Revista Direitos Humanos e Democracia

Editora Unijuí • ISSN 2317-5389 • Ano 13 • nº 26 • Jul./Dez. 2025 • e16272

Programa de Pós-Graduação *Stricto Sensu* em Direito da Unijuí
https://www.revistas.unijui.edu.br/index.php/direitoshumanosedemocracia

http://dx.doi.org/10.21527/2317-5389.2025.26.16272

PROTEÇÃO DE DADOS E GRUPOS VULNERÁVEIS NO BRASIL:
O Mundo Digital Como Reflexo do Mundo Real

Elder Maia Goltzman
Universidade Presbiteriana Mackenzie. São Paulo/SP, Brasil.
https://orcid.org/0000-0002-7503-8092

Juliana Abrusio Florencio
Universidade Presbiteriana Mackenzie. São Paulo/SP, Brasil.
https://orcid.org/0000-0002-3745-0748

Juliana Santos Garcia
Universidade Presbiteriana Mackenzie. São Paulo/SP, Brasil.
https://orcid.org/0009-0008-0730-4476

RESUMO

Este artigo tem como problema de pesquisa investigar se a utilização de dados pessoais pode prejudicar grupos socialmente vulneráveis no Brasil. A hipótese sustentada é a de que os dados coletados podem reforçar desequilíbrios sociais existentes no país e aumentar o controle sobre pessoas em situação de vulnerabilidade. O texto objetiva analisar, de forma breve, a trajetória legislativa acerca do tema da proteção e armazenamento de dados à luz da teoria do capitalismo de vigilância (Zuboff, 2019), tanto em âmbito internacional quanto em relação aos avanços legislativos brasileiros, para, logo em seguida, relacionar a vulnerabilidade social, no Brasil, com a necessidade de proteção de dados pessoais. O texto foi estruturado em duas subseções que correspondem aos seus objetivos. Trata-se de pesquisa que utiliza o método indutivo e apresenta caráter exploratório, ancorada em legislação e bibliografia nacional e internacional. Também foram utilizados dados do IBGE e do Atlas de Violência de 2024.

Palavras-chave: grupos vulneráveis; proteção de dados; dados pessoais; vulnerabilidade social.

**DATA PROTECTION AND VULNERABLE GROUPS IN BRAZIL:
THE DIGITAL WORLD AS A REFLECTION OF THE REAL WORLD**

ABSTRACT

This article's research problem is to investigate whether the use of personal data can harm socially vulnerable groups in Brazil. The hypothesis is that the data collected can reinforce existing social imbalances in the country and increase control over people in vulnerable situations. The text aims to briefly analyze the legislative trajectory on the topic of data protection and storage, in light of the theory of surveillance capitalism (Zuboff, 2019), both at the international level and in relation to Brazilian legislative advances, and then relate social vulnerability in Brazil to the need for personal data protection. The text was structured into two subsections that correspond to its objectives. This research uses the inductive method and is exploratory in nature, anchored in national and international legislation and bibliography. Data from the IBGE and the 2024 Violence Atlas were also used.

Keywords: vulnerable groups; data protection; personal data; social vulnerability.

Submetido em: 11/8/2024
Aceito em: 15/5/2025
Publicado em: 11/8/2025

1 INTRODUÇÃO

A Lei Geral de Proteção de Dados (LGPD), Lei nº 13.709/2018 , representa um marco regulatório crucial na proteção dos dados pessoais no Brasil, estabelecendo direitos e deveres para titulares de dados e agentes de tratamento. Inspirada na *General Data Protection Regulation* (GDPR) da União Europeia, a LGPD surge em um contexto de crescente digitalização, quando a coleta e o processamento de dados se tornaram elementos centrais das atividades econômicas, sociais e políticas.

Nesse cenário, a proteção de dados pessoais transcende a simples privacidade, assumindo um papel fundamental na promoção de direitos fundamentais, especialmente para grupos vulneráveis, os quais incluem crianças e adolescentes, idosos, pessoas com deficiência, população LGBTQIAPN+, pessoas negras, minorias étnicas e indivíduos em situação de rua, que, frequentemente, encontram-se em maior fragilidade social e risco de discriminação e exclusão. A LGPD, ao estabelecer diretrizes específicas para o tratamento de dados sensíveis e exigir medidas adicionais de proteção, também busca assegurar que esses indivíduos possam usufruir de um ambiente digital seguro e inclusivo.

Conforme Elida Séguin (2022), tais grupos sofrem processos discriminatórios e são objetos de intolerância, sendo possível perceber que tanto os minoritários quanto os vulneráveis possuem características comuns relacionados, inclusive, a ter seus direitos fundamentais violados, embora não estabeleçam obrigatoriamente relação de proximidade de outras ordens. Neste ponto, embora haja alguma discussão acadêmica sobre os conceitos “grupos vulneráveis” e “minorias” (Siqueira; Castro, 2017), esta pesquisa adota a terminologia “grupos vulneráveis” pelas razões epistemológicas colocadas no desenvolvimento do trabalho.

O texto propõe-se a analisar, de forma crítica, a necessidade da proteção dos dados pessoais, principalmente em relação aos grupos vulneráveis. Traz luz, inicialmente, para a linha do tempo quanto às inovações legislativas sobre o tema em âmbitos internacional e nacional e destaca, ainda, os desafios e as oportunidades que surgem a partir da criação dessas leis. Em seguida, enfrenta o problema de pesquisa, que é se a utilização de dados pessoais pode prejudicar grupos socialmente vulneráveis. A hipótese sustentada é a de que os dados coletados podem reforçar desequilíbrios sociais existentes e aumentar o controle sobre pessoas em situação de vulnerabilidade.

A pesquisa foi efetuada a partir do método indutivo e adotou como técnicas principais a bibliográfica e a documental, especialmente normas (nacionais e internacionais) e produção literária da área de direito digital.

Ao abordar esses aspectos, este artigo pretende contribuir para o debate acadêmico e fornecer *insights* valiosos para legisladores, formuladores de políticas públicas e profissionais envolvidos na proteção, armazenamento de dados e na defesa dos direitos de grupos vulneráveis. A análise será pautada por uma abordagem multidisciplinar, integrando perspectivas jurídicas, tecnológicas e sociais, com o objetivo de oferecer uma compreensão abrangente e crítica do papel da LGPD na proteção de dados pessoais e na promoção da inclusão digital.

2 SOBRE A NECESSIDADE DE REGULAMENTAR A PROTEÇÃO DE DADOS PESSOAIS

Ante a globalização, a privacidade e a proteção de dados passaram a ser uma das principais prioridades para diversas nações que vislumbraram a importância de garantir a proteção de informação e dados pessoais, sobretudo em relação ao seu armazenamento. Diante de um modelo de negócios em que as informações pessoais são cedidas de forma voluntária por meio de contratos de adesão a serviços gratuitos, o setor de tecnologia consolidou-se; isso sem falar em dados raspados ou obtidos sem consentimento de seus titulares por vazamentos ou compras no mercado ilegal (Meireles, 2023).

Se antes a noção de privacidade era a noção do direito de "ser deixado em paz" (liberdade negativa), atualmente passa a ser compreendida como o espaço de intimidade e autonomia, essencial para o desenvolvimento da própria identidade e personalidade. Em outros termos, a liberdade, que antes era exercida em público, tem se deslocado para a esfera privada. O mercado de dados pessoais explora essa transformação, capitalizando as experiências privadas (Meireles, 2023).

Os algoritmos que permeiam as tecnologias digitais influenciam diversos aspectos da vida social, baseando-se na teoria do capitalismo de vigilância proposta pela professora Shoshana Zuboff (2019). Essa teoria destaca como o uso de dados pessoais ameaça as democracias liberais não só ao impactar os processos políticos e eleitorais, mas também ao transformar as expectativas privadas em fontes de lucro e vantagem para grandes empresas de tecnologia (Meireles, 2023).

Zuboff (2019) alerta para a existência de uma nova ordem econômica mundial que utiliza a experiência humana nas redes para finalidades comerciais ocultas, tais como extração de dados, previsão de comportamentos e vendas de produtos. Ressalta-se que a experiência humana é obtida gratuita e voluntariamente na medida em que cada um dos usuários das plataformas, sem qualquer objeção, passa horas de seu dia utilizando os aplicativos e interagindo com pessoas ao redor do mundo.

O capitalismo de vigilância fortaleceu-se silenciosamente no setor de tecnologia, de modo que o monitoramento constante e automatizado das experiências individuais faz com que a proteção de dados pessoais se transforme em uma questão coletiva, tornando-se objeto de normas jurídicas. É exatamente por isso, inclusive, que o mercado de dados se tornou uma preocupação de toda a sociedade para as democracias contemporâneas (Meireles, 2023).

