CAPÍTULO 13

ENTRE DADOS E DIREITOS: A DISCRIMINAÇÃO ALGORÍTMICA SOB A PERSPECTIVA DA LGPD- LEI GERAL DE PROTEÇÃO DE DADOS

https://doi.org/10.22533/at.ed.9751325050513

Data de aceite: 03/07/2025

Lilian Rodrigues
Mestranda em Direito pela Fundação Escola Superior do Ministério Público-RS.

Raquel Sparemberger
Doutora em Direito. Professora dos Cursos de Graduação e Mestrado em Direito da Fundação Escola Superior do Ministério Público-RS e da FURG-RS. Professora Pesquisadora

RESUMO: Este trabalho tem como objetivo, por meio do método de abordagem indutiva, da análise de conteúdo e da pesquisa bibliográfica, identificar e analisar as disposições da Lei Geral de Proteção de Dados (LGPD) que asseguram a proteção dos dados pessoais dos cidadãos brasileiros. A partir desse referencial, o artigo busca conceituar algoritmos, Big Data, aprendizado de máquina, inteligência artificial e discriminação algorítmica, além de apresentar os tipos de discriminação algorítmica segundo a classificação adotada pela doutrina brasileira. Com base nessa análise, pretende-se esclarecer de que forma a discriminação algorítmica se manifesta no contexto atual.

PALAVRAS-CHAVE: Lei Geral de Proteção de Dados. Algoritmos. Big Data. Aprendizado de Máquina. Inteligência Artificial. Discriminação Algorítmica.

BETWEEN DATA AND RIGHTS: ALGORITHMIC DISCRIMINATION FROM THE PERSPECTIVE OF THE LGPD - GENERAL DATA PROTECTION LAW

ABSTRACT: This work aims, through the inductive approach method, content analysis, and bibliographic research technique, to identify and analyze the provisions in the General Data Protection Law that protect the personal data of Brazilian citizens. Based on this understanding, the paper seeks to explain the concepts of algorithms, Big Data, Machine Learning, Artificial Intelligence, and Algorithmic Discrimination, as well as the types of algorithmic discrimination according to Brazilian doctrinal classification. Based on these findings, the paper aims to clarify how algorithmic discrimination occurs.

KEYWORDS: General Data Protection Law. Algorithm. Big Data. Machine Learning. Artificial Intelligence. Algorithmic Discrimination.

INTRODUÇÃO

O presente trabalho tem como objetivo compreender o fenômeno da discriminação algorítmica, a partir da crescente centralidade da internet nas relações humanas, especialmente intensificada durante a pandemia da COVID-19. Nesse contexto, o uso massivo de plataformas digitais resultou em um grande volume de dados pessoais compartilhados pelos usuários. Um caso emblemático que evidenciou os riscos associados ao uso indevido desses dados foi o escândalo da Cambridge Analytica, durante as eleições presidenciais dos Estados Unidos em 2016, o que impulsionou debates globais sobre a proteção de dados e a necessidade de regulamentação.

Como resposta, a União Europeia instituiu o GDPR e, no Brasil, foi sancionada em 2018 a Lei Geral de Proteção de Dados (LGPD), com inspiração na legislação europeia. O artigo utiliza abordagem indutiva, análise de conteúdo e pesquisa bibliográfica para identificar os dispositivos da LGPD que protegem os dados pessoais dos brasileiros. Além disso, busca esclarecer os conceitos de algoritmo, Big Data, Machine Learning, Inteligência Artificial e Discriminação Algorítmica, e promover uma reflexão crítica sobre como essa discriminação pode se manifestar na sociedade contemporânea.

O objetivo do presente trabalho é compreender o fenômeno denominado discriminação algorítmica. Para alcançar tal compreensão, é necessário lembrar que tudo começa na maior plataforma de relacionamento humano: a internet. É nela que o indivíduo realiza atividades como compras, estudos e relacionamentos afetivos.

