IV SEMANA DA DEMOGRAFIA

DEMOGRAFIA DOS INVISIBILIZADOS: FORTALECENDO PRESENÇAS QUE ESCAPAM

UNICAMP – 06 a 10 de abril de 2026

RACISMO ALGORÍTMICO E VIESES EM TECNOLOGIAS DE RECONHECIMENTO FACIAL: UMA ANÁLISE À LUZ DA LGPD

Daniel Santos do Nascimento[1]

RESUMO

O avanço das tecnologias de vigilância biométrica no Brasil tem suscitado debates urgentes acerca da tensão entre a eficiência na segurança pública e a preservação de garantias fundamentais. O presente trabalho analisa o fenômeno do racismo algorítmico operado por sistemas de reconhecimento facial, sob o prisma da Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018). O problema de pesquisa investiga em que medida a opacidade dos algoritmos de inteligência artificial e os vieses presentes nos bancos de dados de treinamento violam o princípio da não-discriminação e o devido processo legal. O objetivo principal é demonstrar que a neutralidade tecnológica é um mito e que a implementação acrítica dessas ferramentas reproduz desigualdades raciais históricas, configurando uma nova faceta da necropolítica. Para tanto, utiliza-se o método hipotético-dedutivo, operacionalizado por meio de revisão bibliográfica transdisciplinar, articulando a dogmática jurídica de proteção de dados com a Teoria Crítica da Tecnologia e a Criminologia. Os resultados indicam que o tratamento de dados biométricos sensíveis, sem salvaguardas robustas e transparência auditável (explicação algorítmica), fere frontalmente o Artigo 6º, inciso IX da LGPD. Conclui-se pela necessidade de uma interpretação proativa da legislação, que imponha Relatórios de Impacto à Proteção de Dados (RIPD) rigorosos, visando impedir que a inovação tecnológica sirva como instrumento de amplificação da seletividade penal contra a população negra.

Palavras-chave: Racismo algorítmico; Reconhecimento facial; LGPD; Proteção de dados sensíveis; Discriminação tecnológica.

INTRODUÇÃO

A contemporaneidade é marcada pela transição de uma sociedade disciplinar para uma sociedade de controle, onde os mecanismos de vigilância deixaram de ser apenas físicos e arquitetônicos para se tornarem ubíquos, digitais e algorítmicos. Neste cenário, a Inteligência Artificial (IA) e, especificamente, as tecnologias de reconhecimento facial, assumiram um protagonismo central nas políticas de segurança pública e no controle de acesso privado. Contudo, a disseminação dessas ferramentas ocorre sob a égide de um tecnossolucionismo que

[1] Universidade Federal de Pernambuco – UFP. E-mail: danielsantos222005@gmail.com

promete objetividade matemática, mas que, na prática, encobre a reprodução de hierarquias sociais preexistentes.

O problema central deste estudo reside no descompasso entre a capacidade de processamento de dados biométricos e as garantias de isonomia. A literatura especializada aponta que algoritmos de reconhecimento facial apresentam taxas de erro significativamente superior quando aplicados a rostos de pessoas negras, especialmente mulheres negras. Esse fenômeno, longe de ser uma falha técnica isolada, revela o que se convencionou chamar de racismo algorítmico. Diante disso, emerge a questão jurídica fundamental: como a Lei Geral de Proteção de Dados (LGPD) pode atuar como barreira de contenção contra o uso discriminatório de tecnologias biométricas considerando a opacidade inerente às "caixas-pretas" (*black boxes*) desses sistemas?

A relevância deste trabalho é, a um só tempo, social e jurídica. Socialmente, justifica-se pela urgência em denunciar e compreender os mecanismos que têm levado à prisão injusta de cidadãos negros baseadas exclusivamente em correspondências algorítmicas falhas, evidenciando uma atualização tecnológica da seletividade penal brasileira. Academicamente, o estudo se insere na intersecção necessária entre o Direito Digital, a Criminologia Crítica e a Sociologia, preenchendo lacunas sobre a aplicabilidade prática dos princípios de proteção de dados em cenários de alta complexidade técnica. Ademais, justifica-se pela necessidade de fortalecer a cultura de proteção de dados sensíveis no Brasil superando a visão meramente burocrática da conformidade (*compliance*) em favor de uma justiça sociotécnica.