O agigantamento das empresas de tecnologia é um elemento a ser observado pelos Estados diante da ausência de transparência na utilização dos algoritmos que, a partir da coleta de dados dos usuários, fazem priorização de ou recomendação de conteúdos, o que inclui não apenas produtos ou serviços, mas ideologias políticas. Em última medida, países inteiros podem estar sendo influenciados politicamente a partir de informações produzidas e fornecidas por seus próprios cidadãos sem que haja qualquer manifestação pública por parte do setor de tecnologia, que jamais assumiu qualquer responsabilidade por suas ações.

Ante tal cenário, Adriana Veloso Meireles (2023) alerta para o fato de que é necessário dar publicidade aos processos decisórios dos algoritmos inteligentes, de modo que o Estado precisa desempenhar seu papel de intermediário entre os interesses privados e a coletividade. A autorregulação do setor privado tem se mostrado cada vez mais insuficiente em

conter fenômenos que corroem as democracias contemporâneas. Não é sem razão que vozes, como Floridi (2021), têm defendido o fim de uma era: é chegado o momento em que a autorregulação das plataformas digitais e *bigtechs* deve dar espaço à criação de normas de direito que tragam balizas seguras para a proteção dos usuários e cidadãos.

É necessário perceber, contudo, que não se trata apenas de uma exposição aos dispositivos eletrônicos, mas de máquinas "aprendendo o que podem sobre as pessoas, seus atributos e ações passadas, em um esforço para entender suas predisposições e prever ações futuras" (Meireles, 2023, p. 2). As relações humanas estão sendo mediadas por algoritmos em todo tempo, sem que as pessoas estejam cientes ou atentas a tal fato. A ausência de normas impositivas torna a exploração do setor passível de abusos, especialmente violações de direitos humanos, como a autonomia, a liberdade e a dignidade.

Sobre a regulamentação desse cenário, Welligton Franham, CEO da *Century Data*, empresa especializada em cibersegurança, sustenta que o mundo está dando passos significativos sobre o assunto, mas ainda há grandes desafios na área, sobretudo em relação à eficácia das leis e ao fato de que a legislação precisa ser periodicamente atualizada em decorrência dos avanços tecnológicos. Assim, Franham defende que é preciso um esforço conjunto entre os países para garantir a proteção dos dados pessoais no mundo atual (Folha Vitória, 2024).

As normas jurídicas e instituições não podem mais negligenciar o que ocorre na esfera privada, uma vez que a temática em questão se torna cada vez mais política, fazendo com que a proteção de dados pessoais deixe de ser um assunto individual e ganhe uma dimensão coletiva, uma vez que ocorre uma transformação na coleta de dados realizada de forma automatizada e indiscriminada (Meireles, 2023). A ação das empresas, portanto, reflete em toda a sociedade e há preocupação porque, em regra, as pessoas não têm noção da importância da proteção de seus dados por falta de letramento nesta questão, que só mais recentemente ganhou notoriedade.

Segundo um levantamento elaborado pela *United Nations Conference on Trade and Development* (UNCTAD) no ano de 2021, a proteção de dados e privacidade não são mais apenas preocupações de nações desenvolvidas; pelo contrário, trata-se de uma questão global, ainda que as leis variem de país para país (UNCTAD, 2021).

Em meados de maio de 2018, a União Europeia promulgou a *General Data Protection Regulation* (GDPR), que estava em tramitação desde 2012, tendo sido aprovada em 2016 pelo Parlamento. A lei possui a finalidade de proporcionar aos usuários o controle sobre seus dados pessoais, que são armazenados pelas empresas ao navegarem pela internet. Mais do que isso, desde o início a GDPR visa à privacidade das pessoas e se preocupa com a segurança dos dados armazenados, razão pela qual passou a inviabilizar que as empresas armazenem qualquer informação que possa identificar um usuário sem o consentimento dele, como *cookies, e-mail,* endereço IP, dados biométricos, entre outros (O que é GDPR..., 2019).

A *General Data Protection Regulation* é um único regulamento sobre o tratamento das informações pessoais de indivíduos e instituições pautadas nos regramentos desenvolvidos, disponível para os cidadãos da Áustria, Alemanha, Bélgica, Bulgária, Croácia, Chipre, Dinamarca, Eslováquia, Espanha, Estônia, Finlândia, França, Grécia, Hungria, Irlanda, Itália, Islândia, Letônia, Liechtenstein, Lituânia, Luxemburgo, Malta, Noruega, Países Baixos, Polônia, Portugal, Reino Unido, República Checa, Romênia e Suécia (Conheça..., 2023).

De acordo com dados divulgados pela *United Nations Conference on Trade and Development*, 134 países do mundo, o equivalente a 71%, possuem legislações próprias quanto à proteção de dados, em confronto com 15% de países que ainda não têm qualquer texto legal nesse sentido. Segundo os dados mundiais, 9% dos países estão caminhando a passos lentos para adequação de proteção e armazenamento de suas informações pessoais, como é o caso da Índia, seguido por 5% de países sem registros sobre o assunto (UNCTAD, 2021).

As preocupações e discussões acerca do tema da proteção de dados têm ganhado grande destaque tanto em âmbito internacional quanto nacional, por isso criou-se o Dia Internacional da Proteção de Dados. O dia 28 de janeiro marca o Dia Internacional da Proteção de Dados, remetendo ao dia da assinatura do primeiro e único tratado internacional sobre proteção de dados, denominado Convenção para a Proteção de Indivíduos com Relação ao Processamento Automático de Dados Pessoais, comumente referida como "Convenção 108" (Bakonyi; Belli; Chang, 2023).

O Brasil, apesar de ainda não celebrar o Dia Nacional da Proteção de Dados[1], é um dos países que aparecem na lista divulgada pela UNCTAD, haja vista que passou a adotar leis relacionadas à proteção de dados e privacidade, transações eletrônicas, direitos do usuário e crimes cibernéticos.

A partir de 2007 o debate sobre a proteção de dados pessoais no Brasil ganhou certa relevância no contexto da construção do Marco Civil da Internet (MCI). Em 2009, em torno dessa proposta, foi criada uma consulta pública na internet, promovida pelo Ministério da Justiça, para debater os direitos dos usuários da web no país (Meireles, 2023).

A Lei nº 12.965/2014 , fruto dessas discussões, trouxe garantias, princípios, direitos e deveres para o uso da internet no país. O Marco Civil da Internet é uma lei paradigmática para a realidade brasileira, justamente porque é "o resultado da primeira experimentação em larga escala da rede como forma de ampliar o universo de atores que participam do processo de construção legislativa" (Lemos; Souza, 2016, p. 11). Isto é, uma lei que versa sobre a internet teve sua construção pautada pela participação da sociedade civil *on-line*, fazendo proposições, criticando e interagindo.

Ainda que não seja uma norma voltada especificamente para a proteção de dados dos usuários, o MCI traz como um dos seus princípios basilares, no artigo 3º, III, a proteção de dados pessoais na forma de lei. Ademais, assegurou aos usuários, nos termos do artigo 7º: não fornecimento a terceiros de dados pessoais, inclusive registros de conexão, e de acesso a aplicações de internet, salvo mediante consentimento livre, expresso e informado ou nas hipóteses previstas em lei; informações claras e completas sobre coleta, uso, armazenamento, tratamento e proteção de dados pessoais, que somente poderão ser utilizados para finalidades justificadas, não vedadas pela legislação e especificadas em contrato ou termos de uso; além de consentimento expresso sobre coleta, uso, armazenamento e tratamento de dados pessoais, que deverá ocorrer de forma destacada das demais cláusulas contratuais.

[1] Embora o Brasil ainda não se beneficie da instituição de um Dia Nacional da Proteção de Dados, tal tema já é iniciativa do Projeto de Lei 2076/2022, que, inclusive, já foi aprovado pelo Senado e está pronto para apreciação no plenário da Câmara desde 2023 (Câmara, 2023).