A metodologia privilegia o método de abordagem hipotético-dedutivo, pesquisa qualitativa, do tipo exploratória e descritiva. A técnica de pesquisa é essencialmente bibliográfica.

A CENTRALIDADE DOS DADOS NA SOCIEDADE DIGITAL: ENTRE CONEXÕES, RISCOS E DIREITOS

A internet alcançou um novo patamar de centralidade social durante a pandemia de COVID-19. As medidas de isolamento social impulsionaram a digitalização acelerada da vida cotidiana, forçando os cidadãos a fornecerem massivamente seus dados pessoais a plataformas digitais como Google Meet, Zoom, Instagram, YouTube e Facebook. Esse processo gerou um aumento expressivo no volume de dados cadastrados na rede mundial de computadores (Leal; Paulo, 2023, p. 4; Doneda, 2021; Monteiro, 2020).

O debate sobre a proteção de dados pessoais ganhou notoriedade internacional a partir de episódios como o escândalo da *Cambridge Analytica*. Durante as eleições norte-americanas de 2016, a campanha de Donald Trump contratou uma empresa britânica de análise de dados com o objetivo de influenciar eleitores indecisos por meio de técnicas de *micromarketing* e *microtargeting*. Utilizando informações obtidas de redes sociais como o Facebook, perfis comportamentais foram criados e utilizados para disseminar conteúdos

personalizados que buscavam persuadir determinados grupos ou desestimular o voto de opositores. O episódio, amplamente discutido no documentário *The Great Hack* (Netflix), demonstrou o poder da manipulação algorítmica e a fragilidade dos mecanismos de controle sobre o uso de dados pessoais (Leal; Paulo, 2023, p. 5; Zuboff, 2020; Cadwalladr; Graham-Harrison, 2018).

Em resposta a essas preocupações, a União Europeia promulgou, em 2016, o *General Data Protection Regulation* (GDPR), marco normativo que inspirou diversas legislações ao redor do mundo. No Brasil, a Lei Geral de Proteção de Dados (LGPD) foi sancionada em 2018 e entrou plenamente em vigor em agosto de 2021. Antes disso, a proteção de dados era regulada de maneira fragmentada, por meio de dispositivos do Código de Defesa do Consumidor, da Lei do Habeas Data, da Lei do Cadastro Positivo, da Lei de Acesso à Informação, da Lei Carolina Dieckmann e do Marco Civil da Internet (Leal, 2023, p. 6; Doneda, 2014; Monteiro, 2020).

A Constituição Federal de 1988 já assegurava, em seu artigo 5º, direitos fundamentais como a liberdade individual, a inviolabilidade da intimidade e da vida privada (inciso X), bem como o livre desenvolvimento da personalidade e a autodeterminação informativa (inciso XII). No entanto, foi somente com a Emenda Constitucional nº 115/2022 que o direito à proteção de dados pessoais ganhou status constitucional expresso, sendo incluído no artigo 5º, inciso LXXIX, e reconhecido como competência privativa da União (arts. 21, XXVI, e 22, XXX).

A LGPD estabelece normas para o tratamento de dados pessoais por pessoas físicas ou jurídicas, de direito público ou privado, com o objetivo de assegurar os direitos fundamentais à liberdade, à privacidade e ao livre desenvolvimento da personalidade. Entre suas diretrizes, destacam-se o consentimento do titular, a transparência, a responsabilização em casos de vazamento, a vedação a práticas discriminatórias e a possibilidade de revisão de decisões automatizadas (Leal; Paulo, 2023, p. 9; Doneda, 2021; Monteiro, 2020).

O artigo 2º da LGPD destaca como fundamentos da lei a dignidade da pessoa humana, os direitos humanos e a cidadania. O artigo 6º apresenta os princípios norteadores do tratamento de dados, incluindo a finalidade específica, a necessidade, a transparência, a segurança e a não discriminação. Já o artigo 20 assegura ao titular o direito de solicitar revisão de decisões automatizadas, incluindo aquelas que definem perfis de crédito, consumo ou comportamento.

