, atualizar, retificar e cancelar suas informações pessoais. A abordagem colombiana enfatiza a transparência e o consentimento do usuário, refletindo um compromisso robusto com a proteção de dados (Veloso Meireles, 2023). No entanto, a implementação prática dessas diretrizes ainda encontra obstáculos, especialmente em áreas com menor acesso à tecnologia e informação.

O Chile promulgou a Lei de Proteção de Dados Pessoais (LFPD) em 1999, com revisões importantes em 2018. A LFPD proíbe o tratamento inadequado de dados sensíveis e impõe sanções para violações. Embora o Chile tenha uma estrutura legal para a proteção de dados, a lei ainda carece de um órgão regulador independente, o que limita sua eficácia e a confiança do público (Veronese et al., 2023).

O México implementou a Lei Federal de Proteção de Dados Pessoais (LFPDPPP) em 2010, atualizada em 2018, que estabelece princípios como minimização de dados e responsabilidade. A LFPDPPP exige consentimento explícito do usuário antes da coleta e processamento de dados (Baptista Luz Advogados et al., 2022). No entanto, a aplicação prática da legislação ainda enfrenta obstáculos, especialmente em áreas rurais e entre comunidades indígenas, conforme relatado pela Asociación por los Derechos Civiles (ADC, 2021). Essas desigualdades geográficas e econômicas limitam o alcance da lei e permitem que empresas internacionais se aproveitem de lacunas regulatórias para coleta de dados, reforçando uma dependência que reflete o colonialismo digital.

No contexto do colonialismo digital, a América Latina enfrenta a dominação de grandes corporações e países desenvolvidos sobre suas infraestruturas digitais e dados. Essa dinâmica de poder pode resultar na exploração dos dados dos cidadãos latino-americanos, restringindo a autonomia digital da região. Empresas de tecnologia globalmente dominantes frequentemente controlam vastos volumes de dados, o que levanta preocupações sobre soberania digital e proteção adequada dos dados dos cidadãos (Veloso Meireles, 2023).

Deste modo, a complexidade crescente das interações digitais e a expansão da coleta de dados em escala global evidenciam que a privacidade e a proteção de dados transcendem o domínio do controle individual sobre informações pessoais e se inserem profundamente em questões éticas, sociais e políticas. Em um ambiente digital marcado pela interdependência global e por novas formas de poder corporativo, a proteção de dados assume o papel de um contrapeso indispensável à expansão do “capitalismo de vigilância” e à exploração

econômica dos dados pessoais. Nesse contexto, mais do que salvaguardar a dignidade e a liberdade dos indivíduos, as regulamentações como a GDPR e a LGPD representam uma tentativa de estabelecer novos paradigmas de justiça e responsabilidade na era digital.

2. Impacto da digitalização e da IA nos Direitos Fundamentais

A digitalização e a IA revolucionaram a forma como os dados pessoais são coletados, armazenados e processados. A digitalização, aqui, trata-se da "transformação de representações contínuas e analógicas (como som, imagem, texto e formas físicas) em dados digitais que podem ser armazenados, processados e transmitidos em redes computacionais" (Brennen & Kreiss, 2014). Esse processo de digitalização inclui não só a criação de representações digitais de objetos e informações físicas, mas também a reestruturação de práticas sociais, econômicas e culturais para operar dentro do contexto digital.

Estas tecnologias e transformações tecnológicas modificaram radicalmente também a forma como a informação é produzida, distribuída e consumida. Plataformas digitais e redes sociais utilizam aplicações de IA customizando os algoritmos de modo a personalizar o conteúdo que os usuários veem, com base em seus comportamentos e preferências passadas. Embora isso possa aumentar o engajamento e a satisfação dos usuários, também pode criar "bolhas de filtro" e câmaras de eco, limitando a exposição a diferentes pontos de vista e polarizando o discurso público. As “bolhas de filtro”, aqui citadas, são, como explica Pariser (2011, p. 9) " seu próprio universo pessoal e único de informações em que você vive online. E o que está na sua bolha de filtro depende de quem você é e do que você faz. Mas você não decide o que entra – e, mais importante, você não vê o que é filtrado." Ou seja, surgem da personalização feita por algoritmos de recomendação, como os usados em redes sociais, mecanismos de busca e plataformas de conteúdo. Já as câmaras de eco, conforme conceituadas por Sunstein (2018, p. 10), trata-se de “uma situação em que muitas pessoas ouvem ecos de suas próprias vozes, porque estão escutando pessoas com ideias afins ou com pontos de vista semelhantes (...)”.

