REVISTA MUNDO EM MOVIMENTO
Uninassau - Caruaru
2(1): 249-261, 2025
ISSN: 2966-2176

TECNOLOGIA E A VIOLAÇÃO DA ISONOMIA: O RECONHECIMENTO FACIAL COMO AMEAÇA ESTRUTURAL À TUTELA DO DIREITO À NÃO-DISCRIMINAÇÃO

TECHNOLOGY AND THE VIOLATION OF EQUALITY: FACIAL RECOGNITION AS A STRUCTURAL THREAT TO THE PROTECTION OF THE RIGHT TO NON-DISCRIMINATION

Emanuelly Ignez Alves Silva
Graduanda em Bacharelado em Direito – UNINASSAU/Caruaru. E-mail: manulvs44@gmail.com

Alan Rodrigo Alves da Cruz
Advogado, Professor na Uninassau Caruaru e Especialista em Direito penal e Processo Penal pela Escola Superior da Advocacia (ESA). Email: advalancruz@gmail.com

RESUMO: A propagação de fake news com conteúdo calunioso é uma das maiores ameaças da era digital, impactando diretamente a honra, a reputação e a vida de indivíduos. No Brasil, o crime de calúnia está tipificado no artigo 138 do Código Penal, que prevê punição para quem imputar falsamente a alguém um fato definido como crime. No entanto, a velocidade e o alcance proporcionados pelas redes sociais tornam o combate a essa prática mais complexo, levantando questionamentos sobre a eficácia da legislação vigente. O presente artigo analisa como o Código Penal e o Marco Civil da Internet (Lei nº 12.965/2014) abordam a questão da calúnia digital

e os desafios enfrentados pela jurisprudência brasileira. Através de uma análise crítica das jurisprudências recentes do Superior Tribunal de Justiça (STJ) e de casos emblemáticos, como o da vereadora Marielle Franco, este trabalho avalia a efetividade dos mecanismos legais e sugere mudanças necessárias para aprimorar a proteção das vítimas. Além disso, são discutidas as propostas de reforma legislativa que incluem o agravamento das penas para crimes de calúnia na internet e a ampliação da responsabilidade das plataformas digitais.

PALAVRAS-CHAVE: Calúnia Digital, Fake News, Crimes Contra a Honra, Legislação Brasileira, Marco Civil da Internet.

ABSTRACT: The spread of fake news with defamatory content is one of the greatest threats of the digital age, directly impacting the honor, reputation, and lives of individuals. In Brazil, the crime of defamation is defined in Article 138 of the Penal Code, which provides punishment for anyone who falsely imputes a fact defined as a crime to someone. However, the speed and reach provided by social networks make combating this practice more complex, raising questions about the effectiveness of current legislation. This article analyzes how the Penal Code and the Brazilian Internet Bill of Rights (Law No. 12.965/2014) address the issue of digital defamation and the challenges faced by Brazilian jurisprudence. Through a critical analysis of recent case law from the Superior Court of Justice (STJ) and emblematic cases, such as that of councilwoman Marielle Franco, this work evaluates the effectiveness of legal mechanisms and suggests necessary changes to improve the protection of victims. Furthermore, legislative reform proposals are discussed, including harsher penalties for online defamation crimes and increased liability for digital platforms.

KEYWORDS: Digital Defamation, Fake News, Crimes Against Honor, Brazilian Legislation, Marco Civil da Internet (Brazilian Internet Bill of Rights).

1. INTRODUÇÃO

A inserção da Inteligência Artificial (IA) nas esferas de segurança pública tem sido notável, impulsionada por uma promessa de eficiência e objetividade no combate ao crime. Contudo, essa crescente algoritmização do controle social, em vez de eliminar os vieses, tem automatizado e amplificado preconceitos históricos, materializando o que a literatura especializada denomina Racismo Algorítmico (SILVA, 2022). As Tecnologias de Reconhecimento Facial (TRF) representam o vetor mais crítico dessa problemática, uma vez que operam sobre o dado biométrico, um dado pessoal sensível, em um ambiente social profundamente marcado por desigualdades raciais. A falácia da neutralidade técnica é refutada pela perspectiva de autores como Andrew Feenberg (2017), que, pela ótica da Teoria Crítica da Tecnologia e dos Estudos Sociais em Ciência e Tecnologia (STS), argumenta que a tecnologia é um artefato socialmente construído, carregado de relações de poder e, portanto, incapaz de ser isento de valores em sua aplicação prática. A urgência de submeter a TRF a uma análise jurídica e social rigorosa decorre, assim, da necessidade de confrontar a celebração acrítica da eficiência tecnológica com a defesa intransigente dos direitos fundamentais.

