INTELIGÊNCIA ARTIFICIAL E DISCRIMINAÇÃO: DESAFIOS E PERSPECTIVAS PARA A PROTEÇÃO DE GRUPOS VULNERÁVEIS DIANTE DAS TECNOLOGIAS DE RECONHECIMENTO FACIAL

Ramon Costa

Doutorando em Direito pela Pontifícia Universidade Católica do Rio de Janeiro (PUC-Rio). Pesquisador do Núcleo Legalite PUC-Rio: Direito e Novas Tecnologias e do IDP Privacy Lab (CEDIS/IDP).

Bianca Kremer

Doutora em Direito pela Pontifícia Universidade Católica do Rio de Janeiro (PUC-Rio). Professora de Graduação e Pós-Graduação em Direito Digital do Instituto Brasileiro de Desenvolvimento e Pesquisa (IDP). Pesquisadora do Núcleo Legalite PUC-Rio: Direito e Novas Tecnologias, do IDP Privacy Lab (CEDIS/IDP) e Líder de pesquisa no Centro de Justiça e Sociedade (CJUS) da FGV Direito Rio.

Resumo: A pesquisa analisa as formas como as tecnologias de reconhecimento facial afetam direitos fundamentais, especialmente de grupos vulneráveis no Brasil. Desse modo, parte de um questionamento sobre como essas tecnologias impactam a realidade social desses grupos e sobre como é possível protegê-los diante da vigilância digital opressiva e discriminatória. O artigo utiliza um processo metodológico a partir do uso de técnicas de revisão bibliográfica e análise de legislações e projetos de lei no Brasil. O artigo explora casos brasileiros e internacionais na busca de aspectos críticos sobre a implementação de tecnologias de reconhecimento facial, bem como apresenta perspectivas sobre o banimento de tecnologias discriminatórias que podem aumentar contextos de vulnerabilidade, especificamente de pessoas negras e transexuais no Brasil.

Palavras-chave: Inteligência Artificial. Discriminação. Reconhecimento facial. Dados sensíveis. Populações vulneráveis.

Sumário: Introdução – **1** A discussão sobre a Tecnologia de Reconhecimento Facial e sua implementação no Brasil – **2** Sobre as faces da discriminação: tecnologias opressivas e os riscos para grupos vulneráveis – Considerações finais – Referências

Introdução

A inteligência artificial (IA) é um termo guarda-chuva para muitas disciplinas autônomas, reunindo uma variedade de aplicações já ambientadas em nossas

atividades diárias. Muitas pessoas utilizam aplicativos (*apps*) para traçarem rotas enquanto dirigem, para traduzirem textos, para darem comando de voz aos celulares, facilitando pesquisas na *internet*, dentre outros exemplos comuns em nossas rotinas e que são resultado do desenvolvimento de tecnologias de IA.

A inteligência artificial como conhecemos hoje é baseada majoritariamente em *machine learning* (aprendizado de máquinas). Isso significa que essas aplicações baseadas em IA são desenvolvidas de modo que as máquinas possam aprender a traçar modelos e resultados sobre problemas que desejamos resolver. A capacidade dessas tecnologias é exponencial, sendo possível que entreguem muitos resultados de forma ágil e em grande volume. Contudo, o sucesso de uma IA está estritamente relacionado aos dados que fornecemos para que a máquina processe e gere bons resultados, mais exatos e que solucionem ou facilitem algum processo por meio de sua automatização. Nesse contexto, um dos desafios na implementação de um sistema baseado em IA é a adequação do tratamento de dados realizado. Isso porque, quando falamos do uso de dados pessoais nesse processo, estamos falando sobre algo que envolve direitos dos titulares que têm seus dados tratados para o desenvolvimento e/ou aprimoramento de uma tecnologia. A discussão sobre a inteligência artificial, os dados que tratam e seus impactos sociojurídicos está evidente nas tecnologias de reconhecimento facial. O reconhecimento facial é uma tecnologia que funciona por meio de um algoritmo de IA, capaz de analisar detalhadamente uma imagem capturada por uma câmera, definindo um padrão individual para os rostos verificados. É possível alimentar um banco de dados com as informações extraídas dessa tecnologia e consequentemente identificar as pessoas (RAMOS, 2021, p. 1). Desse modo, temos no reconhecimento facial uma problemática inerente ao tratamento de dados biométricos, definidos no art. 5º, II da Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018 – LGPD) como dados sensíveis, ou seja, dados que quando tratados de forma indevida ou irregular podem ocasionar ou ampliar contextos discriminatórios para seus titulares, gerando danos à personalidade, por exemplo. Diante disso, este trabalho busca refletir e trazer apontamentos críticos sobre a implementação da tecnologia de reconhecimento facial no Brasil, país com expressiva diversidade humana e também marcado pela violência a grupos vulneráveis, como pessoas negras, LGBTI+ e mulheres. O trabalho parte das seguintes questões: 1) Como a tecnologia de reconhecimento facial impacta a vida dos grupos vulneráveis no Brasil? 2) De que maneira é possível proteger grupos vulneráveis em um contexto de implementação de tecnologias de reconhecimento facial?