Percebe-se que o MCI trouxe elementos importantes para a cultura da proteção de dados no país, introduzindo salvaguardas e pautando a autodeterminação informativa do usuário na internet, na medida que lhe deu ferramentas para tomar ciência do uso e tratamento de seus dados, também possibilitando ações como pedido de exclusão de informações coletadas[2], tudo isso em 2014, quando a pauta era bem restrita ao universo acadêmico. Sobre a origem da autodeterminação informativa, explicam Maria e Picolo (2021, n.p.):

> O direito à autodeterminação informativa foi reconhecido na decisão do caso referente ao recenseamento da população, em 1983, proferida pelo Tribunal Constitucional Alemão, após o desenvolvimento do tema ao longo de décadas nas cortes do país. Através dessa decisão, o tratamento não transparente de dados pessoais foi repudiado a partir da ideia da dignidade da pessoa humana e do livre desenvolvimento da personalidade. Naquela oportunidade, a Corte constitucional entendeu que, principalmente pela quantidade de informações coletadas, a iniciativa de recenseamento poderia possibilitar a criação de perfis completos da personalidade dos alemães, comprometendo a própria autonomia das pessoas. Então, esclareceu-se que o tratamento de dados deve ocorrer somente quando há uma justificativa legal a partir da finalidade do processamento.

Com o passar do tempo e o desenvolvimento tecnológico, especialmente quando se pensa no modelo de negócios instituído pelo capitalismo de vigilância (Zuboff, 2019), surgiram novas necessidades relacionadas à proteção de dados dos indivíduos. Assim é que, sob forte influência da lei de proteção de dados europeia, foi desenvolvida, em solo brasileiro, a Lei nº 13.709/18, denominada Lei Geral de Proteção de Dados, fazendo com que o Brasil integrasse um grupo de países que conta com uma legislação específica para a privacidade e preservação dos dados de seus cidadãos.

Registra-se que a LGPD teve sua vigência escalonada. Inicialmente entraram em vigor somente os artigos 55-A, 55-B, 55-C, 55-D, 55-E, 55-F, 55-G, 55-H, 55-I, 55-J, 55-K, 55-L, 58-A e 58-B, inseridos pela Lei nº 13.853/19 , que tratam da constituição da Autoridade Nacional de Proteção de Dados – ANPD – e do Conselho Nacional de Proteção de Dados Pessoais e da Privacidade – CNPD. Já em 18 de setembro de 2020 os demais artigos da norma, com exceção dos dispositivos que tratam da aplicação de sanções administrativas, passaram a vigorar. Por fim, em 1º de agosto de 2021, os artigos 52, 53 e 54, que tipificam sanções administrativas, tiveram sua vigência iniciada (Brasil, 2024).

A ANPD é uma autarquia de natureza especial vinculada ao Ministério da Justiça e Segurança Pública, responsável por cuidar da proteção dos dados pessoais e por orientar, regulamentar e fiscalizar o cumprimento da LGPD no Brasil (Brasil, 2022).

O mencionado órgão vem atuando de forma a incentivar e propagar a cultura de proteção de dados brasileiros, desenvolvendo, para tanto, estratégias de conscientização por meio de consultas públicas sobre os temas que necessitam de melhor regulamentação, de modo a permitir uma aproximação multissetorial, além de publicar orientações para processos

[2] A redação original do artigo 7º, X, do MCI, previa como direito do usuário a exclusão definitiva dos dados pessoais que tiver fornecido à determinada aplicação de internet, a seu requerimento e ao término da relação entre as partes, ressalvadas as hipóteses de guarda obrigatória de registros previstas no próprio MCI.

fiscalizatórios e guias de diretivas para os plurais atores previstos pela LGPD (Bakonyi; Belli; Chang, 2023).

Prestes a completar cinco anos, a LGPD incluiu o Brasil no mapa mundial dos países que possuem legislação específica para segurança e privacidade de dados e informações pessoais no âmbito digital.

Além disso, em fevereiro de 2022 foi promulgada a Emenda Constitucional 115/2022, em que, a partir do texto elaborado pela então senadora Simone Tebet (MDB-MS), o direito à proteção de dados pessoais passou a integrar o rol de direitos e garantias fundamentais ao cidadão, bem como foi fixada a competência privativa da União para legislar a respeito da proteção e tratamento de dados pessoais. Em outros termos, busca-se maior segurança jurídica ao país na aplicação da Lei Geral de Proteção de Dados Pessoais, atraindo ainda mais investimentos internacionais para o Brasil (Brasil, 2022).

Pontua-se que, no caso do Brasil, inicialmente veio a regra infraconstitucional, isto é, primeiro foi promulgada a Lei Geral de Proteção de Dados, para, somente em seguida, a questão receber o *status* de direito fundamental no inciso LXXIX do artigo 5º da Constituição Federal (Brasil, 1988). Tal fato demonstra a importância que a LGDP teve no cenário nacional, especialmente porque seus debates legislativos e acadêmicos abriram as portas para a constitucionalização da proteção de dados no país.

De acordo com um levantamento realizado pelo escritório Mattos Filho, o número de ações judiciais que discutem a aplicação da Lei Geral de Proteção de Dados Pessoais (LGPD) cresceu de menos de 20 para cerca de 120 entre os anos de 2020 e 2022, equivalente a um aumento de mais de 500%. A referida pesquisa considerou apenas decisões de natureza cível dos Tribunais de Justiça Estaduais, Superior Tribunal de Justiça e Supremo Tribunal Federal, de modo que processos criminais, trabalhistas e eleitorais foram excluídos do escopo de análise, bem como eventuais decisões da Agência Nacional de Proteção de Dados (Guimarães, 2023).

O fato de o cidadão médio possuir certo conhecimento sobre os seus direitos relacionados aos próprios dados pessoais, faz com que, em caso de eventual violação, ele se sinta legitimado a buscar uma reparação pela via judicial. De acordo com o levantamento realizado pelo escritório em tela, a maioria das demandas ao longo dos anos estudados foi ajuizada por titulares de dados, representando mais de 90% do universo total das ações sobre LGPD (Guimarães, 2023).

Sobre a temática principal dos processos analisados, o levantamento verificou que, majoritariamente, trata-se de prestação de serviços, energia e o sistema financeiro, uma vez que o destaque para os dois primeiros setores se deve à ocorrência de incidentes de segurança, por exemplo, “vazamento de dados da concessionária de energia Enel”. A questão de vazamento de dados pessoais, dentro de todos os aspectos previstos na LGPD, é o que mais chama atenção, pois, quando ocorre, pode efetivamente trazer um dano direto aos titulares de dados e aos controladores, que acabam se expondo nessa situação (Guimarães, 2023).

Ainda que a judicialização e a aplicação da LGPD tenham aumentado no Brasil, e alguns cidadãos tenham procurado o Judiciário por violações, sua difusão ainda está em estágio incipiente. A título de exemplo, somente no ano de 2023 a ANPD aplicou sua primeira multa por descumprimento da legislação nacional que protege dados pessoais.

A discussão precisa ser ampliada, especialmente em perspectiva interseccional com outras áreas do direito e das ciências sociais, posto que a proteção de dados é fundamental para resguardar direitos de toda a população, especialmente de grupos vulnerabilizados e socialmente excluídos. Sobre este assunto, passa-se a discorrer na próxima seção deste estudo.

3 PROTEÇÃO DE DADOS E GRUPOS VULNERÁVEIS

A sociedade é formada por pessoas cujos acessos às oportunidades e bens sociais disponíveis não se dão de maneira igual. Não é sem razão que a Constituição Federal traz, em seu artigo 5º, o princípio da isonomia que, em sua perspectiva material, assegura que as pessoas sejam tratadas de formas desiguais na medida de suas desigualdades se o objetivo é, ao fim, reparar algum desequilíbrio fático. Por isso, políticas públicas são criadas e instrumentos normativos são editados visando a trazer proteção para grupos que necessitem da atuação estatal em razão de suas vulnerabilidades sociais.

O debate sobre fragilidade social gravita sobre as ditas minorias, termo que possui diversas acepções e suscita controvérsias em sua conceituação (Silveira; Freitas, 2017). Em um primeiro momento pode-se pensar que grupos minoritários são aqueles que existem em menor quantidade, como se fosse um conceito relacionado ao aspecto numérico ou quantitativo. A ideia, inclusive, é reforçada pela redação do artigo 27 do Pacto dos Direitos Civis e Políticos, o qual dispõe que nos Estados em que haja minorias étnicas, religiosas ou linguísticas, as pessoas pertencentes a essas minorias não poderão ser privadas do direito de ter, conjuntamente com outros membros de seu grupo, sua característica vida cultural, de professar e praticar sua própria religião e usar sua língua natural.

De fato, inicialmente, a noção de grupo minoritário estava vinculada a números. Ramacciotti e Calgararo (2021, p. 4-5) explicam: “no vocabulário clássico da Filosofia Política herdado pela Ciência Política, o par maioria-minoria é definido pelo elemento numérico, significando o grupo majoritário da situação que exerce o poder de governo e o grupo minoritário, alienado do poder, tornando-se a oposição”.