Apesar da ausência, até o momento, de uma legislação específica sobre inteligência artificial no Brasil, a LGPD já impacta diretamente o uso dessas tecnologias, impondo limites ao tratamento automatizado de dados. A responsabilidade pela conformidade com a lei não se limita ao setor de tecnologia, mas envolve toda a estrutura organizacional das entidades que tratam dados. Além disso, práticas como a *profiling* discriminatória — como a restrição de crédito com base em características inferidas e não declaradas — são vedadas (Leal; Paulo, 2023, p. 16).

O artigo 11, §5º, da LGPD, proíbe planos de saúde de utilizarem dados pessoais sensíveis para estabelecer riscos de contratação ou exclusão de usuários, estendendo essa proibição a bancos de dados que realizem análise de risco com base em *profiling*. O princípio da *accountability*, previsto na legislação, exige que o agente de tratamento demonstre, de forma ativa, a adoção de medidas eficazes de conformidade e segurança, inclusive diante de auditorias conduzidas pela Autoridade Nacional de Proteção de Dados (ANPD).

Por fim, é necessário ponderar o direito à proteção de dados pessoais em relação a outros direitos e interesses públicos, como o acesso à informação em questões de saúde ou processos judiciais. A LGPD contempla hipóteses de relativização do sigilo, desde que orientadas pelo interesse público e em conformidade com os artigos 4º, §1º; 7º, §3º; 15, III; e 23 da lei.

CONCEITO DE ALGORITMO

Os algoritmos são conjuntos estruturados de regras ou instruções codificadas, projetadas para resolver problemas ou executar tarefas específicas a partir do processamento de dados. Conforme destaca Pedro Mendes e Marina Mattiuzzo (2019), sua aplicação no contexto digital visa embasar a tomada de decisões e reduzir riscos, especialmente em setores como seguros, recursos humanos, segurança pública e concessão de crédito, onde decisões baseadas em previsões se tornam cada vez mais comuns.

No campo da ciência de dados, algoritmos operam com base na lógica estatística e matemática para processar grandes volumes de informações — os chamados *big data* — e, a partir disso, gerar inferências, padrões e previsões. A análise desses dados resulta na geração de *scores* e perfis comportamentais, os quais podem indicar, por exemplo, a probabilidade de inadimplência de um consumidor ou a adequação de um candidato a uma vaga de emprego.

Catherine D'Ignazio e Lauren Klein (2020), em *Data Feminism*, chamam atenção para o fato de que algoritmos não são neutros: eles refletem as decisões humanas embutidas em sua programação — escolhas sobre quais dados incluir, quais métricas priorizar e quais resultados considerar válidos. Assim, o algoritmo é sempre uma construção social mediada por interesses, valores e desigualdades preexistentes.

Conforme destaca Frank Pasquale (2015), em *The Black Box Society*, algoritmos complexos — especialmente aqueles utilizados em sistemas de recomendação, segurança preditiva e análise de crédito — funcionam como "caixas-pretas", nas quais o processo decisório é opaco tanto para o público quanto para os próprios reguladores. Essa falta de transparência compromete a accountability e levanta sérias preocupações sobre discriminação algorítmica e violação de direitos fundamentais.

No âmbito da proteção de dados pessoais, os algoritmos são amplamente utilizados para realizar a *perfilização* (*profiling*), ou seja, a categorização de indivíduos com base em características extraídas de seus comportamentos online, preferências, histórico de consumo, localização, entre outros. Como observa Oscar Vilhena Vieira (2021), essa prática pode ser particularmente perigosa quando resulta em decisões automatizadas que afetam significativamente os titulares dos dados — como negar crédito, filtrar currículos ou orientar o policiamento preventivo.

Além disso, Luciano Floridi e Josh Cowls (2019) alertam para os riscos éticos associados ao uso intensivo de algoritmos, especialmente no que diz respeito à autonomia dos indivíduos e à justiça social. Segundo os autores, é preciso estabelecer critérios normativos robustos que assegurem a explicabilidade, a equidade e a contestabilidade das decisões automatizadas.