O presente estudo sustenta a tese de que a adoção indiscriminada da TRF constitui uma ameaça estrutural e direta à tutela da isonomia prevista na Constituição Federal, indo além da mera falha pontual. A aplicação dessas ferramentas por órgãos de segurança reflete e amplifica os vieses de raça e classe que, conforme a Teoria Crítica da Raça (TCR), estruturam o sistema penal (OLIVEIRA; ALVES-BRITO; ROSA, 2024). Essa codificação

de preconceitos se manifesta de forma evidente na Desigualdade Algorítmica Racial, onde os sistemas são programados para serem mais ineficazes e, consequentemente, mais opressivos, contra populações não brancas. No Brasil, essa vigilância automatizada e seletiva se alinha à lógica da Necropolítica (MBEMBE, 2016), configurando-se como uma estratégia de gestão populacional que concentra a penalização, o risco e, em última instância, a morte social e física em corpos racializados e periféricos. Assim, o Judiciário e o arcabouço legal se veem desafiados a estabelecer limites ao poder punitivo que se traveste de inovação tecnológica.

2. MARCO TEÓRICO: VIÉS, ESTRUTURA E OPACIDADE

A ascensão da vigilância automatizada exige que o Direito abandone a crença na neutralidade técnica e mergulhe nos fundamentos da crítica social e da criminologia. A análise dos riscos da TRF deve ser ancorada em um sólido referencial teórico que demonstre como a IA herda e amplifica as mazelas sociais, em flagrante violação dos direitos humanos. As seções a seguir exploram os pilares conceituais que desvendam a falácia da objetividade algorítmica e comprovam a incompatibilidade do reconhecimento facial com o sistema de garantias.

2.1. O Princípio da isonomia e a tutela do direito à não-discriminação

O sistema jurídico brasileiro, sob a égide da Constituição Federal de 1988, elege o princípio da isonomia (Art. 5º, *caput*) e o direito fundamental à não-discriminação (Art. 3º, IV) como pilares inegociáveis. Essa exigência

transcende a mera igualdade formal perante a lei, demandando uma igualdade material que obriga o Estado a neutralizar as desigualdades estruturais existentes e, principalmente, de abster-se de qualquer conduta que possa perpetuar a exclusão social. O avanço das Tecnologias de Reconhecimento Facial (TRF), ao prometerem objetividade, iludem o Judiciário e a segurança pública com a ideia de que a máquina superará a subjetividade humana e os vieses policiais; no entanto, a eficácia desse sistema de vigilância é diretamente confrontada com a realidade estrutural do racismo brasileiro, conforme atestam os dados de super-vigilância e seletividade penal contra a população negra. A tecnologia, inserida nesse contexto de desigualdade histórica, demonstra-se incapaz de promover a justiça sem primeiro ser purificada dos vieses que herdou da sociedade que a criou.

A coleta e o tratamento de dados pessoais sensíveis, como a biometria facial, impõem ao Estado um dever de cautela máxima, conforme preconiza a Lei Geral de Proteção de Dados (LGPD) (BRASIL, 2018). A TRF lida com características identitárias de origem racial, e seu uso negligente coloca em risco a própria dignidade da pessoa humana (Art. 1º, III, CF/88), transformando atributos pessoais em vetores de discriminação e controle. Essa vulnerabilidade é acentuada porque o sistema de justiça, ao utilizar um artefato tecnológico que opera com taxas de erro desproporcionais contra um grupo racial específico, intensifica a desconfiança e a exclusão jurídica dessa população. A isonomia constitucional é violada quando o Estado utiliza um sistema que, comprovadamente, opera com taxas de erro desproporcionais contra um grupo racial específico, intensificando a desconfiança e a vulnerabilidade jurídica dessa população, o que exige a intervenção imediata do arcabouço legal.