Essa noção tradicional, todavia, não mais subsiste porque houve uma modificação no conceito de cidadania. De acordo com Marshall (2021), a partir da realidade e história da Inglaterra, o conceito de cidadania é composto por três elementos distintos: o civil, o político e o social. O elemento civil diz respeito às liberdades individuais, como o direito de ir e vir, o direito à propriedade, a liberdade de expressão e pensamento, a liberdade religiosa, a liberdade de imprensa, o direito de contratar livremente e o direito à justiça. Essas liberdades são garantias contra a intervenção do Estado, que deve se abster de interferir na vida dos cidadãos.

O elemento político abrange o direito ao exercício do poder político, seja como membro de uma autoridade política ou como eleitor dos membros desse órgão (Marshall, 2021). Por sua vez, o elemento social está intimamente ligado aos direitos sociais e às prestações por parte do Estado, tal como saúde e previdência.

Na Inglaterra a construção da cidadania ocorreu de forma gradual e seguiu uma progressão específica: primeiro, foram estabelecidas as liberdades individuais, seguidas pelo

exercício do poder político e, por fim, pelos direitos sociais. Carvalho (2021), ao analisar o contexto brasileiro, observa que o processo seguiu uma ordem ligeiramente diferente: as liberdades individuais vieram primeiro, seguidas pelos direitos sociais e, por último, pelos direitos políticos.

Isso porque os direitos sociais, ao longo da história do Brasil, foram usados como moeda de troca junto a população. Para evitar a emancipação política do povo, dando-lhe o livre-direito de votar e de ser votado, os governantes procuraram medidas sociais e assistenciais com o objetivo de demonstrar a desnecessidade do exercício dos direitos políticos por parte da população. Se tudo andava bem, se nada faltava, o voto direto, por exemplo, seria dispensável.

Ambos os autores concordam que a cidadania plena só é alcançada quando os indivíduos têm acesso aos três elementos. Como destaca Carvalho (2021, p. 170), "tornou-se comum dividir a cidadania em direitos civis, políticos e sociais. O cidadão pleno é aquele que possui todos os três direitos. Os cidadãos incompletos são aqueles que possuem apenas alguns desses direitos".[3]

Como mais e mais pessoas passaram a ser consideradas cidadãs, especialmente pela atuação das massas trabalhadores na reivindicação de seus direitos civis, políticos e sociais, buscando uma cidadania plena, o uso de um critério numérico para classificar as pessoas como minoritárias deixou de fazer sentido.

> A ampliação do uso do termo minorias para referir-se a sujeitos ou grupos minoritários, no sentido de grupos excluídos do direito à cidadania plena, foi tornando cada vez mais visível a insuficiência do critério numérico para a distinção entre os termos minoria-maioria, posto que as minorias, muitas vezes, correspondem numericamente à maioria da população, como no caso das mulheres, dos pretos, pardos e pobres no Brasil (Ramacciotti; Calgararo 2021, p. 6).

Quando se fala de grupos vulneráveis a ideia é sobre desigualdade nas relações de poder. Costa (2009, p. 57) explica que "os grupos vulneráveis representam parcela substancialmente significativa de uma população, mas sujeitos aos padrões de dominação vigentes em determinada sociedade, como acontece com as mulheres, crianças e adolescentes". Para os fins desta pesquisa, adota-se a terminologia grupos vulneráveis exatamente pela relação de desigualdade presente na sociedade brasileira e que pode ser acentuada pelo compartilhamento de dados pessoais, causando maior exclusão.

Um exemplo de grupo considerado vulnerável, no país, é a população negra[4]. Conforme dados do Instituto Brasileiro de Geografia e Estatística (IBGE, 2024), retirados do censo de 2022, cerca de 92,1 milhões de pessoas (ou 45,3% da população do país) declararam-se pardas. De acordo com o órgão, foi a primeira vez, desde 1991, que esse grupo predominou

[3] Em alguma medida, a cidadania plena, com o efetivo exercício de todos os direitos civis, sociais e políticos, é um ideal utópico. Isso porque as necessidades humanas são muitas e os recursos finitos, o que impossibilita que todas as pessoas consigam satisfazer suas carências. De toda forma, é papel do Estado a busca incessante pela completa realização da cidadania de seu povo.

[4] Neste texto o termo negro foi empregado utilizando o critério de autodeclaração de pessoas pretas e pardas, nos moldes do Instituto Brasileiro de Geografia e Estatística (IBGE).

no Brasil (Belandi; Gomes, 2023). O número de pessoas pretas, no mesmo censo, foi de 10,2% da população do país (IBGE, 2024).

Ocorre que, mesmo sendo a maioria populacional, as pessoas negras ocupam apenas 48,3% das vagas universitárias, somando as instituições públicas e privadas (Alfano, 2023). Vê-se, portanto, que o acesso à educação superior ainda é privilégio de uma maioria branca, malgrado o número de pessoas negras no país seja maior em seus termos absolutos.

Assim, a vulnerabilidade, para os fins aqui delineados, vai depender do contexto analisado. Se há uma situação fática ou estrutural que gera desigualdade de forma ordenada e sistemática entre pessoas, entende-se que o grupo excluído é vulnerável. Pode-se citar como exemplo, para além das pessoas negras, a população LGBTQIA+, mulheres, crianças, idosos, migrantes e pessoas com deficiência.

No contexto da utilização de dados pessoais, todas as pessoas são hipossuficientes enquanto consumidoras de produtos e serviços. A utilização e exploração de dados gera assimetrias de poder com base em uma desigualdade informacional, tal como a oriunda da utilização de ferramentas de previsão de comportamentos ou de mecanismos de persuasão que associam dados e psicologia para convencer pessoas. Se os usuários forem comparados com as grandes *bigtechs*, ao fim e ao cabo todos serão vulneráveis porque a assimetria de poder é patente.

Grupos de pessoas socialmente excluídas no Brasil, no entanto, podem ter sua exclusão potencializada quando dados são coletados para fins de vigilância e controle. Historicamente, certas comunidades têm sido alvo de estigmatização, resultando, frequentemente, em um aumento de sua vulnerabilidade. As informações relacionadas a essas populações muitas vezes são manipuladas de maneira acentuada, exacerbando ainda mais sua situação (Costa, 2022).

Kremer (2022) explana, a partir da análise de crédito para contratações no Brasil, que isso acontece porque o indivíduo é julgado não por sua individualidade, mas pelas características do grupo a que pertence. Tradicionalmente, seguros de carros de pessoas jovens são mais caros. Mesmo que o novo motorista seja excepcionalmente cuidadoso ao dirigir, o custo do seguro do carro para sua família pode aumentar significativamente devido à avaliação de um perfil de risco. Esses aumentos são, muitas vezes, baseados em projeções de comportamento, incluindo o histórico de outros jovens na mesma faixa etária. Embora as seguradoras realizem análises de risco individual, elas também consideram os padrões de comportamento de grupos semelhantes ao definir as taxas.

Kremer (2022, p. 231), a partir de dados do Ipea, ilustra que para mulheres negras, no Brasil, o caso é ainda mais complexo: “Apenas 10% das mulheres negras possuem ensino superior completo e mulheres negras são extremamente sub-representadas na política (0,5% dos candidatos eleitos em geral) e sobrerrepresentadas no trabalho doméstico (57,6%)”.

Qualquer instrumento regulatório, o que inclui a Lei Geral de Proteção de Dados Pessoais, precisa estar atento aos processos históricos e sociais de exclusão que perpassam a sociedade sob pena de acabar reforçando iniciativas estigmatizantes e excludentes. Por isso, a LGPD prevê, como princípio norteador na atividade de tratamento de dados pessoais, a não

discriminação, estabelecendo, no artigo 6º, IX, a impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos.

Nesse sentido, chama-se atenção para a potencialização do racismo estrutural[5] por meio do uso indiscriminado de dados pessoais por empresas de crédito. A coleta de dados de pessoas negras, sem análise crítica ou curadoria, especialmente por meio de mecanismos de controle e vigilância (Zuboff, 2019), pode levar à prática do racismo creditício, conforme definido por Amparo e Prado (2024).

O racismo creditício manifesta-se como uma discriminação racial estrutural no acesso ao crédito, caracterizada pela repetição de práticas excludentes e pela negligência em lidar com o risco discriminatório (Amparo; Prado, 2024). No contexto brasileiro, marcado por uma histórica exclusão e marginalização da população negra, essa prática pode perpetuar e até mesmo intensificar as desigualdades já existentes.