Portanto, embora os algoritmos sejam ferramentas essenciais à era digital e à inteligência artificial, sua utilização em processos decisórios exige mecanismos de controle e regulação que garantam a transparência, a não discriminação e a proteção dos direitos fundamentais dos cidadãos.

BIG DATA, MACHINE LEARNING E INTELIGÊNCIA ARTIFICIAL: FUNDAMENTOS TÉCNICOS E IMPLICAÇÕES NA DISCRIMINAÇÃO ALGORÍTMICA

A compreensão adequada da discriminação algorítmica demanda, como ponto de partida, o domínio de três conceitos centrais no ecossistema digital contemporâneo: Big Data, Machine Learning e Inteligência Artificial (IA). Esses elementos compõem a base técnica sobre a qual se estruturam os sistemas automatizados de tomada de decisão que permeiam cada vez mais a vida social.

Big Data refere-se ao conjunto massivo de dados gerados continuamente por indivíduos, dispositivos e aplicações em rede. Sua caracterização é comumente descrita pelos chamados *5 Vs*: volume (a escala dos dados), velocidade (a rapidez com que são gerados e processados), variedade (diversidade de formatos e fontes), veracidade (qualidade e confiabilidade dos dados) e valor (potencial informativo e estratégico). A coleta e análise desses dados permite a identificação de padrões comportamentais, a formulação de previsões e a modelagem de perfis — práticas que são centrais ao funcionamento dos sistemas algorítmicos modernos (Mayer-Schönberger & Cukier, 2013).

Machine Learning (ou Aprendizado de Máquina) é um subcampo da IA que se baseia em algoritmos capazes de aprender com os dados, sem a necessidade de programação explícita para cada cenário. Como explica Russell e Norvig (2020), trata-se de sistemas que ajustam suas ações com base em experiências anteriores, aprimorando sua capacidade de previsão e classificação à medida que são alimentados com novos dados. Em contextos práticos, esses algoritmos podem ser usados para aprovar ou negar crédito, detectar fraudes, recomendar produtos e muito mais — frequentemente de forma autônoma.

Já a Inteligência Artificial, em sentido amplo, refere-se ao desenvolvimento de sistemas computacionais capazes de executar tarefas que tradicionalmente requereriam cognição humana, como reconhecimento de padrões visuais, linguagem natural, resolução de problemas e raciocínio lógico. A IA integra diferentes técnicas — como redes neurais, deep learning e processamento de linguagem natural — para simular capacidades humanas de percepção, aprendizagem e decisão (Floridi, 2014).

Essas tecnologias, quando aplicadas em larga escala, permitem um monitoramento e intervenção altamente precisos sobre indivíduos e grupos sociais. No entanto, como alertam autores como Zuboff (2020) e Eubanks (2018), sua implementação não está isenta de riscos. A opacidade dos modelos algorítmicos, a reprodução de vieses históricos e a ausência de mecanismos de prestação de contas podem conduzir a práticas discriminatórias automatizadas, especialmente quando algoritmos são utilizados em setores sensíveis como segurança pública, saúde, educação e finanças.

Nesse sentido, a interrelação entre Big Data, machine learning e IA forma o pano de fundo técnico e sociopolítico sobre o qual se assentam os debates atuais em torno da justiça algorítmica, da governança de dados e da proteção de direitos fundamentais em sociedades digitalizadas.

DISCRIMINAÇÃO ALGORÍTMICA: CONCEITO E FORMAS

A discriminação algorítmica ocorre quando decisões automatizadas, tomadas com base em algoritmos, resultam em tratamento desigual, injusto ou excludente de determinados indivíduos ou grupos sociais. Tais decisões são produzidas a partir da análise de grandes volumes de dados (Big Data), processados por sistemas de *machine learning* e inteligência artificial. Ainda que esses sistemas se apresentem como neutros ou objetivos, os dados utilizados e as escolhas de modelagem carregam valores, pressupostos e, muitas vezes, vieses sociais, históricos e culturais.