Além disso, o uso de IA para moderar conteúdo nas plataformas digitais levanta preocupações sobre censura e liberdade de expressão. Crawford (2021) explica que os sistemas de IA usados na moderação são, por vezes, “opacos e tendenciosos,” porque operam sob algoritmos que refletem preconceitos embutidos, resultando em uma censura inadvertida de conteúdos de minorias ou de temas sensíveis. Ela menciona: “A censura algorítmica frequentemente opera sob uma lógica binária, onde nuances de expressão e contexto cultural são sacrificados em prol da padronização e da obediência a diretrizes muitas vezes inflexíveis" (Crawford, 2021, p. 215). Ademais, Douek (2020), professora e pesquisadora de liberdade de expressão, aponta que a IA aplicada à moderação automatizada frequentemente toma decisões de remoção de conteúdo com base em categorias binárias e inconsistentes com a complexidade da linguagem e do contexto humano. Ela argumenta que “a tecnologia de IA carece da capacidade de contextualizar o discurso, o que frequentemente resulta em uma aplicação desproporcional de normas de censura” (Douek, 2020, p. 231).

Assim, conteúdos que seriam permitidos no contexto humano podem ser censurados erroneamente pela IA. Algoritmos de moderação de conteúdo podem remover injustamente postagens e perfis, muitas vezes sem explicação ou recurso adequado. Isso pode resultar na supressão de vozes dissidentes e na limitação

do debate democrático, comprometendo o direito à liberdade de expressão protegido pela Constituição e por tratados internacionais de direitos humanos.

No trabalho de Wu (2017) se explora como as plataformas digitais competem pela atenção dos usuários, muitas vezes manipulando informações e criando ambientes propícios à desinformação e à manipulação. Para proteger a liberdade de expressão na era digital, é essencial equilibrar a moderação de conteúdo com a transparência e a responsabilidade das plataformas, além de garantir que os usuários tenham acesso a um processo justo de apelação contra decisões automatizadas.

A digitalização e a IA também oferecem oportunidades para melhorar o acesso à justiça, mas apresentam desafios que precisam ser cuidadosamente gerenciados. Ferramentas de IA podem ser usadas para automatizar tarefas jurídicas, como a revisão de documentos e a previsão de resultados judiciais, aumentando a eficiência e reduzindo os custos legais. Isso pode tornar os serviços jurídicos mais acessíveis para indivíduos e pequenos negócios que de outra forma não poderiam arcar com os custos.

No entanto, a automação do processo judicial também levanta questões sobre transparência, responsabilidade e justiça. Algoritmos de IA utilizados em decisões judiciais e administrativas devem ser transparentes e passíveis de auditoria para garantir que suas decisões sejam justas e imparciais. Além disso, é crucial garantir que os indivíduos afetados por essas decisões automatizadas tenham o direito de contestá-las e buscar reparação.

Yeung (2017) destaca a necessidade de um quadro regulatório robusto para governar o uso de IA no sistema judicial. Ela argumenta que a regulação algorítmica deve ser orientada por princípios de justiça procedimental, transparência e responsabilidade, a fim de proteger os direitos fundamentais e garantir a equidade nas decisões automatizadas.

Ademais, a IA tem o potencial de perpetuar e amplificar discriminações existentes na sociedade. A discriminação algorítmica é uma consequência direta do colonialismo digital, afetando desproporcionalmente os grupos vulneráveis. Algoritmos treinados em conjuntos de dados históricos tendem a replicar os vieses e preconceitos presentes nesses dados. Quando esses algoritmos são usados para tomar decisões em áreas críticas, como emprego, crédito, habitação e justiça criminal, eles podem replicar e até exacerbar esses preconceitos.

O'Neil (2016) discute como algoritmos de IA podem ser "armas de destruição matemática", criando ciclos de discriminação e desigualdade. Ela destaca casos em que algoritmos de pontuação de crédito, predição de crimes e contratação de funcionários resultaram em discriminação contra minorias e grupos marginalizados. "Os modelos matemáticos podem perpetuar a discriminação existente, pois são treinados com dados históricos que refletem essas desigualdades" (O'Neil, 2016, p. 45).

Essas preocupações são ecoadas por Eubanks (2018), onde ela examina como os sistemas automatizados utilizados para fornecer serviços públicos podem reforçar a exclusão social. Eubanks argumenta que "os algoritmos que determinam quem recebe assistência social, quem é elegível para moradia pública e quem é monitorado pelo sistema de justiça criminal muitas vezes refletem e ampliam preconceitos e desigualdades sociais existentes" (Eubanks, 2018, p. 29).

À medida que a digitalização e a IA reconfiguram o espaço dos direitos fundamentais, emergem, portanto, questões profundas sobre a interseção entre controle automatizado e dignidade humana. Essas tecnologias, ao mesmo tempo em que facilitam o acesso à informação e a justiça, também introduzem um novo paradigma: a de uma sociedade que, inadvertidamente, delega suas decisões e julgamentos a sistemas opacos e impessoais. Se a digitalização, na

busca por eficiência, não contemplar o necessário respeito ao pluralismo e à autonomia individual, ela corre o risco de substituir os valores democráticos pela tirania algorítmica. Emerge, assim, a necessidade de um amplo debate sobre o tema, abarcando as mais diversas áreas dos setores público e privado.

3. Colonialismo Digital e Capitalismo de Vigilância

Couldry e Mejias (2019, p.1) definem o colonialismo de dados como uma nova forma de colonialismo, onde as práticas extrativistas do período colonial histórico são replicadas através da captura de dados em massa. Eles afirmam, ainda, que "o colonialismo de dados combina as práticas extrativas predatórias do colonialismo histórico com os métodos abstratos de quantificação da computação, transformando a vida humana em dados que podem ser apropriados para o capitalismo".