Os dados coletados inevitavelmente refletem a exclusão social historicamente imposta às pessoas negras no Brasil. Consequentemente, a utilização desses dados brutos e não tratados em análises de crédito, tende a reproduzir e legitimar essa exclusão, restringindo o acesso ao crédito e, por extensão, a outros direitos. Essa restrição não é apenas uma consequência da análise de dados, mas, sim, um reflexo de uma estrutura social desigual que se perpetua por meio da tecnologia, caso não haja uma abordagem crítica e consciente.

Nesse sentido, deve-se considerar o recorte racial na análise creditícia que utiliza a coleta de dados. Tal consideração é fundamental para que o Brasil não continue a reproduzir a discriminação estrutural enraizada em seu processo histórico. Ignorar a dimensão racial na análise de crédito significa perpetuar um ciclo de exclusão, em que dados que refletem a marginalização passada são utilizados para justificar a marginalização presente e futura.

Uma análise creditícia verdadeiramente equitativa no Brasil deve incorporar uma perspectiva racial crítica. Isso implica não apenas coletar dados, mas também compreender como esses dados são formados e influenciados por um histórico de desigualdade racial. A ausência dessa análise crítica e curadoria nos processos de coleta e utilização de dados pelas empresas de crédito pode, inadvertidamente ou não, reforçar o racismo estrutural e o racismo creditício, perpetuando a exclusão de uma parcela significativa da população brasileira.

A pesquisadora Cathy O'Neil (2020) ressalta o papel desempenhado pelos algoritmos na geração e perpetuação de preconceitos. Isso deve-se ao fato de que os sistemas algorítmicos empregados em aplicativos têm o poder de modelar a interação das pessoas nessas plataformas; contudo, são criações humanas com limitações inerentes. O'Neil (2020) caracteriza os algoritmos como potenciais "instrumentos de devastação matemática", pois são fundamentados em decisões tomadas por seres humanos suscetíveis a erros, resultando em consequências sociais profundamente prejudiciais, especialmente para comunidades mais marginalizadas (Costa; Kremer, 2022).

[5] Bersani (2018, p. 193) assevera que "o racismo estrutural corresponde a um sistema de opressão cuja ação transcende a mera formatação das instituições, eis que perpassa desde a apreensão estética até todo e qualquer espaço nos âmbitos público e privado, haja vista ser estruturante das relações sociais e, portanto, estar na configuração da sociedade, sendo por ela naturalizado".

Na mesma linha, Mittelstadt *et al.* (2016) entendem que a utilização de dados por algoritmos pode ocasionar resultados discriminatórios para certos grupos de pessoas vulneráveis porque traz efeitos negativos gerados, afinal, os algoritmos não conseguem julgar a justiça de suas decisões, elemento que depende de uma valoração humana.

Frazão (2021) utiliza a expressão discriminação estatística para se referir à mesma problemática:

> É interessante observar que os problemas da discriminação estatística ocorrem mesmo quando os dados estão corretos e também as estatísticas. Aliás, é comum se dizer que quanto mais arraigado for um preconceito na vida real, mais os algoritmos tenderão a vê-lo como um padrão e mais tenderão a replicá-lo se não houver nenhum cuidado para conter esse processo.
>
> Ademais, os problemas da discriminação estatística se tornarão ainda mais graves quando os dados não são de qualidade ou quando há falhas na própria utilização da metodologia estatística ou na interpretação dos seus resultados, como acontece nas hipóteses em que se confunde correlação com causalidade.

Em relação às pessoas LGBTQIAPN+ no Brasil, a discriminação e violência são preocupantes. Embora haja uma dificuldade na produção de dados sobre esta camada da população, o Atlas da Violência de 2024 (Cerqueira; Bueno, 2024, p. 62-63) expõe que:

> ... em 2022, 8.028 pessoas dissidentes sexuais e de gênero foram vítimas de violência no Brasil, um aumento de 39,4% em relação a 2021, quando foram registrados 5.759 casos. Analisando a série histórica desde 2014, nota-se que os casos cresceram ano a ano, à exceção de 2020, primeiro ano da pandemia de Covid-19, quando os serviços presenciais caíram consideravelmente. O salto entre 2021 e 2022, no entanto, é o segundo maior da série10, acendendo um alerta para o aumento da violência contra essa população.

Sabe-se que no Brasil a LGBTfobia é um problema estrutural da sociedade. Para Ramos e Nicoli (2016, p. 183), "LGBTfobia é o sentimento, a convicção ou a atitude dirigida contra lésbicas, gays, bissexuais, pessoas trans e travestis que inferioriza, hostiliza, discrimina ou violenta esses grupos em razão de sua sexualidade e/ou identidade de gênero"[6]. Para Pedra (2020), a estruturalidade do preconceito contra pessoas LGBTQIAPN+ não se explica analisando comportamentos individuais, mas compreendendo que a LGBTfobia atravessa uma gama de aspectos da vida e das relações sociais, tomando inclusive nuances institucionais, o que inclui evidentemente as normas e os aparatos do Direito. Tanto é assim que, até hoje, todos os direitos adquiridos por este grupo populacional vieram a partir de demandas judicializadas e não por lei federal.

A coleta de dados e vigilância sobre estas pessoas pode aumentar ainda mais o preconceito e o estigma social. A exposição da orientação sexual, um dado sensível, sem o consentimento explícito e informado da pessoa, representa uma grave violação da privacidade. No contexto brasileiro, em que a violência e a discriminação contra pessoas LGBTQIA+ são uma realidade, essa exposição pode ter consequências sérias, como ostracismo social, violência

[6] Para a LGPD, a orientação sexual é um dado pessoal sensível, isto é, merece maior atenção que outros dados pessoais.

física ou psicológica e dificuldades no acesso a emprego e moradia. O medo dessa exposição pode levar pessoas a omitir sua orientação sexual, limitando sua liberdade e autenticidade.

A ideia da estigmatização da população LGBTQIA+ como promíscua pode ser reforçada pelo uso inadequado de dados. Se informações sobre encontros, relacionamentos ou hábitos de consumo forem coletadas e analisadas de forma enviesada, podem criar ou reforçar estereótipos negativos. Por exemplo, a análise de padrões de consumo em aplicativos de relacionamento ou a inferência da vida sexual a partir de outros dados, podem ser usadas para estigmatizar e discriminar pessoas LGBTQIA+, alimentando preconceitos já existentes na sociedade brasileira.

Além disso, a falta de transparência sobre como esses dados são coletados, armazenados e utilizados impede que a população LGBTQIA+ possa se proteger contra práticas discriminatórias. A ausência de mecanismos de controle e contestação desses usos de dados dificulta a responsabilização de empresas ou instituições que venham a praticar discriminação com base na orientação sexual.

Outra preocupação gerada pela utilização de dados, especialmente para fins preditivos, é o fenômeno da fossilização. Matsumi e Solove (2024 , p. 6) ponderam que as previsões são baseadas em dados sobre o passado. “Decisões que envolvem previsões algorítmicas podem reforçar padrões de dados antigos e podem consolidar ainda mais a discriminação, a desigualdade e os privilégios”.

Como a sociedade é desigual por processos de exclusão, tais como o racismo estrutural e a LGBTfobia, decisões tomadas com base em dados refletirão os mesmos problemas presentes no seio social. Não há como utilizar informações “poluídas” e esperar resultados “puros”. Mittelstadt *et al.* (2016) explicam que se entra lixo sai lixo.

Dessa forma, a previsão de comportamos pode reforçar padrões sociais de maneira que o dado reforça a desigualdade e esta será ainda mais difícil de romper. Frazão (2021) alerta, igualmente, que algoritmos são construídos por programadores que possuem vieses e preconceitos, os quais podem ser incorporados aos sistemas criados, mesmo que de forma não intencional.

Os seres humanos colocam suas subjetividades nas suas criações, que acabam por refletir suas crenças e valores. Ainda que haja um discurso de neutralidade, a ausência de transparência no funcionamento do algoritmo ou da própria coleta de dados dificulta o entendimento do processo de exclusão e de possibilidades de correções. Maranhão, Florêncio e Almada (2021) pontuam que esta opacidade de como o processo é decidido inviabiliza a própria contestação dos resultados.

Com a crescente utilização da internet e de mecanismos de tecnologia da informação e comunicação, dados sobre a vida das pessoas são coletados o tempo inteiro alimentando modelos de negócios lucrativos que buscam explorar as emoções humanas em uma sistemática de economia da atenção (Wu, 2016). Quanto mais tempo os indivíduos permanecem em telas mais sua atenção é capturada e redirecionada para fins diversos, como comerciais e políticos.