Segundo a literatura especializada no âmbito nacional, a **discriminação algorítmica** pode ser classificada em diferentes modalidades, a depender do modo como os vieses são incorporados aos sistemas automatizados de tomada de decisão. Conforme categorizam Leal e Paulo (2023), destacam-se as seguintes formas principais:

A **Discriminação direta** caracteriza-se pela utilização explícita de **dados sensíveis** — como raça, gênero, religião, deficiência, orientação sexual ou identidade de gênero — como parâmetros na modelagem ou no funcionamento do algoritmo. Essa forma de discriminação é juridicamente mais evidente, pois decorre da inserção deliberada de atributos protegidos como critérios de decisão. Um exemplo paradigmático é o de sistemas automatizados de recrutamento que rejeitam candidaturas com base em filtros associados a características étnico-raciais. (Leal, Paulo, 2023).

Um exemplo da chamada discriminação direta é o que, por exemplo, apresenta um sistema de triagem de currículos foi treinado com dados históricos de contratações de uma empresa majoritariamente masculina. O algoritmo aprendeu a penalizar currículos que incluíam termos associados a mulheres, como “capitã do time feminino” ou “presidente do clube de alunas”. A Amazon abandonou um projeto semelhante após detectar esse viés em 2018. (Jeffrey, 2018).

Segundo os autores, a chamada **Discriminação indireta** Decorre da aplicação de variáveis aparentemente neutras que, na prática, funcionam como **substitutos funcionais** (*proxies*) de dados sensíveis, resultando em impactos desproporcionais sobre determinados grupos. Trata-se de uma discriminação estrutural, muitas vezes invisibilizada, mas que gera efeitos excludentes sistemáticos. Um exemplo recorrente é o uso do código postal (CEP) na análise de crédito, que pode servir como marcador indireto de raça ou classe social, penalizando indivíduos residentes em áreas historicamente marginalizadas.(Leal, Paulo, 2023). Exemplo interessante, nesse caso são os Sistemas de análise de crédito nos EUA utilizaram **ZIP codes** (códigos postais) como critério relevante. Em muitos casos, regiões predominantemente negras ou latinas receberam pontuações de risco mais altas, embora o critério utilizado fosse geográfico e não racial. (O’neil, 2019).

Temos ainda a chamada **Discriminação por proxy** Essa modalidade refere-se à utilização de atributos não sensíveis que possuem **alta correlação estatística** com características protegidas, permitindo inferências automáticas sobre tais atributos. Trata-se de uma subcategoria da discriminação indireta, porém mais sofisticada, pois o viés emerge da arquitetura estatística do modelo, sem que haja intenção discriminatória direta. A proxy discrimination evidencia a dificuldade de neutralizar preconceitos quando estão embutidos nos próprios dados de treinamento. (Barocas; Selbst, 2016, p. 691). Exemplo a ser demonstrado são as Plataformas de anúncios do Facebook que permitiam segmentar anúncios de emprego e habitação com base em interesses ou comportamentos correlacionados a raça ou gênero, mesmo sem esses dados sendo explicitamente utilizados. Isso foi investigado pelo Departamento de Habitação dos EUA por possíveis violações à Fair Housing Act. (Kang, 2019).

Temos ainda a **Discriminação por exclusão (ou Omissão de Representatividade).** Ocorre quando determinados grupos sociais estão **sub-representados ou ausentes** nos conjuntos de dados utilizados para treinar os algoritmos, resultando em modelos com baixa acurácia ou vieses de generalização. Essa exclusão compromete a eficácia do sistema no tratamento equitativo de indivíduos pertencentes a essas populações, especialmente no caso de pessoas negras, indígenas, LGBTQIA+ ou com deficiência, cujos dados frequentemente não compõem os repositórios utilizados. (**Silva, Doneda, Monteiro, Alves, 2021).** Um bom exemplo são os Sistemas de reconhecimento facial testados em contextos de segurança pública apresentaram acurácia significativamente menor ao identificar rostos de pessoas negras e asiáticas, comparados a rostos brancos. Estudo de Buolamwini e