O colonialismo digital é um conceito, portanto, utilizado para descrever as dinâmicas de poder e controle exercidas por empresas de tecnologia e Estados sobre os dados, informações e infraestruturas digitais de outros países ou regiões, especialmente aquelas em desenvolvimento. Este conceito é empregado para analisar como as práticas de coleta, processamento e monetização de dados podem perpetuar desigualdades econômicas, sociais e políticas, replicando padrões históricos de exploração e dominação colonial.

Em sua análise, Faustino e Lippold (2023) destacam que o colonialismo digital não é apenas uma metáfora, mas uma dominação concreta que envolve a "subordinação econômica, política, social e racial de determinados territórios" por meio de tecnologias digitais. Eles afirmam que esse modelo de dominação reproduz as lógicas coloniais, agora reconfiguradas pela dependência tecnológica, onde as infraestruturas e o acesso a dados são controlados majoritariamente pelos países do Norte Global, como Estados Unidos.

Uma das características centrais do colonialismo digital é a centralização do poder nas mãos de poucas corporações tecnológicas. Essas empresas possuem não apenas os recursos financeiros, mas também a infraestrutura e os dados necessários para influenciar comportamentos e decisões em uma escala global. O controle sobre os dados permite que essas corporações direcionem a inovação tecnológica, moldem políticas públicas e influenciem economias inteiras.

Assim, no contexto do colonialismo digital, a assimetria de poder entre as corporações tecnológicas e os usuários individuais se torna evidente. Os dados pessoais, coletados muitas vezes sem consentimento informado, são transformados em commodities valiosas. Os usuários, por outro lado, frequentemente desconhecem a extensão da coleta de dados e a forma como seus dados são utilizados. Essa falta de transparência e de consentimento informado perpetua uma dinâmica de exploração, onde os benefícios econômicos são concentrados nas mãos de poucos, enquanto os riscos e as vulnerabilidades são distribuídos entre muitos.

O colonialismo digital também cria dinâmicas de dependência tecnológica e econômica. Países em desenvolvimento, sem a infraestrutura ou os recursos para competir com gigantes tecnológicas, tornam-se dependentes das tecnologias e serviços oferecidos por essas corporações. Essa dependência limita a capacidade desses países de desenvolverem suas próprias soluções tecnológicas e econômicas, perpetuando um ciclo de subordinação e exploração. Empresas e governos de países em desenvolvimento são frequentemente obrigados a confiar nesses serviços para suas operações diárias, criando vulnerabilidades significativas. A centralização dos dados em infraestruturas controladas por corporações

estrangeiras também levanta questões de soberania e segurança nacional.

Outra forma de enxergar o colonialismo digital é a partir da compreensão de que ele é uma forma contemporânea de extrativismo, onde os dados pessoais são explorados como recursos naturais. Couldry e Mejias (2020) afirmam que "a exploração de dados é uma forma contemporânea de extrativismo, onde os dados pessoais são coletados e transformados em mercadorias exploráveis, perpetuando desigualdades globais" (Couldry & Meijas, 2019, p.2). A coleta massiva de dados é realizada sem a devida compensação para os indivíduos ou comunidades de onde esses dados são extraídos. Os benefícios econômicos dessa exploração são concentrados nas mãos das corporações tecnológicas, enquanto os custos e os riscos são externalizados para os indivíduos e as sociedades.

Essa dinâmica de extrativismo de dados reflete práticas históricas de colonialismo, onde recursos naturais eram extraídos de regiões colonizadas para o benefício econômico dos colonizadores. No colonialismo digital, os dados pessoais substituem os recursos naturais, mas as dinâmicas de poder e exploração permanecem semelhantes. Os dados são coletados e processados de maneiras que maximizam o lucro para as corporações, muitas vezes à custa da privacidade e da autonomia dos indivíduos.

A prática de coleta e monetização de dados pessoais por empresas tecnológicas globais em países africanos, como Gana e Nigéria, exemplifica o fenômeno conhecido como colonialismo digital. Conforme destacado pela Privacy International (n.d), essas empresas frequentemente utilizam dados dos cidadãos africanos para fins de publicidade direcionada e personalização de serviços, muitas vezes sem o consentimento claro dos usuários.

Essa prática levanta sérios questionamentos sobre a soberania digital, uma vez que os dados produzidos dentro desses países são explorados economicamente por corporações estrangeiras, sem que o valor gerado retorne para a economia local. Cidadãos ganeses e nigerianos, por exemplo, geram grandes volumes de dados ao usar aplicativos e serviços móveis, mas, em muitos casos, esses dados são monetizados por empresas estrangeiras sem transparência. Como consequência, países africanos perdem o potencial de desenvolver suas próprias economias digitais, ficando tecnologicamente dependentes de soluções e infraestruturas externas (Stevenson, 2024).