Costa e Kremer (2022, p. 156) asseveram que “as tecnologias digitais conseguem mapear e reunir informações relevantes sobre nossas vidas, identidade e personalidades, a

partir dos dados que disponibilizamos ao utilizarmos seus serviços". Como o volume de dados coletados é amplo e massificado, os detentores das informações acabam conseguindo fazer previsões precisas ou influenciar comportamentos de uma forma preocupante para a sociedade. A situação é alarmante, sobretudo porque não há transparência sobre os modelos de negócios adotados. Instrumentos normativos, como a Lei Geral de Proteção de Dados, acabam ajudando a enfraquecer essa assimetria de poder que conta com grandes empresas de tecnologia de um lado e pessoas cidadãs do outro.

Frazão (2021) entende que surgem possibilidades para discriminações altamente personalizadas e complexas em cenários como este, às vezes explorando as fragilidades e vulnerabilidades individuais. A ideia é que a exclusão seria altamente pessoal e prejudicial porque é feita de maneira customizada.

Um exemplo seria o compartilhamento ilícito de dados de saúde de pessoas idosas, reunidos a partir de dispositivos que registram horas de sono e pressão cardíaca, tais como os novos relógios de grandes empresas de tecnologia. Como o aparelho capta informações específicas e individualizadas, o compartilhamento com empresas gestoras de planos de saúde poderia gerar prejuízos direcionados, como o aumento no valor do plano. A companhia podia alegar que o paciente idoso não tem dormido as horas necessárias para manter sua qualidade de vida e estaria assumindo riscos que oneram o plano. A questão é relevante porque, no Brasil, conforme dados do censo de 2022 (IBGE, 2024), o número de pessoas com 65 anos ou mais de idade cresceu 57,4% em 12 anos (Gomes; Britto, 2023). Com o envelhecimento da população e o aumento do número de idosos, sua proteção digital ganha mais relevância ainda.

Da mesma forma, devem-se proteger crianças e adolescentes da coleta de dados e da vigilância. De acordo com o Censo de 2022 (IBGE, 2024), o percentual de crianças de até 14 anos de idade, que era de 38,2% em 1980, passou a 19,8% em 2022. Sendo pessoas em formação, as estratégias de microssegmentação voltadas para crianças e adolescentes têm potencial prejudicial.

Em primeiro lugar, essa segmentação excessivamente específica pode levar à estereotipagem de gênero precoce e reforçada. Ao direcionar brinquedos considerados "de menino" ou "de menina" de forma tão precisa, a publicidade limita o universo de possibilidades e interesses que crianças e adolescentes poderiam explorar livremente. Isso pode influenciar suas escolhas, restringindo o desenvolvimento de habilidades e gostos que não se encaixam nos estereótipos tradicionais, como meninas se interessarem por ciências exatas ou meninos por atividades consideradas mais sensíveis.

Em segundo lugar, a microssegmentação pode contribuir para a criação de desejos e necessidades artificiais. Ao apresentar repetidamente um determinado tipo de brinquedo a um grupo específico, a publicidade pode induzir um sentimento de falta e a necessidade de possuir aquele item para se sentir incluído ou aceito. Isso pode gerar frustração, ansiedade e até mesmo comportamentos consumistas desde cedo, moldando uma relação com o consumo baseada no desejo induzido e não em um interesse genuíno.

Além disso, a segmentação focada em crianças e adolescentes pode explorar sua menor capacidade de discernimento e senso crítico. Eles podem ter dificuldade em distinguir a intenção persuasiva da publicidade e podem ser mais facilmente influenciados por mensagens

que apelam à emoção, à novidade ou à pressão dos pares. A microssegmentação permite que a publicidade seja altamente personalizada para atingir esses pontos de vulnerabilidade, tornando a persuasão ainda mais eficaz e potencialmente manipuladora.

Novamente, como explorado anteriormente, tal sistema de vigilância a partir de dados, mas com lucros altos para algumas empresas, foi desenvolvido pela professora Shoshana Zuboff (2019 , p. 7) como capitalismo de vigilância. Em suas palavras:

> O capitalismo de vigilância reivindica unilateralmente a experiência humana como matéria-prima gratuita para tradução em dados comportamentais. Embora alguns desses dados sejam aplicados à melhoria de produtos ou serviços, o restante é declarado como um excedente comportamental proprietário, alimentado em processos de fabricação avançados conhecidos como "inteligência de máquina" e fabricado em produtos de previsão que antecipam o que você fará agora, em breve, e depois. Finalmente, estes produtos de previsão são negociados num novo tipo de mercado para previsões comportamentais que chamo de mercados futuros comportamentais. Os capitalistas de vigilância enriqueceram imensamente com estas operações comerciais, pois muitas empresas estão ansiosas por apostar no nosso comportamento futuro.

A circulação de dados pessoais de forma indiscriminada é prejudicial porque acaba fomentando esse sistema predatório de previsão e influência sobre a vontade humana. Quando a pessoa faz parte de algum grupo vulnerável, o acesso a informações pessoais sem qualquer controle traz contornos mais preocupantes. No contexto brasileiro, a Lei Geral de Proteção de Dados conceitua dado pessoal como informação relacionada à pessoa natural identificada ou identificável (artigo 5º, I).

Para que haja tratamento de dados pessoais é necessário que alguma base legal da norma seja adotada como fundamento. As bases legais estão previstas no artigo 7º da LGPD e a ideia do legislador é de que a utilização de dados pessoais esteja amparada em uma justificativa socialmente aceitável ou com o consentimento livre e informado da pessoa titular.

A LGPD traz um conceito importante para os grupos vulneráveis que é a definição de dado pessoal sensível, expresso no artigo 5º, II. Para o diploma, dados pessoais sensíveis são aqueles sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou à organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural.

> [...] a própria seleção sobre quais dados seriam sensíveis demonstra que a circulação de determinadas informações pode acarretar maior potencial lesivo aos seus titulares, em uma determinada configuração social (DONEDA, 2019, p. 143). Partindo desse pressuposto, a compreensão sobre os mecanismos que devem ser empregados na proteção de dados sensíveis perpassa um entendimento sobre as dinâmicas discriminatórias que são articuladas na sociedade (Costa; Kremer, 2022, p. 157).

Logo, a escolha legislativa de que existem dados cujos acessos devem ser considerados sensíveis está conectada e demonstra a necessidade da proteção de grupos de pessoas cujas informações pessoais, se compartilhadas, podem gerar prejuízos graves.

Quando se pensa em pessoas com deficiência, explorar seus dados de saúde pode gerar prejuízos. No Brasil, estima-se que 18,6 milhões de pessoas de 2 anos ou mais tenham algum tipo de deficiência (Gomes, 2023). O compartilhamento de dados entre estabelecimentos comerciais, como farmácias e planos de saúde, por exemplo, tem potencial de causar danos financeiros.

Compartilhar dados detalhados sobre seus gastos com medicamentos, terapias e outros produtos de saúde, pode fornecer aos planos de saúde informações adicionais para aumentar as mensalidades ou impor restrições de cobertura. Ao identificarem um padrão de uso contínuo e potencialmente elevado de recursos de saúde, os planos podem considerar essas pessoas como "de maior risco" financeiro, mesmo que essa utilização seja inerente à sua condição e necessária para sua qualidade de vida e inclusão social. Esse aumento de custos pode tornar os planos de saúde inacessíveis, prejudicando ainda mais o acesso à saúde e, consequentemente, sua autonomia e bem-estar.

Ademais, o compartilhamento de dados pode levar à criação de perfis de riscos financeiros específicos para pessoas com deficiência. Ao analisar os dados de compra em farmácias, os planos de saúde podem identificar quais medicamentos, produtos e serviços são mais utilizados por pessoas com diferentes tipos de deficiência. Essa informação pode ser usada para segmentar o mercado e aplicar preços diferenciados ou condições contratuais menos favoráveis para esse grupo. Por exemplo, um plano de saúde poderia aumentar a coparticipação ou limitar o acesso a determinados tratamentos para pessoas com deficiências específicas, sob a justificativa de gerenciar seus custos.