Gebru (2018) mostrou taxas de erro de até 34,7% para mulheres negras, contra 0,8% para homens brancos. (Buolameini; Gebru, 2018)

Por fim, ainda é possível trazer a chamada **Discriminação por retroalimentação (Feedback Loop), que se manifesta quando padrões históricos de exclusão e desigualdade** são internalizados e replicados pelo algoritmo, perpetuando ciclos de marginalização. Nesse modelo, decisões tomadas com base em dados enviesados geram novos dados que reforçam o viés original. Um exemplo típico é o uso de registros policiais para determinar áreas de patrulhamento, o que leva à intensificação da presença policial em bairros estigmatizados e à produção de novos dados de criminalidade, mesmo que esses não reflitam a realidade objetiva da violência urbana. (O'Neil, 2016, p. 83). Exemplo, os chamados sistemas de policiamento preditivo, como o *PredPol* nos EUA, usavam registros de prisões anteriores para prever onde ocorreria o próximo crime. Áreas já mais patrulhadas — muitas vezes bairros pobres e racializados — passaram a ser ainda mais vigiadas, gerando mais prisões e perpetuando o ciclo. (O'Neil, 2016, p. 83)

É importante frisar que tais formas de discriminação podem ocorrer de maneira não intencional, o que dificulta sua identificação e responsabilização. A opacidade dos sistemas algorítmicos (a chamada *black box*) agrava esse problema, pois impede que o titular de dados compreenda os critérios e lógicas utilizadas na tomada de decisões automatizadas que o afetam diretamente.

A discriminação algorítmica, portanto, constitui uma nova fronteira de desafios para o Direito, exigindo respostas normativas, regulatórias e técnicas que garantam o respeito aos direitos fundamentais, especialmente o direito à igualdade, à privacidade e à não discriminação.

CONSIDERAÇÕES FINAIS

A presente pesquisa buscou compreender o fenômeno da discriminação algorítmica à luz da Lei Geral de Proteção de Dados Pessoais (LGPD), identificando os dispositivos legais que visam tutelar os direitos fundamentais frente ao uso crescente de tecnologias baseadas em algoritmos, Big Data e inteligência artificial.

Verificou-se que, embora a LGPD não trate de forma específica e exaustiva da discriminação algorítmica, ela oferece fundamentos normativos relevantes que possibilitam o controle social, a responsabilização e a revisão de decisões automatizadas que afetem negativamente os indivíduos. Destacam-se, nesse sentido, os princípios da finalidade, da transparência, da não discriminação, da segurança e da responsabilização (accountability), bem como os direitos conferidos aos titulares de dados, especialmente o direito à revisão de decisões automatizadas (art. 20 da LGPD).

Compreender os conceitos de algoritmo, machine learning, inteligência artificial e suas implicações no tratamento de dados é essencial para identificar práticas discriminatórias

veladas e mitigar os riscos decorrentes da opacidade dos sistemas automatizados. A partir da classificação doutrinária das formas de discriminação algorítmica, torna-se evidente que tais práticas não são meramente técnicas, mas carregam profundas consequências sociais, jurídicas e éticas, especialmente em contextos como concessão de crédito, contratação, policiamento preditivo e acesso a serviços públicos.

Conclui-se que a LGPD representa um avanço importante no ordenamento jurídico brasileiro, mas não é suficiente, por si só, para enfrentar todos os desafios impostos pela discriminação algorítmica. Faz-se necessária uma atuação coordenada entre os setores públicos e privado, a Autoridade Nacional de Proteção de Dados (ANPD), o Poder Judiciário e a sociedade civil para garantir um ambiente digital mais justo, transparente e inclusivo, que respeite a dignidade da pessoa humana e os valores democráticos.