A Privacy International (2020) destaca que a falta de regulamentações robustas de proteção de dados em muitos países africanos permite que grandes empresas de tecnologia operem praticamente sem supervisão. Diferente da Europa, que conta com a GDPR para regulamentar e limitar o uso de dados pessoais, muitos países africanos ainda não dispõem de marcos legais que protejam os dados de seus cidadãos. Essa lacuna regulatória facilita práticas que perpetuam relações econômicas e tecnológicas desiguais, típicas do colonialismo, onde os recursos – no caso, dados pessoais – são extraídos e explorados por empresas do Norte Global.

O conceito de capitalismo de vigilância, por sua vez, dialoga diretamente com a lógica do colonialismo digital. Em seu trabalho, Zuboff (2019) define o "capitalismo de vigilância" como a prática de coleta massiva de dados pessoais por grandes corporações para prever e influenciar comportamentos futuros, transformando a vigilância em um modelo de negócios lucrativo. Zuboff (2019, p. 15) explica que "o capitalismo de vigilância monetiza a experiência humana transformando-a em dados comportamentais que podem ser vendidos e comprados, criando novas formas de poder e controle".

O capitalismo de vigilância representa uma ameaça significativa à privacidade e à autonomia individual. A coleta constante e a análise de dados pessoais permitem que as empresas construam perfis detalhados dos indivíduos, frequentemente sem o seu consentimento

explícito. Esses perfis são utilizados para prever e influenciar comportamentos, comprometendo a capacidade dos indivíduos de tomar decisões livres e informadas. Zuboff (2019, p. 15) destaca que "a vigilância constante cria um ambiente onde os indivíduos são manipulados sem seu conhecimento, comprometendo a liberdade e a dignidade humanas".

A capacidade das empresas de influenciar o comportamento individual também tem implicações significativas para a democracia. A personalização de conteúdo nas plataformas digitais limita a exposição a diferentes pontos de vista e polarizando o discurso público, conforme exposto anteriormente. Além disso, a manipulação da informação pode ser utilizada para influenciar processos eleitorais e minar a confiança nas instituições democráticas.

As práticas de colonialismo digital e capitalismo de vigilância exemplificam, portanto, em escala internacional, como as dinâmicas de poder e exploração históricas podem ser replicadas e amplificadas na era digital. Estas dinâmicas impõem desafios práticos na proteção de dados e na governança da internet.

3.1. Desafios do Colonialismo Digital para a Proteção de Dados

A era digital trouxe consigo uma série de avanços tecnológicos que revolucionaram a maneira como a sociedade opera, interage e consome informações. No entanto, essa transformação também gerou desafios significativos para a proteção dos direitos fundamentais, especialmente no contexto do colonialismo digital. O controle e a exploração de dados pessoais por grandes corporações tecnológicas criam barreiras jurídicas e tecnológicas que dificultam a defesa desses direitos.

A primeira barreira jurídica significativa é a inadequação das legislações existentes. As leis de proteção de dados, como a GDPR (General Data Protection Regulation) na Europa e a LGPD (Lei Geral de Proteção de Dados) no Brasil, foram desenvolvidas para fornecer um marco regulatório robusto para a proteção dos dados pessoais. No entanto, a rápida evolução das tecnologias digitais muitas vezes supera a capacidade dessas leis de oferecer proteção adequada. Como destaca Zuboff (2019, p. 156) em seu trabalho, a velocidade com que as tecnologias avançam frequentemente excede a capacidade das legislações de se adaptar, criando lacunas que podem ser exploradas pelas corporações tecnológicas.

A GDPR, por exemplo, estabelece princípios fundamentais de transparência e consentimento, mas a implementação prática desses princípios enfrenta desafios significativos. A complexidade dos mecanismos de consentimento e a opacidade das práticas de coleta de dados por grandes corporações dificultam a aplicação desses princípios de maneira eficaz. Na visão de Veale e Binns (2017, p. 10), a exigência de consentimento informado e explícito é muitas vezes comprometida pela falta de clareza e pela complexidade dos termos de serviço apresentados aos usuários.

Além disso, a falta de harmonização global das leis de proteção de dados cria um ambiente desigual onde corporações tecnológicas podem explorar jurisdições com regulamentações mais fracas. Enquanto a GDPR e a LGPD estabelecem padrões elevados de proteção, muitos países ainda não possuem legislações robustas ou mecanismos de aplicação eficazes. Esta disparidade permite que as corporações movam suas operações para regiões com menos regulamentação, exacerbando a exploração de dados. Nissenbaum (2011) argumenta em seu trabalho que a fragmentação das leis de proteção de dados cria uma 'terra de ninguém' regulatória onde os direitos dos indivíduos são vulneráveis à exploração.

V. 5 / N. 1 / JULHO DE 2024
PÁGINAS 148 A 167

Outro desafio jurídico é a dificuldade de responsabilizar grandes corporações tecnológicas. Empresas como Google, Facebook e Amazon possuem recursos jurídicos consideráveis e operam em várias jurisdições, complicando a aplicação das leis nacionais. A natureza transnacional da internet permite que os dados frequentemente cruzem fronteiras nacionais, escapando à jurisdição de uma única entidade reguladora. Como observam De Hert e Papakonstantinou (2016), a globalização dos fluxos de dados requer uma abordagem internacional coordenada para a regulamentação, o que muitas vezes é difícil de alcançar devido às diferenças culturais e políticas entre os países.