A vulnerabilidade social deve ser percebida também a partir do mundo virtual. O capitalismo de vigilância não pode ser um instrumento de controle, dominação e discriminação de pessoas por características individuais, que são, por vezes, imutáveis. É dever, sobretudo do Estado, promover a cidadania ampla, protegendo os vulneráveis em todas as searas de sua vida. Não é por acaso que Bruzaca e Dos Santos (2024, p. 5) entendem que, apesar da evolução, reconhecimento e previsão dos direitos humanos, "não raro é percebida sua ineficácia, com contínuas situações de violações". A exploração indiscriminada de dados num contexto de capitalismo de vigilância tem o condão de aumentar estas violações.

Longe de esgotar todas as hipóteses de discriminação que o acesso a dados pessoais pode acarretar, este texto, até aqui, demonstrou algumas das possibilidades de prejuízos possíveis para grupos vulneráveis nas hipóteses de compartilhamento indevido de dados no Brasil, provando a hipótese inicial aventada.

4 CONCLUSÃO

A proteção de dados é uma questão central no contexto da sociedade contemporânea, especialmente quando se trata de grupos vulneráveis. A Constituição Federal estabelece o princípio da isonomia, que busca corrigir desigualdades sociais por meio de políticas públicas e instrumentos normativos. O debate sobre fragilidade social envolve diferentes concepções de minorias, que vão além de uma mera contagem numérica, abrangendo grupos que historicamente foram excluídos do pleno exercício da cidadania.

A evolução do conceito de cidadania, conforme observado por Marshall (2021), engloba não apenas direitos civis e políticos, mas também direitos sociais, essenciais para uma participação plena na sociedade. A realidade, no entanto, mostra que, mesmo com avanços legislativos, certos grupos continuam enfrentando desigualdades estruturais, como mulheres, minorias étnicas e LGBT+, que, muitas vezes, são vítimas de discriminação e exclusão.

O advento das tecnologias digitais trouxe consigo novos desafios, especialmente no que diz respeito à proteção de dados pessoais. O uso indiscriminado e a exploração de dados podem agravar ainda mais a vulnerabilidade desses grupos, perpetuando preconceitos e injustiças sociais. Algoritmos, quando não utilizados com cautela, podem reforçar padrões discriminatórios e excludentes, ampliando assimetrias de poder e aprofundando desigualdades.

A legislação, como a Lei Geral de Proteção de Dados Pessoais, desempenha um papel crucial na regulamentação do uso de dados pessoais e na proteção dos direitos individuais. Ao reconhecer a existência de dados sensíveis e estabelecer regras para seu tratamento, a LGPD busca mitigar os riscos de discriminação e exclusão. É fundamental, entretanto, que haja uma vigilância constante e um engajamento ativo da sociedade para garantir que os princípios de igualdade e justiça sejam efetivamente aplicados no contexto digital.

Diante desse cenário, é imperativo que sejam adotadas medidas que promovam uma maior transparência, responsabilidade e *accountability* no uso de dados pessoais, especialmente em relação aos grupos vulneráveis. Somente por intermédio de um esforço conjunto entre governo, sociedade civil e empresas será possível construir uma sociedade mais justa e inclusiva, em que todos os indivíduos tenham seus direitos respeitados e protegidos, independentemente de sua origem étnica, orientação sexual ou condição socioeconômica.

5 REFERÊNCIAS

ALFANO, Bruno. Proporção de negros nas universidades cai pela primeira vez desde 2016. *O Globo*. 8 jun. 2023. Disponível em: https://oglobo.globo.com/brasil/educacao/noticia/2023/06/proporcao-de-universitarios-negros-cai-pela-primeira-vez-desde-2016.ghtml. Acesso em: 4 jun. 2024.

BAKONYI, Erica; BELLI, Luca; CHANG, Sofia. *Dia Internacional da Proteção de Dados:* O que celebramos, por que e como? Fundação Getúlio Vargas, 30 de janeiro de 2023. Disponível em: https://portal.fgv.br/artigos/dia-internacional-protecao-dados-lgpd. Acesso em: 3 jun. 2024.

BELANDI, Caio; GOMES, Irene. Censo 2022: pela primeira vez, desde 1991, a maior parte da população do Brasil se declara parda. *Agência IBGE Notícias.* 22 dez. 2023. Disponível em: https://agenciadenoticias.ibge.gov.br/agencia-noticias/2012-agencia-de-noticias/noticias/38719-censo-2022-pela-primeira-vez-desde-1991-a-maior-parte-da-populacao-do-brasil-se-declara-parda#:~:text=Desde%201991%2C%20esse%20contingente%20n%C3%A3o,amarelas%20(0%2C4%25). Acesso em: 0 jun. 2024.

BERSANI, Humberto. Aportes teóricos e reflexões sobre o racismo estrutural no Brasil. *Revista Extraprensa,* São Paulo, v. 11, n. 2, p. 175-196, 2018.

BRASIL. Constituição Brasileira (1988). *Constituição da República Federativa do Brasil:* promulgada em 5 de outubro de 1988. Brasília, DF: Senado, 1988.

BRASIL. *Lei nº 12.965*, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Brasília, DF: Presidência da República, 2014. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 17 abr. 2025.

BRASIL. *Lei nº 13.709*, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República, 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 17 abr. 2025.

BRASIL. *Lei nº 13.853*, de 8 de julho de 2019. Altera a Lei nº 13.709, de 14 de agosto de 2018, para dispor sobre a proteção de dados pessoais e para criar a Autoridade Nacional de Proteção de Dados; e dá outras providências. Brasília, DF: Presidência da República, 2019. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/lei/l13853.htm. Acesso em: 17 abr. 2025.

BRASIL. *Emenda Constitucional nº 115*, de 10 de fevereiro de 2022. Altera a Constituição Federal para incluir a proteção de dados pessoais entre os direitos e garantias fundamentais e para fixar a competência privativa da União para legislar sobre proteção e tratamento de dados pessoais. Brasília, DF: Presidência da República, 2022. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/emendas/emc/emc115.htm. Acesso em: 17 abr. 2025.

BRASIL. *Proteção de Dados Pessoais agora é um direito fundamental.* 10 de fevereiro de 2022. Disponível em: https://www.gov.br/anpd/pt-br/protecao-de-dados-pessoais-agora-e-um-direito-fundamental. Acesso em: 30 maio 2024.

BRASIL. *Quando a LGPD entrou em vigor?* 25 de julho de 2024. Disponível em: https://www.gov.br/anpd/pt-br/acesso-a-informacao/perguntas-frequentes/perguntas-frequentes/1-lei-geral-de-protecao-de-dados-pessoais-lgpd/1-3-quando-a-lgpd#:~:text=A%20Lei%20entrou%20em%20vigor,que%20tratam%20das%20san%C3%A7%C3%B5es%20administrativas. Acesso em: 12 abr. 2025.

BRUZACA, Ruan Didier; DOS SANTOS, Claudineide Alves. Implicações do neoliberalismo na garantia de direitos da pessoa humana em saúde mental: Uma análise a partir do contexto da política pública de saúde mental brasileira. *Revista Direitos Humanos e Democracia,* Ijuí: Editora Unijuí, v. 12, n. 24, p. e16007, 2024. DOI: 10.21527/2317-5389.2024.24.16007. Disponível em: https://revistas.unijui.edu.br/index.php/direitoshumanosedemocracia/article/view/16007. Acesso em: 17 abr. 2025.

CARVALHO, José Murilo de. *Cidadania no Brasil:* o longo caminho. Rio de Janeiro: Editora Civilização Brasileira, 2021.

CERQUEIRA, Daniel; BUENO, Samira (coord.). *Atlas da violência 2024.* Brasília: Ipea; FBSP, 2024. Disponível em: https://repositorio.ipea.gov.br/handle/11058/14031 Acesso em: 17 abr. 2025.

CONHEÇA as Leis de Proteção de Dados ao redor do mundo. 30 de junho de 2023. Disponível em: https://www.lgpdbrasil.com.br/conheca-as-leis-de-protecao-de-dados-ao-redor-do-mundo/. Acesso em: 30 maio 2024.

COSTA, Rodrigo Vieira. Direitos e reconhecimento dos homossexuais no município de Fortaleza durante a gestão Fortaleza Bela 2005-2008. *Espaço Jurídico Journal of Law [EJJL]*, v. 10, n. 1, p. 52-76, 2009. Disponível em: https://portalperiodicos.unoesc.edu.br/espacojuridico/article/view/1920 Acesso em: 14 abr. 2025.

COSTA, Ramon; KREMER, Bianca. Inteligência artificial e discriminação: desafios e perspectivas para a proteção de grupos vulneráveis diante das tecnologias de reconhecimento facial. *Direitos Fundamentais & Justiça,* Belo Horizonte, ano 16, p. 145-167, out. 2022. Número especial.