O objetivo geral é analisar a compatibilidade do uso de tecnologias de reconhecimento facial com os princípios norteadores da LGPD, especificamente o da não-discriminação. Como objetivos específicos, pretende-se:

- Conceituar o racismo algorítmico e suas manifestações na arquitetura das redes neurais e nos dados de treinamento;
- Examinar o regime jurídico dos dados pessoais sensíveis (biométricos) na LGPD e as hipóteses legais de seu tratamento;

- Investigar os limites e as possibilidades do direito à explicação e à revisão de decisões automatizadas (Art. 20 da LGPD) como instrumentos de combate ao viés racial.

A fundamentação teórica deste estudo alicerça-se em três eixos. No eixo da Sociologia da Tecnologia, Ruha Benjamin (2019) oferece o conceito de "New Jim Code", argumentando que as inovações tecnológicas podem reforçar sistemas de discriminação racial sob o disfarce de neutralidade e progresso. A autora demonstra como o design tecnológico codifica preconceitos históricos. No contexto brasileiro, Tarcízio Silva (2022) é a referência central para compreender o racismo algorítmico não como erro, mas como funcionalidade de sistemas desenvolvidos em sociedades racistas. O autor explicita como a branquitude normativa molda os bancos de dados, tornando a tecnologia hostil a corpos negros. No eixo jurídico, Danilo Doneda (2019) e Laura Schertel Mendes (2021) fornecem a base dogmática sobre a proteção de dados. Doneda (2019) alerta para os riscos da perfilização e a necessidade de que a proteção de dados vá além da privacidade individual, alcançando a tutela contra discriminações coletivas. Já Cathy O'Neil (2021) contribui com a crítica aos modelos matemáticos opacos que ela denomina Armas de Destruição Matemática, pela sua capacidade de escalar desigualdades sem responsabilização clara. Por fim, dialoga-se com a biopolítica de Michel Foucault (1999) e a necropolítica de Achille Mbembe (2018) para situar o reconhecimento facial como uma ferramenta de gestão da morte e da vida de populações vulneráveis.

MATERIAIS E MÉTODOS

Para o desenvolvimento deste resumo expandido, adota-se o método hipotético-dedutivo. Parte-se da premissa maior de que todo artefato tecnológico produzido em uma sociedade desigual carrega consigo os vieses de seus criadores e dos dados que o alimentam. A partir disso, deduz-se que a aplicação acrítica do reconhecimento facial no Brasil tende a violar os direitos fundamentais da população negra, testando essa hipótese frente ao ordenamento jurídico pátrio.

A abordagem do problema é qualitativa, visando compreender a complexidade das relações entre tecnologia, raça e direito, sem se limitar à análise quantitativa de dados, mas focando na interpretação dos fenômenos sociais e jurídicos.

Quanto aos procedimentos técnicos, utiliza-se a pesquisa bibliográfica e documental. A pesquisa documental foca na análise da legislação pertinente, especificamente a Constituição Federal de 1988 e a Lei nº 13.709/2018 (Lei Geral de Proteção de Dados Pessoais). A pesquisa bibliográfica abrange a leitura e fichamento de obras de referência nos campos do Direito Digital, Direitos Humanos, Filosofia da Tecnologia e Teoria Crítica Racial. Foram selecionados doutrinadores nacionais e estrangeiros que tratam da governança algorítmica, da ética de dados e do racismo estrutural, permitindo uma análise transdisciplinar que o tema exige. A coleta de dados teóricos priorizou publicações recentes (últimos 10 anos) para garantir a atualidade do debate frente à rápida obsolescência tecnológica.

RESULTADOS E DISCUSSÃO

É imperativo iniciar esta análise desconstruindo o mito da neutralidade tecnológica. Ao contrário do senso comum que enxerga no algoritmo uma ferramenta matemática pura e imune às paixões humanas, a sociologia digital revela que as tecnologias são produtos culturais que carregam os valores, visões de mundo e preconceitos de seus criadores. Conforme argui Tarcízio Silva (2022), a opacidade dos sistemas automatizados serve muitas vezes como um véu que encobre a manutenção de hierarquias raciais, transformando o preconceito velado em decisão técnica.