A resistência das corporações tecnológicas à transparência e à responsabilização também representa uma barreira significativa. Muitos algoritmos e práticas de coleta de dados são protegidos como segredos comerciais, o que impede a fiscalização e a responsabilização por violações de direitos. Citando Pasquale (2015, p. 146), "a 'caixa preta' dos algoritmos corporativos oculta os processos de tomada de decisão, dificultando a identificação e a correção de práticas discriminatórias ou invasivas".

As barreiras tecnológicas incluem a complexidade dos sistemas de coleta e processamento de dados, que são frequentemente opacos e incompreensíveis para a maioria dos usuários. A falta de transparência nos algoritmos utilizados para processar dados pessoais é uma preocupação significativa. Esses algoritmos, muitas vezes protegidos por segredos comerciais, são complexos demais para serem auditados ou compreendidos por pessoas comuns. Esta opacidade impede a responsabilização e dificulta a proteção dos direitos dos indivíduos.

A centralização das infraestruturas de dados nas mãos de poucas corporações tecnológicas representa outra barreira tecnológica crítica. Essas corporações possuem vastos recursos para desenvolver tecnologias avançadas de coleta e análise de dados, criando uma disparidade de poder tecnológico entre elas e os usuários individuais ou governos de países em desenvolvimento. Esta centralização de poder tecnológico não apenas limita a capacidade desses países de desenvolver suas próprias soluções tecnológicas e econômicas, mas também os torna dependentes das tecnologias oferecidas pelas grandes corporações. Isso perpetua uma dinâmica de dependência e subordinação, onde os países em desenvolvimento não têm autonomia para controlar suas próprias infraestruturas digitais.

A infraestrutura tecnológica centralizada permite que grandes corporações tecnológicas exerçam um controle significativo sobre os fluxos de dados globais. Essa centralização não só facilita a coleta e análise massiva de dados pessoais, mas também cria um ponto único de vulnerabilidade, onde violações de dados ou ataques cibernéticos podem ter impactos devastadores. Schneier (2015) argumente, dentre outros temas, que a centralização dos dados em grandes plataformas tecnológicas cria alvos para atores maliciosos, aumentando os riscos de segurança para os indivíduos e as sociedades.

A complexidade técnica dos sistemas de IA e aprendizado de máquina utilizados pelas corporações tecnológicas também representa uma barreira significativa para a proteção dos direitos. Esses sistemas frequentemente operam como "caixas pretas", onde os processos de tomada de decisão são opacos e difíceis de interpretar. Isso dificulta a identificação e a correção de práticas discriminatórias ou invasivas. Burrell (2016) observa em seu trabalho que a opacidade dos sistemas algorítmicos cria um 'déficit de responsabilidade', onde as decisões automatizadas que afetam profundamente a vida dos indivíduos são tomadas sem a devida transparência ou supervisão.

A falta de alfabetização digital entre os usuários também contribui para a vulnerabilidade aos abusos de dados. Muitos indivíduos não possuem o conhecimento técnico necessário para compreender as implicações das práticas

de coleta de dados ou para proteger adequadamente sua privacidade. Esta falta de compreensão impede que os usuários tomem decisões informadas sobre o uso de seus dados pessoais. Citando Selwyn (2004, p. 352), "a alfabetização digital é essencial para a participação plena na sociedade da informação, mas a lacuna de conhecimento técnico entre os usuários e as corporações tecnológicas perpetua uma dinâmica de exploração e vulnerabilidade".

Desse modo, a governança da proteção de dados na era digital enfrenta desafios significativos devido à natureza global e interconectada da internet. A criação de um quadro regulatório eficaz requer a cooperação internacional e a harmonização das leis de proteção de dados. No entanto, diferenças culturais, políticas e econômicas entre os países dificultam essa harmonização. Como observa Bennett (2011) em sua obra, a governança global da privacidade requer um equilíbrio delicado entre a soberania nacional e a necessidade de normas internacionais consistentes.

4. Políticas Públicas para Proteger Direitos na Era Digital

Diante dos desafios e barreiras impostos a partir do colonialismo digital e do capitalismo de vigilância, políticas públicas robustas são essenciais para garantir que os direitos dos cidadãos sejam protegidos contra abusos e explorações no ambiente digital. Essas políticas devem abordar a privacidade, a segurança de dados, a igualdade de acesso e a transparência.

Uma das principais áreas de foco das políticas públicas na era digital é a privacidade e a proteção de dados. Governos em todo o mundo têm implementado legislações para regular a coleta, o armazenamento e o uso de dados pessoais por empresas e entidades governamentais. A GDPR na União Europeia e a LGPD no Brasil são exemplos de tais legislações que estabelecem diretrizes claras para o tratamento de dados pessoais e garantem os direitos dos titulares dos dados. Essas leis exigem que as organizações obtenham consentimento explícito dos indivíduos antes de coletar seus dados, informando-os sobre como esses dados serão usados e armazenados. Além disso, proporcionam aos indivíduos o direito de acessar, corrigir e excluir suas informações pessoais.