COSTA, Ramon. Personalidade hackeada: considerações sobre proteção de dados pessoais sensíveis, vigilância digital e discriminação. *In:* TEFFÉ, Chiara Spadaccini de; BRANCO, Sérgio (coord.). *Proteção de dados e tecnologia:* estudos da Pós-Graduação em Direito Digital. Rio de Janeiro: Instituto de Tecnologia e Sociedade do Rio de Janeiro: ITS/Obliq, 2022.

UNCTAD. United Nations Conference on Trade and Development. *Data protection and privacy legislation worldwide*. 2021. Disponível em: https://unctad.org/page/data-protection-and-privacy-legislation-worldwide. Acesso em: 29 maio 2024.

FLORIDI, Luciano. The End of an Era: from Self-Regulation to Hard Law for the Digital Industry. *Philosophy and Technology*, v. 34, p. 619-622, 2021.

FRAZÃO, Ana. Discriminação algorítmica: Por que algoritmos preocupam quando acertam e erram? *Jota,* 4 ago. 2021. Disponível em: https://www.jota.info/opiniao-e-analise/colunas/constituicao-empresa-e-mercado/discriminacao-algoritmica-por-que-algoritmos-preocupam-quando-acertam=-e-erram04082021-?non-beta1=#:~:text-Discrimina%C3%A7%C3%A3o%20algor%C3%ADtmica%3A%20por%20que%20algoritmos%20preocupam%20quando%20acertam%20e%20erram%3F,-Mapeando%20algumas%20das&text=Como%20os%20artigos%20anteriores%20da,par%C3%A2metros%20%C3%A9ticos%20e%20jur%C3%ADdicos%20fundamentais. Acesso em: 5 jun. 2024.

FOLHA VITÓRIA. 12 mar. 2024. Disponível em: https://www.folhavitoria.com.br/geral/noticia/03/2024/protecao-de-dados-71-dos-paises-tem-leis-sobre-o-tema. Acesso em: 5 jun. 2024.

GUIMARÃES, Arthur. Ações judiciais sobre LGPD aumentam mais de 500% em dois anos. *Jota,* São Paulo, 9 mar. 2023. Disponível em: https://www.jota.info/justica/acoes-judiciais-sobre-lgpd-aumentam-em-mais-de-500-em-dois-anos-09032023#:~:text=O%20n%C3%BAmero%20de%20a%C3%A7%C3%B5es%20judiciais,realizado%20pelo%20escrit%C3%B3rio%20Mattos%20Filho. Acesso em: 5 jun. 2024.

GOMES, Irene; BRITTO, Vinícius. Censo 2022: número de pessoas com 65 anos ou mais de idade cresceu 57,4% em 12 anos. *Agência IBGE Notícias*. 27 out. 2023. Disponível em: https://agenciadenoticias.ibge.gov.br/agencia-noticias/2012-agencia-de-noticias/noticias/38186-censo-2022-numero-de-pessoas-com-65-anos-ou-mais-de-idade-cresceu-57-4-em-12-anos. Acesso em: 16 abr. 2025.

GOMES, Irene. Pessoas com deficiência têm menor acesso à educação, ao trabalho e à renda. *Agência IBGE Notícias,* 7 jul. 2023. Disponível em: https://agenciadenoticias.ibge.gov.br/agencia-noticias/2012-agencia-de-noticias/noticias/37317-pessoas-com-deficiencia-tem-menor-acesso-a-educacao-ao-trabalho-e-a-renda. Acesso em: 17 abr. 2025.

IBGE. Instituto Brasileiro de Geografia e Estatística. *Censo 2022*. Disponível em: https://censo2022.ibge.gov.br/panorama/. Acesso: 6 jun. 2024.

LEMOS, Ronaldo; SOUZA, Carlos Affonso. *Marco civil da internet:* construção e aplicação. Juiz de Fora: Editar Editora Associada, 2016.

MARIA, Isabela; PICOLO, Cynthia. Autodeterminação informativa: Como esse direito surgiu e como ele me afeta? *Blog do Lapin.* 27 abr. 2021. Disponível em: https://lapin.org.br/2021/04/27/autodeterminacao-informativa-como-esse-direito-surgiu-e-como-ele-me-afeta/ Acesso em: 10 abr. 2025.

KREMER, Bianca. Discriminações do sistema de pontuação de crédito: uma perspectiva de gênero e raça. *In:* OMS, Juliana. *O consumidor na era da pontuação de crédito*. Belo Horizonte: Casa do Direito, 2022.

MARANHÃO, Juliano Souza de Albuquerque; FLORÊNCIO, Juliana Abrusio; ALMADA, Marco. Inteligência artificial aplicada ao direito e o direito da inteligência artificial. *Suprema – Revista de Estudos Constitucionais*, Brasília, v. 1, n. 1, p. 154-180, jan./jun. 2021.

MARSHALL, T. H. *Cidadania e classe social.* São Paulo: Editora Unesp, 2021.

MATSUMI, Hideyuki; SOLOVE, Daniel J., The Prediction *Society:* AI and the Problems of Forecasting the Future (January 24, 2024). GWU Legal Studies Research Paper No. 2023-58. Disponível em: https://ssrn.com/abstract=4453869

MEIRELES, Adriana Veloso. Privacidade no século 21: proteção de dados, democracia e modelos regulatórios. *Revista Brasileira de Ciência Política,* n. 41, p. 1-35, 2023.

MITTELSTADT, Brent Daniel; ALLO, Patrick; TADDEO, Mariarosaria; WATCHER, Sandra; FLORIDI, Luciano. The ethics of algorithms: Mapping the debate. *Big Data and Society,* p. 1-21, jul./dez. 2016.

O'NEIL, Cathy. *Algoritmos de destruição em massa.* Como o big data aumenta a desigualdade e ameaça a democracia. São Paulo: Editora Rua do Sabão, 2020.

O QUE É GDPR e o que muda para as empresas e os brasileiros? 1º abr. 2019. Disponível em: https://hsclabs.com/pt-br/gdpr/. Acesso em: 31 maio 2024.

PEDRA, Caio Benevides. *Direitos LGBT:* a LGBTfobia estrutural e a diversidade de gênero no direito brasileiro. Curitiba: Appris, 2020.

RAMACCIOTTI, Barbara Lucchesi; CALGARARO, Gerson Amauri. Construção do conceito de minorias e o debate teórico no campo do Direito. *Sequência,* Florianópolis, v. 42, n. 89, p. 1-30, 2021.

RAMOS, Marcelo Maciel; NICOLI, Pedro Augusto Gravatá. O que é LGBTfobia? *In:* RAMOS, Marcelo Maciel; NICOLI, Pedro Augusto Gravatá; BRÊNER, Paula Rocha Gouvêa. (org.). *Gênero, sexualidade e direito:* uma introdução. Belo Horizonte: Initia Via, 2016. p. 183-192.

SÉGUIN, Elida. *Minorias e grupos vulneráveis:* uma abordagem jurídica. Rio de Janeiro: Forense: Imprenta, 2002. p. 252.

SILVEIRA, Rebecca Costa Gadelha da; FREITAS, Raquel Coelho de. Definindo minorias: desafios, tentativas e escolhas para se estabelecer critérios mínimos rumo à conceituação de grupos minoritários. *Revista de Teoria e Filosofia do Estado,* v. 3, n. 2, p. 95-116, 2017.

SIQUEIRA, D. P.; CASTRO, L. R. B. Minorias e grupos vulneráveis: a questão terminológica como fator preponderante para uma real inclusão social. *Revista Direitos Sociais e Políticas Públicas,* Unifafibe, [*S. l.*], v. 5, n. 1, p. 105-122, 2017. DOI: 10.25245/rdspp.v5i1.219. Disponível em: https://portal.unifafibe.com.br:443/revista/index.php/direitos-sociais-politicas-pub/article/view/219. Acesso em: 13 abr. 2025.

AMPARO, Thiago; PRADO, Viviane Muller. Racismo creditício no Brasil e nos EUA: risco discriminatório no acesso a crédito. *Revista Direito GV,* São Paulo, v. 20, e2422, 2024. DOI: https://doi.org/10.1590/23176172202422

WU, Tim. *The attention merchants*. New York: Knopf, 2016.

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

ZUBOFF, Shoshana. *The age of Surveillance Capitalism.* Nova York: Public Affairs, 2019.

Autor Correspondente
Juliana Abrusio Florencio
Universidade Presbiteriana Mackenzie
R. da Consolação, 930 – Consolação, São Paulo/SP, Brasil. CEP 01302-907
juliana.abrusio@mackenzie.br