O trabalho tem como objetivo compreender como o reconhecimento facial pode intensificar contextos discriminatórios para populações vulneráveis e o que pode ser feito para proteger as pessoas nessa conjuntura. Portanto, utiliza-se

da técnica de revisão bibliográfica como forma de articular a literatura e discutir os principais aspectos do tema. O artigo preocupa-se em levantar uma análise bibliográfica diversificada, apresentando referenciais expressivos na temática de inteligência artificial e discriminação, articulando este conteúdo com referenciais jurídicos e análises legislativas e regulatórias. Dessa forma, a pesquisa caracteriza-se pela interdisciplinaridade nas análises jurídicas e sociais do problema proposto.

O artigo tem seu desenvolvimento dividido em dois itens. O primeiro aborda a discussão da tecnologia de reconhecimento facial no Brasil, trazendo casos nacionais e internacionais para contextualizar os efeitos da tecnologia, bem como discute as questões regulatórias acerca do reconhecimento facial. Em um segundo momento, o artigo articula uma perspectiva crítica sobre como grupos vulneráveis, especialmente pessoas negras, transexuais, travestis e não binárias, tendem a sofrer discriminação opressiva por meio da vigilância tecnológica, o que intensifica problemas já presentes na sociedade brasileira. Por fim, o trabalho apresenta suas considerações finais, indicando brevemente a discussão e seus resultados.

1 A discussão sobre a Tecnologia de Reconhecimento Facial e sua implementação no Brasil

Não há um consenso sobre qual seria a melhor definição para inteligência artificial, mas partindo do conceito de John McCarthy (2000), a IA está contida na produção de uma máquina capaz de comportar-se de modo que, caso se tratasse de um ser humano, fosse considerada inteligente. A tecnologia de reconhecimento facial é dotada de IA com o objetivo de reconhecer pessoas, ou seja, é uma tecnologia capaz de realizar uma atividade humana, de modo exponencial.

O reconhecimento facial é uma tecnologia possível a partir do desenvolvimento tecnológico e da formação de expressivos bancos de dados – *big datas* – que reúnem grandes volumes de dados biométricos, utilizados no processamento para identificação das pessoas. A necessidade do uso dessa tecnologia vem de um processo de crescimento urbano e populacional acelerado nas cidades pelo mundo (OLIVEIRA, 2021, p. 40). Nesse contexto, a demanda por um maior controle estatal foi aumentada, sendo comum que a Administração Pública se utilize de novas formas de vigilância sobre as pessoas. Não por acaso, as chamadas "cidades inteligentes" são o reflexo do interesse estatal em tecnologias de comunicação e informação (TIC) e no tratamento de bancos de dados pessoais volumosos, tendo em vista a utilidade para o planejamento urbanístico (BARROS; VENTURINI, 2018, p. 32).

O reconhecimento facial é uma tecnologia de identificação biométrica realizada a partir da coleta de dados faciais, que podem ser provenientes de fotografias ou segmentos de vídeos. Esses sistemas automatizados extraem representações matemáticas de traços específicos como, por exemplo, a distância entre os olhos ou o formato do nariz, produzindo o que é chamado de padrão facial. É justamente no processo de comparação desse padrão facial a outros padrões faciais contidos na base de dados prévia do sistema que a tecnologia identifica indivíduos desconhecidos, como no caso das câmeras de monitoramento nas ruas, ou autentica pessoas conhecidas, como ocorre no desbloqueio de celulares com *Face ID* e com validação de contas bancárias em *smartphones* (KREMER, 2022).