Outra dimensão crítica das políticas públicas na era digital é a segurança de dados. As violações de dados e os ataques cibernéticos representam ameaças significativas à segurança nacional, à economia e aos direitos individuais. Os governos devem investir em tecnologias avançadas de segurança e promover a cooperação entre o setor público e o privado para combater ameaças cibernéticas. A criação de centros nacionais de resposta a incidentes cibernéticos (CSIRTs) e a implementação de programas de conscientização sobre segurança cibernética são exemplos de iniciativas políticas que podem fortalecer a resiliência contra-ataques cibernéticos.

As políticas públicas também devem abordar com centralidade a questão da desigualdade de acesso à tecnologia e à internet. Políticas de inclusão digital são essenciais para garantir que todos os cidadãos tenham acesso equitativo à internet e às tecnologias digitais. Essas políticas podem incluir, por exemplo, a expansão da infraestrutura de banda larga para áreas rurais e remotas, a oferta de subsídios para dispositivos tecnológicos para famílias de baixa renda e a promoção da alfabetização digital. A inclusão digital também envolve o desenvolvimento de conteúdos e serviços acessíveis a pessoas com deficiência, garantindo que todos os cidadãos possam participar plenamente da sociedade digital. Warschauer (2003) observa que a inclusão digital é fundamental para a equidade social, o

que permite que todos os indivíduos tenham acesso às oportunidades educacionais, econômicas e sociais proporcionadas pela era digital.

Por fim, a transparência e a responsabilidade são pilares fundamentais das políticas públicas na era digital. A implementação de políticas de transparência pode incluir a obrigatoriedade de relatórios de impacto sobre a privacidade, a realização de auditorias regulares de segurança de dados e a criação de mecanismos para que os cidadãos denunciem abusos ou violações de dados.

4.2. A Importância da Colaboração Internacional

A natureza global da internet e das tecnologias digitais torna a colaboração internacional essencial para a proteção dos direitos na era digital. A harmonização das leis de proteção de dados, a cooperação na aplicação da lei e a troca de informações são fundamentais para enfrentar os desafios transnacionais do colonialismo digital.

Nesse sentido, a cooperação entre as autoridades de proteção de dados e as agências de aplicação da lei de diferentes países também é essencial para combater violações de dados transnacionais. Isso pode incluir a realização de investigações conjuntas, a partilha de informações e a assistência mútua na aplicação da lei. A criação de redes internacionais de cooperação, como a Global Privacy Enforcement Network (GPEN), pode facilitar essa colaboração, bem como a troca de informações e melhores práticas entre países pode ajudar a melhorar a eficácia das políticas de proteção de dados. Isso pode incluir a organização de conferências internacionais, a publicação de relatórios conjuntos e a criação de plataformas de conhecimento compartilhado. Essas iniciativas podem ajudar os países a aprenderem uns com os outros e a adotar as melhores práticas em suas próprias jurisdições.

Por outro lado, tratados internacionais e os acordos de cooperação são instrumentos igualmente importantes para garantir a proteção dos dados em um contexto global. Esses acordos podem estabelecer normas mínimas de proteção de dados, promover a cooperação na aplicação da lei e garantir que os direitos dos indivíduos sejam respeitados em todas as jurisdições. No sentido do que observa o trabalho de Kuner (2013), cabe ressaltar que os tratados internacionais são essenciais para criar um quadro regulatório global que proteja os direitos dos indivíduos e promova a confiança no ambiente digital.

A colaboração internacional também pode incluir o desenvolvimento de capacidades e a assistência técnica para países em desenvolvimento que estão implementando e aprimorando suas leis de proteção de dados. Isso pode incluir a oferta de treinamento para reguladores, a criação de programas de intercâmbio e a provisão de suporte técnico para a implementação de tecnologias de proteção de dados. Essas iniciativas são essenciais para garantir que todos os países possam proteger os direitos de seus cidadãos na era digital.

Conclusão

A análise sobre o impacto da inteligência artificial (IA) e do colonialismo digital nas políticas públicas e na proteção dos direitos fundamentais evidencia a necessidade urgente de um reexame profundo das estruturas legais e sociais vigentes. O avanço tecnológico trouxe benefícios incontestáveis, porém, também revelou e amplificou desigualdades sociais e econômicas, exigindo uma abordagem holística para mitigar seus efeitos adversos.

O conceito de colonialismo digital nos alerta para uma nova forma de dominação e exploração, onde dados pessoais são utilizados como recursos a serem extraídos e monetizados, muitas vezes sem o consentimento adequado dos indivíduos. Essa dinâmica não apenas perpetua desigualdades históricas, mas também cria formas de controle e vigilância que ameaçam a autonomia e a liberdade dos cidadãos. A concentração de poder nas mãos de poucas corporações tecnológicas é um reflexo preocupante dessa nova era, onde o controle de informações se traduz em poder econômico e político.