A Teoria Crítica da Raça (TCR), ao analisar essa dinâmica, argumenta que o racismo é estrutural e sistêmico, não se limitando a atos individuais, mas permeando as instituições e o próprio Direito, o que resulta na definição de Racismo Algorítmico. O algoritmo se torna, assim, o braço tecnológico dessa opressão, promovendo uma ordenação racializada de classificação social e violência em detrimento de grupos minorizados (OLIVEIRA; ALVES-BRITO; ROSA, 2024). Essa vigilância automatizada e seletiva se alinha diretamente à lógica da Necropolítica (MBEMBE, 2016), configurando-se como uma estratégia de gestão populacional que concentra a penalização, o risco e a super-vigilância em corpos racializados e periféricos. Essa codificação de preconceitos se manifesta de forma evidente na Desigualdade Algorítmica Racial, onde os sistemas são programados para serem mais ineficazes e, consequentemente, mais opressivos, contra populações não brancas.

2.2. A Crítica da tecnologia e a violação do devido processo legal

Para compreender o porquê de um sistema supostamente lógico falhar de forma tão enviesada, é fundamental recorrer aos Estudos Sociais em Ciência e Tecnologia (STS) e à Teoria Crítica da Tecnologia de Andrew Feenberg (2017). Feenberg sustenta que a tecnologia não é um dado pré-existente e neutro, mas um artefato socialmente construído, carregado de escolhas e relações de poder. A falha do algoritmo não é um *bug* técnico isolado, mas uma falha de design social que reflete os dados de treinamento enviesados e as prioridades dos desenvolvedores (SILVA, 2022). A opacidade inerente aos sistemas de *machine learning* (a *black box*) impede que se conheça a ponderação exata dos fatores que resultaram na

identificação. Essa insindicabilidade algorítmica viola o direito à fundamentação das decisões (Art. 93, IX, CF/88) e compromete o Devido Processo Legal (Art. 5º, LIV).

A ausência de transparência não é um mero inconveniente técnico; é um bloqueio jurídico que impede a realização da justiça, transformando a IA em uma "caixa-preta" que impede a prestação de contas (*accountability*) (SILVA, 2019). O exemplo mais evidente da codificação seletiva foi encontrado na análise do edital original do projeto *Smart Sampa* em São Paulo. O documento inicial exigia que o sistema de vigilância fosse capaz de monitorar e emitir alertas para "situações de vadiagem" (OLIVEIRA; FAGUNDES; SPOLLE, 2025). Essa exigência não é um mero erro de vocabulário; é uma reminiscência direta da Lei de Contravenções de 1941, utilizada historicamente para criminalizar e perseguir a população negra e pobre pós-abolição, provando que o Direito deve atuar sobre a origem dos dados e sobre os padrões de poder que orientam o desenvolvimento dos algoritmos.

A violação do Devido Processo Legal é completa quando a defesa não pode contraditar ou inspecionar o código que determinou a suspeita ou a prisão (Art. 5º, LV), o que torna a decisão incontrolável e ilegítima. A crítica da tecnologia exige que o Judiciário atue sobre a origem dos dados e sobre os padrões de poder que orientam o desenvolvimento dos algoritmos, em vez de apenas reagir aos seus danos na ponta final do processo. A ausência de transparência e auditabilidade permite que o Racismo Algorítmico se perpetue sob o manto da legalidade, exigindo que o arcabouço normativo estabeleça mecanismos de controle que obriguem o Estado a justificar cientificamente e eticamente a utilização de sistemas que demonstram taxas de erro racialmente enviesadas.

3. VIGILÂNCIA AUTOMATIZADA E O RACISMO ALGORÍTMICO

A etapa de discussão é o coração do artigo, onde a tese crítica sobre a falácia da neutralidade algorítmica é comprovada por meio de dados e estudos empíricos. A realidade da implementação da TRF no Brasil, regida pela Desigualdade Algorítmica Racial, revela-se um instrumento de policiamento enviesado que concentra a super-vigilância em corpos racializados, aprofundando o encarceramento seletivo.