Outros elementos podem ser indicados na necessidade de implementação das tecnologias de reconhecimento facial, alinhados a interesses privados e públicos, com objetivos de autenticação e identificação. Em âmbito privado, vemos cada vez mais empresas, bancos e serviços utilizarem o método para cadastrar e dar acesso às pessoas. Mas o Estado também passou a ter maior interesse na implementação de tecnologias digitais de vigilância, com o uso de câmeras sofisticadas e sistemas de reconhecimento robustos, que operam por meio da coleta massiva de dados pessoais dos cidadãos.

Fato é que as tecnologias digitais remodelaram os sentidos de privacidade na sociedade contemporânea. A utilização expressiva das TIC vem acompanhada de justificativas mercadológicas de aumento da segurança, praticidade e conforto para os consumidores e também de interesse público, pela possibilidade de melhorias no oferecimento de serviços públicos, até mesmo como tentativa de aumento e manutenção da segurança pública. Os eventos ocorridos no 11 de setembro de 2001 nos Estados Unidos configuram um momento histórico recente que demarcou a necessidade do aumento da vigilância em nível global, acarretando o controle massivo de dados pessoais e a implementação de tecnologias apuradas de reconhecimento facial em câmeras de vias públicas e sistemas de aeroportos, por exemplo. Sendo assim, a vigilância constante por meio de tecnologias digitais tem se mostrado uma tendência no mundo inteiro (RODOTÁ, 2008).

Em termos de Brasil, o país já conta com um uso expressivo de tecnologias de reconhecimento facial. Segundo dados levantados pela Privacy.co, o Brasil é o quinto país que mais possui câmeras do tipo Hikvision e Dahua – conhecidas por sua alta capacidade de reconhecimento facial. Essas câmeras de vigilância são utilizadas na China e o uso já foi apontado como violador de direitos humanos, tendo em vista a capacidade das câmeras de perfilamento das pessoas, com base na raça/etnia, o que foi usado na China para perseguição aos povos uigures, no Norte do país. Essa funcionalidade pode ser ainda adaptada para outros padrões, o que evidencia a possibilidade de uso dessas tecnologias para opressão e violação

de direitos fundamentais (LOURENÇO, 2021). Há casos de prisões no Brasil que ocorreram após identificação por reconhecimento facial. No carnaval de 2019 um homem foi preso em Salvador após ser identificado por uma câmera. Ele era procurado por homicídio. No Rio de Janeiro, a polícia militar utilizou 28 câmeras com reconhecimento facial que identificaram quatro criminosos durante o carnaval (RAMOS, 2021, p. 11).

Apesar dos casos que podem ser vistos como positivos para a segurança pública e investigação criminal, as tecnologias de reconhecimento facial possuem uma face nebulosa em sua aplicação no Brasil, que antecede a própria tecnologia, o racismo. Não são raros os casos de pessoas inocentes sendo presas por crimes que não cometeram, tendo sido identificadas de forma incorreta pelo chamado reconhecimento fotográfico, feito por pessoas e não máquinas. A repórter Hellen Guimarães (2021) reuniu diversos casos desses, relatando a prisão de um cientista de dados, um mototaxista, um motorista de *app*, um músico e um produtor cultural, todos homens negros. O problema é que as máquinas utilizadas no reconhecimento facial carregam as percepções de quem as produzem e do tratamento fornecido aos bancos de dados que as alimentam, portanto, há grandes chances de erros como esses se tornarem mais comuns por meio do reconhecimento facial. Isso porque existem questões estruturais sobre como a sociedade e o Estado leem quem são os indivíduos que devem ser vigiados, perseguidos, ou seja, sobre quem são as pessoas que oferecem perigo e devem ser detidas.