No caso específico do reconhecimento facial, o viés se manifesta primariamente na etapa de treinamento das redes neurais. Os algoritmos aprendem a identificar rostos processando milhões de imagens pré-existentes. Ocorre que, como demonstrado por Joy Buolamwini e Timnit Gebru (2018) em seu estudo seminal “Gender Shades”, os bancos de dados (*datasets*) utilizados globalmente são compostos majoritariamente por indivíduos brancos e do sexo masculino. Ao treinar a inteligência artificial com uma amostra não

representativa da diversidade humana, cria-se uma branquitude normativa codificada. O resultado é que a máquina desenvolve uma alta acurácia para identificar homens brancos, mas falha drasticamente – confundindo, invisibilizando ou criminalizando – rostos de mulheres negras. Não se trata, portanto, de um erro aleatório, mas de uma negligência sistêmica no design da tecnologia.

À luz da Lei Geral de Proteção de Dados (Lei nº 13.709/2018), a face humana é inequivocamente classificada como dado pessoal sensível quando utilizada para fins de identificação inequívoca, conforme o Artigo 5º, inciso II. Essa categorização não é trivial; ela impõe um regime de proteção mais rigoroso, restringindo as hipóteses legais de tratamento elencadas no Artigo 11. Entretanto, a mera legalidade do tratamento (por exemplo, sob a justificativa de segurança pública ou proteção da vida) não isenta o controlador de observar os princípios basilares da lei.

O ponto fulcral desta discussão reside no Artigo 6º, inciso IX da LGPD, que estabelece o princípio da não-discriminação. O dispositivo veda expressamente a realização de tratamento para fins discriminatórios, ilícitos ou abusivos. A interpretação deste artigo, em consonância com a doutrina de Danilo Doneda (2019) deve ser orientada pelo resultado, e não apenas pela intenção. Mesmo que o Estado ou uma empresa de segurança privada não tenha a *intenção* direta de discriminar pessoas negras, se a ferramenta utilizada, ou seja, o algoritmo enviesado produz resultados que segregam, constrangem ou punem desproporcionalmente um grupo racial, há uma violação flagrante da LGPD. A responsabilidade, neste cenário, deve ser objetiva, visto que o risco da atividade de processamento de dados sensíveis foi assumido pelo controlador.

A LGPD tentou antecipar os problemas da automação através do seu Artigo 20, que garante ao titular dos dados o direito a solicitar a revisão de decisões tomadas unicamente com base em tratamento automatizado. Contudo, a eficácia prática deste dispositivo é severamente limitada pelo fenômeno da “Caixa-Preta” (*Black Box*). Como alerta Frank Pasquale (2015),

vivemos em uma sociedade onde os algoritmos que decidem oportunidades de vida (crédito, emprego, liberdade) são protegidos por segredo industrial e complexidade técnica inacessível.

No contexto do reconhecimento facial aplicado à segurança pública, a revisão humana prevista na lei enfrenta dois obstáculos intransponíveis sem uma regulação complementar. Primeiro, a opacidade: como o advogado de defesa pode questionar a decisão da máquina de identificar seu cliente como um criminoso, se o funcionamento interno da rede neural não é auditável? Segundo o viés de automação (*automation bias*), Cathy O'Neil (2021) aponta que os operadores humanos tendem a confiar cegamente na precisão matemática da máquina. Assim, a revisão humana torna-se, na prática, uma mera ratificação burocrática do erro algorítmico. Sem a obrigatoriedade de uma explicabilidade robusta e compreensível, o Artigo 20 torna-se uma garantia esvaziada.

Por fim, é impossível dissociar o debate técnico do contexto criminológico brasileiro. A introdução do reconhecimento facial massivo nas cidades brasileiras dialoga diretamente com o conceito de necropolítica de Achille Mbembe (2018), onde o poder soberano se manifesta na capacidade de ditar quem pode viver e quem deve morrer ou ser encarcerado.