3.1. Disparidade de desempenho, falso positivo e a necropolítica

A premissa de objetividade da TRF é destituída de validade pelos dados de desempenho técnico, que atestam a falha de engenharia social do sistema ao discriminar. O algoritmo, ao ser treinado com bases de dados que não representam a diversidade, manifesta taxas de erro significativamente maiores para grupos minorizados, confirmando que a tecnologia herda o viés de raça e classe. O Centro de Estudos de Segurança e Cidadania (CESEC) revelou um dado estatístico inquestionável: 90,5% das pessoas presas por monitoramento facial no Brasil eram negras (CESEC, 2019). Este dado, alarmante por sua seletividade, não reflete a criminalidade em sua totalidade, mas sim o foco operacional da vigilância estatal, comprovando a eficácia do sistema em localizar, identificar e penalizar grupos historicamente marginalizados, traduzindo o Racismo Algorítmico em encarceramento seletivo (MELO, 2024).

A interpretação desses dados é indissociável da Necropolítica (MBEMBE, 2016), que atesta como o racismo de Estado atua na gestão da

morte e da vida, concentrando a penalização em corpos racializados. A TRF não busca a justiça universal, mas sim a validação de suspeitas pré-existentes do policiamento ostensivo. Ao criar um círculo vicioso de vigilância e erro (o algoritmo é treinado com dados enviesados e, ao ser aplicado, gera mais prisões enviesadas, que alimentam o sistema), o algoritmo transforma a injustiça histórica em uma predição supostamente objetiva. A falha técnica, portanto, materializa-se em violência institucional ao concentrar a penalização onde o viés histórico já atuava, o que é um indicador direto da ameaça estrutural à isonomia.

A disparidade é ainda mais evidente quando comparada globalmente, como demonstram os estudos do MIT (Massachusetts Institute of Technology). As margens de erro do reconhecimento facial são dramaticamente diferentes de acordo com a cor da pele e o gênero: a taxa de erro chega a 34% no caso de mulheres negras, contrastando com apenas 0,8% para homens brancos (BUOLAMWINI; GEBRU, 2018 *apud* MELO, 2024). A alta taxa de falso positivo em desfavor da população negra comprova que a vulnerabilidade imposta pela TRF é uma questão de design social, e não de acaso. Essa falha de engenharia social é o cerne da seletividade penal, que submete indivíduos inocentes a abordagens indevidas e prisões ilegais, violando o direito à liberdade e o devido processo legal em nome de uma eficiência algorítmica comprovadamente racista.

3.2. Casos emblemáticos, falso positivo e a construção do inimigo público

Os casos concretos de erro do sistema preditivo demonstram que o risco não é teórico, mas uma violação direta da liberdade e da dignidade da

pessoa humana. A urgência da questão é reforçada pela análise da criminalização histórica subjacente ao uso da TRF. O artigo de Paulo Victor Melo (2024) atesta que o edital original do projeto *Smart Sampa* em São Paulo exigia a monitoração de "situações de vadiagem". Essa exigência não é um mero erro de vocabulário; é uma reminiscência direta da Lei de Contravenções de 1941, utilizada historicamente para criminalizar e perseguir a população negra e pobre pós-abolição. A tecnologia, ao invés de buscar a modernidade, foi conscientemente direcionada para o controle de um perfil social pré-definido como "suspeito".

A materialização dessa injustiça se dá através de casos de falso positivo com alto impacto social e jurídico. O G1 Bahia noticiou o caso de um homem negro inocente detido por 26 dias após ser identificado erroneamente pelo sistema de reconhecimento facial, com o próprio órgão de segurança afirmando 95% de similaridade (G1, 2023). De forma semelhante, o Rede Brasil de Fato relatou o caso de Danilo Félix no Rio de Janeiro, um jovem negro que foi preso e inocentado múltiplas vezes por erro de identificação (REDE BRASIL DE FATO, 2023). Estes eventos atestam que a tecnologia opera com um alto índice de falso positivo em detrimento de uma população específica, resultando em prisões indevidas e no aprofundamento do estigma.

A gravidade do problema transcende o erro individual e atinge o Direito Penal do Inimigo (JAKOBS, 2012). A conexão explícita entre a tecnologia de vigilância e a legislação arcaica de controle social, como a da vadiagem, comprova que a TRF não é apenas uma ferramenta neutra; ela é um instrumento de legitimação para padrões opressivos sob a roupagem da inovação. Desta forma, a vigilância algorítmica revela-se uma ameaça estrutural ao comprometer a promessa constitucional de igualdade material

(Art. 5º, *caput*, CF/88), exigindo uma intervenção regulatória que trate a TRF não como uma ferramenta de segurança, mas como um risco à tutela da liberdade e da isonomia.