A construção de uma governança algorítmica ética e inclusiva passa, portanto, pela adoção de critérios de justiça algorítmica, pelo desenvolvimento de tecnologias explicáveis (explainable AI) e pela efetiva aplicação dos direitos previstos na LGPD. Somente assim será possível garantir que a inteligência artificial sirva ao ser humano — e não o contrário.

REFERÊNCIAS

BAROCAS, Solon; SELBST, Andrew D. Big Data's Disparate Impact. California Law Review, v. 104, 2016.

BUOLAMWINI, Joy; GEBRU, Timnit. Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification. In: Proceedings of the Conference on Fairness, Accountability and Transparency (FAT*), 2018.

CADWALLADR, Carole; GRAHAM-HARRISON, Emma. "Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach." The Guardian, 2018.

DASTIN, Jeffrey. Amazon scraps secret AI recruiting tool that showed bias against women. Reuters, 10 out. 2018. Disponível em: https://www.reuters.com/article/us-amazon-com-jobs-automation-insight-idUSKCN1MK08G. Acesso: 15 de junho 2015.

D'IGNANZIO, Catherine; KLEIN, Lauren. Data Feminism. Cambridge, Massachusetts: MIT Press, 2020.

DONEDA, Danilo. Da privacidade à proteção de dados pessoais: elementos da formação da legislação brasileira. Rio de Janeiro: Forense, 2021.

EUBANKS, Virginia. *Automating Inequality: How High-Tech Tools Profile, Police, and Punish the Poor*. St. Martin's Press, 2018.

FLORIDI, Luciano. *The Ethics of Information*. Oxford University Press, 2014.

KANG, Cecilia. Facebook Engages in Housing Discrimination With Its Ad Practices, U.S. Says. The New York Times, 28 mar. 2019. https://www.nytimes.com/2019/03/28/us/politics/facebook-housingdiscrimination.html. Acesso: 15 de junho 2015.

LEAL, M.C. Hennig; PAULO, L. M. Algorítmos discriminatórios e jurisdição constitucional: os riscos jurídicos e sociais do impacto dos vieses nas plataformas de inteligência artificial de amplo acesso**.** Revista De Direitos E Garantias Fundamentais, 24(3), 165–187. 2023

LEAL, Mônia Clarissa Hennig; PAULO, Lucas Moreschi. A Lei Geral de Proteção de Dados, a vulnerabilidade dos usuários da internet e a tutela dos direitos: linhas introdutórias à dinâmica dos dados, do Big Data, da economia de dados e da discriminação algorítmica. Civilistica.com. Rio de Janeiro, a. 12, n. 3, 2023.

MAYER-SCHÖNBERGER, Viktor; CUKIER, Kenneth. *Big Data: A Revolution That Will Transform How We Live, Work, and Think*. Eamon Dolan/Houghton Mifflin Harcourt, 2013.

MENDES, Pedro; MATTIUZZO, Marina. ***Privacidade, proteção de dados e o uso de algoritmos****: riscos e perspectivas*. São Paulo: Revista dos Tribunais, 2019.

O'NEIL, Cathy. Algoritmos de destruição em massa: como o big data aumenta a desigualdade e ameaça a democracia. Tradução de Léa Arena. São Paulo: Editora Valentina, 2019.

PASQUALE, Frank. The Black Box Society: The Secret Algorithms That Control Money and Information. Cambridge, Massachusetts: Harvard University Press, 2015.

RUSSELL, Stuart; NORVIG, Peter. *Artificial Intelligence: A Modern Approach*. 4ª ed. Pearson, 2020.

SILVA, Ronaldo Lemos; DONEDA, Danilo; MONTEIRO, Fabrício da Mota Alves. Proteção de Dados Pessoais: A Função e os Limites do Consentimento. 1. ed. Rio de Janeiro: Forense, 2021.

VIEIRA, Oscar Vilhena. ***Direitos Fundamentais e Justiça***. São Paulo: Malheiros, 2021.

ZUBOFF, Shoshana. A era do capitalismo de vigilância: A luta por um futuro humano na nova fronteira do poder. Rio de Janeiro: Intrínseca, 2020.