Ao aplicar uma tecnologia comprovadamente falha contra populações negras em um sistema de justiça criminal já historicamente seletivo, o Estado automatiza a suspeição. A tecnologia não apenas reproduz o racismo; ela o escala e lhe confere uma aura de legitimidade científica. O reconhecimento facial atua, assim, como um mecanismo de biopolítica digital, gerindo os corpos no espaço urbano e retirando a cidadania da população negra através da vigilância constante e do erro sistemático. A LGPD, portanto, não deve ser lida apenas como uma norma de regulação de mercado, mas como um instrumento de defesa da dignidade da pessoa humana contra a violência algorítmica estatal.

CONSIDERAÇÕES FINAIS

A análise empreendida neste estudo permite concluir que a implementação de tecnologias de reconhecimento facial no Brasil, no atual estágio de desenvolvimento técnico e

regulatório, representa uma ameaça concreta aos direitos fundamentais da população negra, configurando uma violação sistemática dos princípios basilares da Lei Geral de Proteção de Dados (LGPD).

Restou demonstrado que a neutralidade algorítmica é um mito perigoso. A transposição de vieses sociais para o código-fonte transforma ferramentas de segurança em instrumentos de discriminação automatizada. A alta taxa de falha na identificação de faces negras, aliada à opacidade das caixas-pretas, inviabiliza o exercício pleno do contraditório e da ampla defesa, esvaziando a garantia de revisão humana prevista no Artigo 20 da LGPD. O dispositivo legal, embora bem-intencionado, mostra-se insuficiente diante da complexidade das redes neurais e da falta de auditabilidade pública dos sistemas.

Portanto, conclui-se que o cumprimento da LGPD exige mais do que conformidade burocrática; exige uma Justiça de Design. É imperioso que a Autoridade Nacional de Proteção de Dados (ANPD) e o Poder Judiciário adotem uma postura rígida, considerando ilegal qualquer tratamento de dados biométricos sensíveis que não comprove, mediante Relatórios de Impacto à Proteção de Dados Pessoais (RIPD) auditáveis, a eliminação de vieses raciais. Sugere-se, em última análise, a necessidade de debater moratórias ao uso dessas tecnologias na segurança pública até que se garantam taxas de acerto equitativas, impedindo que a inovação tecnológica sirva à manutenção de uma necropolítica que gere a morte civil e a exclusão social de grupos historicamente vulnerabilizados.

REFERÊNCIAS

BENJAMIN, Ruha. **Race after technology:** abolitionist tools for the new Jim Code. Medford: Polity Press, 2019.

BRASIL. Presidência da República. Secretaria-Geral. **Lei nº 13.709, de 14 de agosto de 2018.** Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF, 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 23 jan. 2026.

BUOLAMWINI, Joy; GEBRU, Timnit. Gender shades: intersectional accuracy disparities in commercial gender classification. **Proceedings of Machine Learning Research,** New York, NY, v. 81, p. 77-91, 2018.

DONEDA, Danilo. **Da privacidade à proteção de dados pessoais.** 2. ed. Rio de Janeiro, RJ: Renovar, 2019.

FOUCAULT, Michel. **Em defesa da sociedade:** curso no Collège de France (1975-1976). São Paulo, SP: Martins Fontes, 1999.

MBEMBE, Achille. **Necropolítica.** 3. ed. São Paulo, SP: N-1 Edições, 2018.

MENDES, Laura Schertel. **Privacidade, proteção de dados e defesa do consumidor:** linhas gerais de um novo direito fundamental. São Paulo, SP: Saraiva Educação, 2021.

O'NEIL, Cathy. **Algoritmos de destruição em massa:** como o big data aumenta a desigualdade e ameaça a democracia. Tradução de: Rafael Abraham. Santo André, SP: Editora Rua do Sabão, 2021.

PASQUALE, Frank. **The black box society:** the secret algorithms that control money and information. Cambridge: Harvard University Press, 2015.

SILVA, Tarcízio. **Racismo algorítmico:** inteligência artificial e discriminação nas redes digitais. São Paulo, SP: Edições Sesc São Paulo, 2022.

SILVEIRA, Sérgio Amadeu. **Tudo sobre tod@s:** redes digitais, privacidade e venda de dados pessoais. São Paulo, SP: Edições Sesc São Paulo, 2019.