A proteção de dados e a privacidade emergem como direitos fundamentais indispensáveis para a dignidade humana na era digital. A implementação de regulamentações como a Lei Geral de Proteção de Dados (LGPD) no Brasil e a General Data Protection Regulation (GDPR) na Europa são passos significativos, mas não suficientes. A eficácia dessas leis depende não apenas de sua aplicação rigorosa, mas também da capacidade das instituições de se adaptarem às rápidas mudanças tecnológicas. Além disso, a cooperação internacional é crucial para enfrentar os desafios transfronteiriços impostos pela globalização dos fluxos de dados.

A digitalização e a IA têm o potencial de melhorar o acesso à justiça e aumentar a eficiência em diversos setores, mas também apresentam riscos significativos. A automação de processos decisórios pode perpetuar preconceitos e discriminações se não for acompanhada de transparência e mecanismos de auditoria. A responsabilidade e a equidade nas decisões automatizadas são princípios que devem ser rigorosamente observados para garantir que a tecnologia sirva ao bem comum e não aos interesses de uma minoria privilegiada.

O colonialismo digital e o capitalismo de vigilância exemplificam como as dinâmicas de poder e exploração podem ser replicadas na era digital. Essas práticas representam uma ameaça não apenas à privacidade, mas também à própria estrutura democrática das sociedades. A manipulação de informações e a criação de "bolhas de filtro" nas plataformas digitais comprometem o debate público e a liberdade de expressão, pilares fundamentais de qualquer democracia saudável. Para enfrentar esses desafios, é essencial que políticas públicas sejam formuladas com base em princípios de transparência, responsabilidade e inclusão.

V. 5 / N. 1 / JULHO DE 2024
PÁGINAS 148 A 167

Notas finais

1 ?

2 "Dados pessoais referem-se a qualquer informação relacionada a uma pessoa natural identificada ou identificável. Uma pessoa natural é considerada identificável quando é possível identificar essa pessoa, direta ou indiretamente, em particular por referência a um identificador como um nome, um número de identificação, dados de localização, identificadores online, ou a um ou mais fatores específicos à identidade física, fisiológica, genética, mental, econômica, cultural ou social dessa pessoa" (MENDES; LEITE, 2019).

Referências bibliográficas

ACLU Michigan. (2020). *Man Wrongfully Arrested Because Face Recognition Can't Tell Black People Apart. American Civil Liberties Union*. https://www.aclu.org/press-releases/man-wrongfully-arrested-because-face-recognition-cant-tell-black-people-apart

ADC. (2016). *El sistema de protección de datos personales en América Latina: oportunidades y desafíos para los derechos humanos – Vol. I | Asociación por los Derechos Civiles*. Asociación Por Los Derechos Civiles. https://adc.org.ar/informes/sistema-proteccion-datos-personales-latam

Angwin, J., Larson, J., Mattu, S., & Kirchner, L. (2016). *Machine Bias*. ProPublica. https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing

Baptista Luz Advogados, da Silva, D. R. S., Silva, G. H. L., Ribeiro, N. G., Júnior, O. P., & Braoios, R. R. (2022, December). *Guia América Latina: Legislações de Proteção de Dados | A Year in Privacy #11* - Baptista Luz. Baptista Luz. https://baptistaluz.com.br/america-latina-legislacoes-de-protecao-de-dados-a-year-in-privacy-11

Bartlett, R. P., Morse, A., Stanton, R., & Wallace, N. (2019). *Consumer Lending Discrimination in the FinTech Era. SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3063448

Bioni, B. R. (2018). *Proteção de dados pessoais: a função e os limites do consentimento. Editora Forense*.

Brennen, S., & Kreiss, D. (2014, September 8). *Digitalization and Digitization – Culture Digitally. Culturedigitally.org*. https://culturedigitally.org/2014/09/digitalization-and-digitization/

Burrell, J. (2015). How the Machine "Thinks:" Understanding Opacity in Machine Learning Algorithms. *SSRN Electronic Journal*, *3(1)*. https://doi.org/10.2139/ssrn.2660674

Cassino, J. F., Souza, J., & Amadeu da Silveira, S. (Eds.). (2022). *Colonialismo de dados*. Autonomia Literária.

Couldry, N., & Mejias, U. A. (2019). The Costs of Connection: How Data Is Colonizing Human Life and Appropriating it for Capitalism. *Stanford University Press*.

Crawford, K. (2021). Atlas of AI: Power, Politics, and the Planetary Costs of Artificial Intelligence. *Yale University Press*.

de Hert, P., & Papakonstantinou, V. (2016). The new General Data Protection Regulation: Still a sound system for the protection of individuals? *Computer Law & Security Review*, 32(2), 179–194. https://doi.org/10.1016/j.clsr.2016.02.006

de Oliveira, S. R. (2021). Sorria, você está sendo filmado!: repensando direitos na era do reconhecimento facial. *Thomson Reuters, Revista Dos Tribunais*.

Douek, E. (2020). Governing Online Speech: From "Posts-As-Trumps" to Proportionality and Probability. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3679607

Eubanks, V. (2018). *Automating Inequality: how high-tech tools profile, police, and punish the poor*. St. Martin's Press.