Acompanhando essa problemática, os pesquisadores Woodrow Hartzog e Evan Sellinger (2020) indicam que o reconhecimento facial pode ser uma ferramenta "perfeita" para a opressão, visto que podem lesionar direitos à privacidade e outras garantias fundamentais, ocasionando a perseguição a pessoas negras e grupos étnicos específicos. No Brasil, esse debate tem ganhado notoriedade e algumas medidas já foram tomadas. Em 2021, o CNJ (Conselho Nacional de Justiça) instaurou o grupo de trabalho denominado "GT Reconhecimento Pessoal", atendendo a um pedido da organização não governamental *Innocence Project Brasil* em conjunto com outros parceiros que pediram a criação de um GT responsável pela avaliação sobre regulamentação, parametrização, critérios de realização e valoração de reconhecimento de pessoas sob suspeita de crime. A instalação do GT tem como objetivo evitar prisão de inocentes e baseia-se em dados que revelam números expressivos de procedimentos incorretos, tendo como principais vítimas pessoas negras. Na esteira da discussão sobre parâmetros e regulamentações para processos de reconhecimento de pessoas, as tecnologias de reconhecimento facial (TRF) ganham destaque como possibilidades de ampliação do problema. Isso porque as TRFs utilizam inteligência artificial por meio de atividade algorítmica, algo ainda não regulado e que, muitas vezes, pode ser utilizado em desconformidade com leis e garantias fundamentais.

A Lei Geral de Proteção de Dados não regula diretamente os casos de uso de dados para fins de segurança pública e persecução penal, mas garante que serão tratados em legislação específica (art. 4º, inc. III). A LGPD foi aprovada em 2018, e em 2019 a Câmara dos Deputados tomou a iniciativa de criar uma Comissão de Juristas para elaboração do anteprojeto da chamada LGPD Penal. Em 2020, um ano após sua formação, a Comissão apresentou à Presidência da Câmara uma proposta de anteprojeto que teve duas inspirações principais: a LGPD e a Diretiva nº 2016/680 da União Europeia (COSTA; REIS, 2021). O documento foi composto por 12 capítulos e 68 artigos, divididos em oito eixos temáticos: 1. Âmbito de aplicação da Lei; 2. Condições de aplicação; 3. Base principiológica; 4. Direitos e obrigações; 5. Segurança da informação; 6. Tecnologias de monitoramento; 7. Transferência internacional de dados; e 8. Autoridade de supervisão.

O documento é abrangente e, no momento, encontra-se na Câmara dos Deputados à espera de ser apresentado formalmente por algum parlamentar a fim de tornar-se um Projeto de Lei (PL). Somente após isso, o futuro PL seguirá os trâmites comuns do processo legislativo e será submetido à avaliação das mais diversas comissões, votação, envio ao Senado e, por fim, submissão à sanção presidencial. O uso crescente de tecnologias de reconhecimento facial em atividades de investigação criminal e repressão de infrações no Brasil já é uma realidade em diversas unidades da Federação, razão pela qual se mostra imperiosa a aprovação de uma regulação que norteie os limites e possibilidades do tratamento de dados pessoais (sobretudo biométricos) no campo da segurança pública.

Ressalva-se que o objetivo das limitações de aplicação da LGPD nas hipóteses do art. 4º, III, é garantir o interesse público no combate às infrações penais, crime organizado, fraude digital, ou até mesmo terrorismo. No entanto, a não aplicabilidade da LGPD nesses contextos não é absoluta, visto que o §1º do mesmo artigo determina que os princípios gerais de proteção ao titular de dados continuarão norteando qualquer esfera de tratamento, até mesmo em contextos de interesse público. Assim, os princípios da finalidade, adequação, necessidade, transparência e não discriminação, bem como os direitos de acesso aos dados, correção, anonimização e eliminação das informações inadequadas (dispostos nos arts. 6º, 17 e 18 da referida lei), continuam servindo como exemplos de formas de garantia dos direitos fundamentais dos titulares de dados e impedindo tratamentos irregulares de dados por parte do Poder Público (NEGRI; OLIVEIRA; COSTA, 2020, p. 97).

O reconhecimento facial tem sido o carro-chefe de grandes promessas na segurança pública, ao passo que populações socialmente vulneráveis têm sido constantemente sujeitas à automatização de constrangimentos e violências, também com uso de tecnologias, como abordagens policiais indevidas e atribuição inverídica de

antecedentes criminais. Foi o caso do cientista de dados Raoni Lázaro Barbosa, preso injustamente no portão de sua casa em setembro de 2021, acusado de integrar a base de dados de procurados pela polícia por pertencer a uma milícia em Duque de Caxias (LEMOS, 2021).