CONCLUSÕES

A análise crítica da aplicação das Tecnologias de Reconhecimento Facial (TRFs) no Brasil demonstra, de forma categórica, que a tecnologia, longe de ser um instrumento neutro de segurança, é um vetor de Racismo Algorítmico que aprofunda a exclusão e a violência do Estado. O uso indiscriminado e não regulamentado da TRF desestabiliza a própria fundação da igualdade (Art. 5º, *caput*, CF/88), pois opera com um viés estatisticamente comprovado que penaliza a população negra com taxas desproporcionais de falso positivo e vigilância massiva (CESEC, 2019; MELO, 2024). A TRF, ao transformar o estigma social em categoria jurídica de risco (MBEMBE, 2016), impõe uma barreira tecnológica ao acesso à justiça, violando as garantias do Devido Processo Legal. A urgência do debate reside no fato de que esta prática configura uma nova modalidade de discriminação institucional incompatível com os pilares do Estado Democrático de Direito, e esta violação sistêmica não pode ser remediada por simples advertências aos órgãos de segurança.

É imperativo que a regulamentação ética e técnica no Brasil avance para além de medidas paliativas, estabelecendo uma intervenção regulamentar e política que aborde a raiz do problema. O arcabouço normativo deve urgentemente incorporar a auditabilidade (para a fiscalização da LGPD) e o Direito à Explicação como garantias processuais essenciais contra o viés algorítmico. A solução técnica para a opacidade

reside na Inteligência Artificial Explicável (XAI), que visa converter o algoritmo opaco (*black box*) em um modelo auditável, permitindo que a defesa e o Judiciário compreendam e contestem a origem do viés em cada identificação (STELMASHCHUK, 2023). Portanto, é crucial a adoção de padrões rigorosos de *accountability* e precisão equitativa, exigindo que nenhuma restrição de direitos (prisão, abordagem ou investigação) seja baseada unicamente no *score* ou na identificação gerada pelo algoritmo. O direito à não-discriminação (Art. 3º, IV, CF/88) e o princípio da dignidade da pessoa humana impõem que a tecnologia sirva à inclusão social, e não à automatização da exclusão.

REFERÊNCIAS

BRASIL. (2018). **Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais**. Diário Oficial da União, Brasília, DF, 15 ago. 2018.

CESEC - CENTRO DE ESTUDOS DE SEGURANÇA E CIDADANIA. (2019). **Levantamento revela que 90,5% dos presos por monitoramento facial no Brasil são negros**. Rio de Janeiro: CESEC.

FEENBERG, A. (2017). Critical theory of technology and STS (Teoria Crítica da Tecnologia e STS). **Theory, Culture & Society**, *34*(1), 3–24.

INOV(AÇÃO): DISCRIMINAÇÃO ALGORÍTMICA RACIAL E AS INTELIGÊNCIAS ARTIFICIAIS NO BRASIL. (2023). **Revista do Centro Acadêmico Afonso Pena**, *28*(2).

G1. (2023, 01 de setembro). **Com mais de mil prisões na BA, sistema de reconhecimento facial é criticado por 'racismo algorítmico'; inocente ficou preso por 26 dias.** G1 Bahia.

MBEMBE, A. (2016). Necropolítica. **Arte & ensaios Revista do PPGAV**, *32*(1), 123-151.

MELO, P. V. (2024). Para quais rostos as câmeras apontam? Resistências à banalização institucional do reconhecimento facial no Brasil. **Contemporânea: Revista de Comunicação e Cultura**, *22*(1).

REDE BRASIL DE FATO. (2023, 06 de outubro). *RJ:* **Jovem negro acusado por reconhecimento facial é inocentado pela terceira vez**. Brasil de Fato.

OLIVEIRA, C. B., FAGUNDES, M. C. F., & SPOLLE, M. V. (2025). Racismo digital e gestão populacional: uma análise sobre câmeras com reconhecimento facial. **Revista da Mesaco**, *17*(27).

OLIVEIRA, A. C. de, ALVES-BRITO, A., & ROSA, K. D. (2024). Uma revisão de literatura sobre a teoria crítica da raça na educação científica. **Investigações em Ensino de Ciências**, *29*(1), 23.

SILVA, T. (2022). **Racismo Algorítmico: inteligência artificial e discriminação nas redes digitais**. São Paulo: Edições Sesc São Paulo.