Faustino, D., & Lippold, W. (2023). *Colonialismo digital*. Boitempo Editorial.

Greengard, S. (2021). *The internet of things*. Mit Press.

Kuner, C. (2013). *Transborder data flows and data privacy law*. Oxford University Press.

Mayer-Schönberger, V., & Cukier, K. (2013). *Big Data: a Revolution That Will Transform How We Live, Work and Think*. John Murray.

Newman, A. (2009). Bennett, Colin. 2008. The Privacy Advocates: Resisting the Spread of Surveillance. Cambridge: *MIT Press. Surveillance & Society*, 6(3), 343–344. https://doi.org/10.24908/ss.v6i3.3299

Nissenbaum, H. F. (2009). *Privacy in context: technology, policy, and the integrity of social life*. Stanford University Press.

Nunes, P. (2022). *Um Rio de olhos seletivos– uso de reconhecimento facial pela polícia fluminense*. CeSEC–Centro de Estudos de Segurança e Cidadania.

O'neil, C. (2016). *Weapons of math destruction: How big data increases inequality and threatens democracy*. Penguin Books.

Obermeyer, Z., Powers, B., Vogeli, C., & Mullainathan, S. (2019). Dissecting Racial Bias in an Algorithm Used to Manage the Health of Populations. *Science*, *366*(6464), 447–453. https://doi.org/10.1126/science.aax2342

Pariser, E. (2011). *The Filter Bubble: What the internet is hiding from you*. Penguin Press.

Pasquale, F. (2016). The Black Box Society: The Secret Algorithms That Control Money and Information. *Contemporary Sociology: A Journal of Reviews*, 45(3), 367–368. https://doi.org/10.1177/0094306116641409c

Privacy International. (n.d.). *A world without data exploitation | Privacy International*. *Privacyinternational.org*. https://privacyinternational.org/demand/a-world-without-data-exploitation

Privacy International. (2020). *2020 is a crucial year to fight for data protection in Africa*. Privacy International. https://privacyinternational.org/long-read/3390/2020-crucial-year-fight-data-protection-africa

R7. (2021, December 15). "*Disseram que eu era traficante*", *diz pedreiro preso injustamente*. Notícias R7. https://noticias.r7.com/brasilia/disseram-que-eu-era-traficante-diz-pedreiro-preso-injustamente-16122021/

Rede de Observatórios de Segurança (Ed.). (2019). Retratos da Violência: *Cinco meses de monitoramento, análises e descobertas*. Centro de Estudos de Segurança e Cidadania (CESeC).

Rodotà, S., Moraes, M. C. B. de, Doneda, D., & Doneda, L. C. (2008). *A vida na sociedade da vigilância: a privacidade hoje* (p. 381). Renovar.

Russel, S., & Norvig, P. (2021). *Artificial intelligence: A Modern approach* (4th ed.). Prentice Hall.

Schneier, B. (2015). *Data and Goliath: the hidden battles to collect your data and control your world*. WW Norton &Company.

Selwyn, N. (2004). Reconsidering Political and Popular Understandings of the Digital Divide. *New Media & Society*, *6*(3), 341–362. https://doi.org/10.1177/1461444804042519

Stevenson, T. (2024). *Navigating Digital Neocolonialism in Africa*. Centre for International Governance Innovation. https://www.cigionline.org/publications/navigating-digital-neocolonialism-in-africa/

Stokes, E., & CBS News. (2020, November 19). *Wrongful arrest exposes raciais bias in facial recognition technology*. CBS News. https://www.cbsnews.com/news/detroit-facial-recognition-surveillance-camera-racial-bias-crime/

Sunstein, C. R. (2018). #Republic : Divided Democracy In The Age Of Social Media. Princeton University Press.

Veale, M., & Binns, R. (2017). Fairer machine learning in the real world: Mitigating discrimination without collecting sensitive data. *Big Data & Society*, 4(2), 205395171774353. https://doi.org/10.1177/2053951717743530

Veloso Meireles, A. (2023). Privacidade no século 21: proteção de dados, democracia e modelos regulatórios. *Revista Brasileira de Ciência Política*, *41*. https://doi.org/10.1590/0103-3352.2023.41.265909

Veronese, A., Igreja, R. L., & Silveira, A. (2023). Cultura, privacidade e proteção de dados pessoais na América Latina. *Revista de Estudos Empíricos Em Direito*, 10, 1–44. https://doi.org/10.19092/reed.v10.766

Warren, S. D., & Brandeis, L. D. (1890). The Right to Privacy. *Harvard Law Review*, 4(5), 193–220. https://doi.org/10.2307/1321160

Warschauer, M. (2002). *Technology and social inclusion: Rethinking the digital divide*. MIT Press.

Wu, T. (2017). *The attention merchants: from the daily newspaper to social media, how our time and attention is harvested and sold*. London Atlantic Books.

Yeung, K. (2017). Algorithmic regulation: A critical interrogation. *Regulation & Governance*, *12*(4), 505–523. https://doi.org/10.1111/rego.12158

Zuboff, S. (2019). *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. Public Affairs.