Outro caso expressivo foi o do pedreiro José Domingos Leitão em dezembro de 2021, no Piauí, acordado por policiais civis de madrugada com gritos e chutes na porta de sua casa, após um programa de reconhecimento facial confundi-lo com o autor de um crime que não cometeu em Brasília, aproximadamente 1.200 quilômetros de distância de onde reside (R7, 2021). Tanto Raoni quanto José tinham um elemento em comum: eram homens negros. Os vieses raciais contidos nos algoritmos de reconhecimento facial ganham outros contornos no campo da segurança pública. E as condições atuais de produção, armazenamento e atualização das bases de dados desses sistemas pelo setor público são uma verdadeira caixa preta. Somado a isso, no contexto regulatório brasileiro, ainda não existe uma legislação que regulamente o uso de reconhecimento facial e outras técnicas de inteligência artificial.

O Projeto de Lei (PL) 21/2020, que visa a regulamentação do uso da Inteligência Artificial no Brasil, de autoria do deputado Eduardo Bismarck (PDT-CE), foi votado e aprovado na Câmara dos Deputados e seguiu para avaliação do Senado Federal. O PL indica de forma genérica possibilidades regulatórias para o setor de IA. Contudo, foi aprovado de forma célere e em um contexto distante dos processos de aprovação de outras leis importantes para temas de tecnologia e sociedade no Brasil, como o Marco Civil da Internet e a LGPD, visto que a lei de IA não foi discutida fortemente pela sociedade civil e houve pouco debate em torno de seu conteúdo, objetivos e estruturação, sendo ausente um contexto robusto de consulta pública em sua elaboração e andamento, o que é de extrema necessidade em um processo de regulamentação do tema.

Entretanto, vale destacar que o PL 21/2020 faz menção a alguns aspectos importantes no debate sobre discriminação algorítmica. O art. 3º estipula que na interpretação da lei proposta será levada em conta a relevância da inteligência artificial para a inovação, salientando aspectos econômicos, mas também a promoção do desenvolvimento humano e social. Nessa esteira, o art. 4º, IV apresenta como fundamento do uso da IA no Brasil, a igualdade, a não discriminação, a pluralidade, o respeito aos direitos trabalhistas, a privacidade e a proteção de dados, o respeito aos direitos humanos e aos valores democráticos, dentre outros fundamentos.

Destaca-se ainda o art. 5º, I, que, ao abordar os objetivos do uso de IA no Brasil, indica a promoção de uma IA ética e livre de preconceitos. O PL conta ainda com elementos interessantes para a consolidação de uma legislação atenta à

proteção de dados, determinando garantias de transparência dos dados sensíveis utilizados em uma IA (art. 7º, III) e assegurando que os dados tratados no uso de uma IA devem seguir os parâmetros previstos na LGPD (art. 9º, III). Os próprios princípios do PL são muito semelhantes aos princípios da LGPD, sendo destacados no art. 6º como: finalidade, centralidade no ser humano, não discriminação, transparência e explicabilidade, segurança, responsabilização e prestação de contas. Sendo assim, uma leitura básica sobre o PL de regulamentação de IA mais proeminente no Brasil demonstra que, mesmo com severas falhas no que diz respeito ao conteúdo generalizado e falta de diálogo com a sociedade, ainda refletiu uma preocupação do legislador em garantir que sistemas de IA não gerassem processos discriminatórios e danos aos direitos humanos e ao Estado democrático. Porém, o texto demonstra instabilidade nesta defesa de uma regulamentação mais protetiva para as pessoas, visto que não especifica formas de controle e responsabilização com clareza. O art. 6º, VI, ao tratar do princípio de responsabilização e prestação de contas, possibilita uma interpretação de responsabilidade subjetiva para os agentes, visto que não avança nas questões de riscos iminentes dessas tecnologias e na possibilidade de danos concretos, o que configuraria uma possível responsabilidade objetiva. Nesse sentido, uma regulamentação da IA no Brasil deve partir do pressuposto que tecnologias como o reconhecimento facial são extremamente vigilantes e podem gerar consequências graves na vida das pessoas, a depender de seu uso e contexto social em que está inserida, sendo necessário questionar até mesmo a eficiência de um processo regulatório neutralizado e que vislumbra apenas aspectos técnicos relacionados à tecnologia e pouco discute o fator humano no controle e efeitos dessas tecnologias. Quando observamos essa discussão ao redor do mundo, identificamos movimentos consolidados de banimento das TRF devido ao potencial altamente discriminatório e lesivo, especialmente em seus usos para segurança pública.

Em 2019, a cidade de São Francisco nos EUA baniu o uso de *softwares* de reconhecimento facial que eram usados pela polícia e agências locais na investigação de crimes e busca de suspeitos. A decisão chamou atenção, tendo em vista que a cidade é um epicentro tecnológico no mundo e mesmo assim as autoridades locais ratificaram a importância de impor limites ao uso da tecnologia, devido ao seu grande potencial opressivo (CONGER; FAUSSET *et al.*, 2019). Em junho de 2021, a Europa também demonstrou avanços significativos em uma análise sobre o uso do reconhecimento facial nos países europeus. O Comitê Europeu de Proteção de Dados (EDPB) e a Autoridade Europeia para a Proteção de Dados (EDPS), da União Europeia apresentaram uma opinião conjunta que sugeriu o banimento do reconhecimento de pessoas por inteligência artificial em espaços públicos: o *AI Act*. As justificativas para a sugestão estão centradas na ausência

de uma regulamentação bem definida sobre o uso dessas tecnologias, bem como pelo alto risco de gerarem violações aos direitos fundamentais (GOMES, 2021).

Entidades do poder público como a Comissão Europeia, o Conselho da Europa e Autoridades de Proteção de Dados têm exigido uma aplicação imediata do princípio da precaução, e recomendado a proibição geral de qualquer utilização de tecnologias de reconhecimento facial em espaços acessíveis ao público. Com especial enfoque em reconhecimento automatizado de características humanas como reconhecimento de rostos, formas de andar, impressões digitais, DNA, voz e outros sinais biométricos ou comportamentais, em qualquer contexto. Além disso, demarcaram a proibição de sistemas de Inteligência Artificial "que utilizem biometria para categorizar indivíduos em grupos com base em sua etnia, sexo, orientação política ou sexual ou outros motivos pelos quais a discriminação é proibida à luz do artigo 21 da Carta dos Direitos Fundamentais" (GOMES, 2021).

O uso de tecnologias de biometria facial tem sido mal recebido no continente europeu, e uma forte expressão do que se verifica como um movimento em direção ao banimento pelas vias regulatórias e de políticas públicas pode ser percebida na recente posição da nova coalizão que compõe o governo alemão, datada de novembro de 2021. Apenas dois meses após as eleições gerais em que Olaf Scholz sucedeu Angela Merkel como novo chanceler alemão, os social-democratas alemães (SPD), os *Greens* e os Liberais (FDP) finalizaram seu acordo de coalizão para o novo governo em que, dentre os compromissos assumidos pelos três partidos, uma das principais pautas políticas se voltava à proibição de tecnologias de reconhecimento facial no espaço público, bem como restrição do uso de ferramentas de vigilância em massa ao mínimo necessário (NOYAN, 2021).

No mesmo sentido, o Parlamento italiano também proibiu o uso de reconhecimento facial em espaços públicos e abertos ao público, introduzindo uma moratória nos sistemas de vigilância por vídeo que utilizam sistemas de reconhecimento facial. Esta lei introduziu, pela primeira vez na história da União Europeia, a proibição a entidades privadas de utilizarem esses sistemas em locais públicos, ou acessíveis ao público. Essa moratória tem sido considerada uma importante conquista política de admissão dos perigos representados por tecnologias de reconhecimento facial para os direitos e liberdade das pessoas. A moratória estará em vigor até 31 de dezembro de 2023 (EDRI, 2021).

No contexto latino-americano, diversas organizações de sociedade civil têm pautado o debate público sobre os riscos das tecnologias de reconhecimento facial, e promovido campanhas em prol do seu banimento. É o caso de iniciativas promovidas em países como Chile, por meio da *Red en la Defensa de los Derechos Digitales*, na Argentina, com a campanha *Con Mi Cara Non*, encabeçada pela *ADC por los Derechos Civiles*, e México, pela *Amnistia Internacional*. No Brasil, a

Coalizão Direitos na Rede também promoveu em junho de 2022 o lançamento de uma campanha nacional pelo banimento das tecnologias de reconhecimento facial na segurança pública, denominada *Tire meu rosto da sua mira*.

Esses exemplos demonstram como o debate sobre o reconhecimento facial requer um olhar social atencioso em um processo regulatório. Uma legislação que contemple essas tecnologias não pode estar apartada de uma avaliação concreta sobre quais os efeitos que seus usos geram em uma sociedade. No Brasil, pesquisadores e ativistas também estão debatendo e estudando essa conjuntura. Pablo Nunes, pesquisador coordenador do *Panóptico*, projeto do Centro de Estudos de Segurança e Cidadania (CESeC), aponta que "apesar do movimento mundial ser de crítica, banimento ou moratória ao uso do reconhecimento facial pelas polícias, no Brasil temos visto o movimento contrário" (NUNES, 2021).

Uma pesquisa feita pelo Instituto Igarapé que levantou dados entre os anos de 2011 e 2019, demonstrou que 30 cidades brasileiras, de 16 estados, utilizavam tecnologias de reconhecimento facial em atividades de guardas, policiais e outros órgãos (IGARAPÉ, 2019). A partir das últimas eleições municipais de 2020, houve considerável aumento do interesse de municípios brasileiros na implementação de tecnologias da informação e comunicação na segurança pública. Dentre os 26 prefeitos eleitos em capitais, 17 apresentaram propostas que, de algum modo, preveem isso (MELO, 2021). Diante desse contexto, há também um movimento contrário ao uso e ampliação de sistemas de vigilância e segurança baseados em tecnologias como o reconhecimento facial.

A *Artigo 19*, organização não governamental de direitos humanos, fundada em Londres no ano de 1987 e presente no Brasil desde 2007, assinou junto a outras 170 entidades, uma carta aberta em prol do banimento global de usos de reconhecimento facial e outros reconhecimentos biométricos remotos que permitam vigilância em massa, discriminatória e enviesada. O documento indica em sua justificativa para o banimento, o fato do reconhecimento facial e outras tecnologias de reconhecimento biométrico remoto possuírem falhas técnicas significativas, incluindo sistemas de reconhecimento facial com vieses raciais, que são menos acurados para pessoas com tons de pele mais escuros. A carta enfatiza que, mesmo ocorrendo melhorias técnicas nesses sistemas, isso não evitará a ameaça que representam aos direitos humanos (ARTIGO 19, 2021). Na esteira do movimento pela perspectiva crítica quanto ao uso dessas tecnologias, Pablo Nunes (2021) destaca o movimento de projetos e profissionais no Brasil:

> O Panóptico, projeto do Centro de Estudos de Segurança e Cidadania (CESeC) que coordeno desde o início deste ano, procura mapear os usos de reconhecimento facial pelas polícias do país; o AqualtuneLab, coletivo de juristas negros, tem se dedicado a racializar o debate

sobre direitos digitais no país; e o DataPrivacy Brasil tem tido papel fundamental nas questões de proteção de dados. Além dessas instituições, Nina da Hora, cientista da computação, tem se dedicado a trazer mais gente para o debate por meio de uma comunicação didática e fácil, e o Tarcízio Silva, que compila uma linha do tempo do racismo algorítmico, tem discutido o tema em fóruns diversos.

Diante disso, fica evidente que a discussão sobre a TRF envolve um debate amplo sobre a necessidade de implementação de mecanismos tecnológicos para maiores resultados em nível de controle social e segurança pública, além das contrapartidas desse processo, que inevitavelmente geram vigilâncias discriminatórias e ampliam problemas sociais expressivos, como o racismo já presente nas atividades policiais e de gestão pública da segurança. Nesse sentido, o próximo item aborda as dimensões sociais da implementação de tecnologias de reconhecimento biométrico no Brasil, levantando dados e discussões sobre como as populações vulneráveis são afetadas por esses sistemas e sobre como o debate jurídico deve estar atento para a defesa dos direitos fundamentais e para o combate à discriminação por ferramentas munidas de inteligência artificial.

2 Sobre as faces da discriminação: tecnologias opressivas e os riscos para grupos vulneráveis

Atualmente temos um debate expressivo sobre tecnologias cada vez mais avançadas e com enorme capacidade de impactarem os rumos da humanidade em termos sociais, culturais, políticos e econômicos. Mas a verdade é que muitas estruturas sociais e comportamentais já estão consolidadas nas sociedades contemporâneas, de modo que o processo de inovação tecnológica é inserido em um terreno no qual suas potencialidades e riscos são definidos substancialmente pelos fatores humanos, ou seja, sobre a forma como produzimos e conduzimos as tecnologias.

Nesse campo, estruturar uma iniciativa regulatória para sistemas de inteligência artificial envolve a compreensão sobre os processos históricos e socioculturais que embasam uma sociedade. Isso porque, é a partir da compreensão sobre a estrutura social que podemos vislumbrar os reais efeitos do aumento da vigilância digital.

Danilo Doneda *et al*. (2018), apontam que o desenvolvimento dos mecanismos de inteligência artificial possui uma relação estreita com o aumento do fluxo e tratamento de dados pessoais, o que deixou reflexos na regulação que começou

a ser concebida em relação à proteção de dados pessoais. Assim, o desenvolvimento e a implementação de tecnologias de inteligência artificial geraram efeitos que "implicam uma mudança na subjetividade das relações entre as pessoas e a tecnologia" (DONEDA *et al.*, 2018, p. 2). Os algoritmos são ferramentas imprescindíveis para a economia movida a dados, que é operada pela vigilância sobre os dados pessoais, utilizada para a formação de nichos de mercado e controle social, o que é sustentado pelas informações pessoais das mais diversas naturezas, que nos são retiradas especialmente pela digitalização das atividades cotidianas e uso dos meios digitais. Sobre esse cenário de vigilância constante e tratamento exponencial dos dados pessoais, Stefano Rodotá (2008) salienta o advento de uma sociedade da vigilância, baseada nas possibilidades tecnológicas de controle social.

Os algoritmos podem ser definidos como conjuntos de regras que os computadores e outras tecnologias seguem para resolver problemas e tomar decisões sobre um determinado curso de ação. O algoritmo é uma sequência lógica, finita e definida de instruções destinadas a resolver uma tarefa. A era computacional digital baseia-se expressivamente em sistemas de *big data*, que são grandes conjuntos de dados que precisam ser armazenados e processados, sendo inclusive analisados e classificados por algoritmos. Nesse sentido, "a lógica algorítmica foi expandida para processos de inteligência artificial estreita, presente nos sistemas informacionais do cotidiano" (SILVA, 2019, p. 4). A pesquisadora Cathy O'Neil (2020) destaca o papel dos algoritmos na produção e reprodução de discriminações. Isso porque os modelos algorítmicos utilizados nos *apps* acabam por moldar a experiência das pessoas nessas redes, mas são construções humanas limitadas. O'Neil classifica os algoritmos como possíveis "armas de destruição matemática", justamente por serem baseados em escolhas de seres humanos falíveis, o que ocasiona impactos sociais extremamente nocivos, especialmente a discriminação de populações mais vulneráveis.

Um dos efeitos mais expressivos do crescente uso e desenvolvimento das TICs é a vigilância sobre os dados pessoais dos cidadãos. 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. Nossos dados são tratados e controlados com o auxílio de algoritmos potentes e para a formação dos bancos de dados. Esse controle sobre as informações pessoais gera interesses econômicos e políticos e tem como vertente o chamado "capitalismo de vigilância", que Shoshana Zuboff (2019) conceitua como um sistema econômico que utiliza toda experiência humana, incluindo vozes, personalidades e emoções que estão contidas em nossos dados pessoais, que são controlados e capitalizados como dados comportamentais para os mais diversos mercados.

Contudo, a vigilância sobre as pessoas não é um processo novo, mesmo que esteja sendo constantemente renovado e potencializado pelas tecnologias. Em seus estudos sobre a sociedade disciplinar, Michel Foucault (2015) já indicava o percurso histórico de uso de ferramentas de conhecimento sobre a sociedade moderna como uma forma de exercer poder e impor controle sobre as populações. Nessa conjuntura, o chamado biopoder articulado por Foucault, compreende a sistemática reunião de informações pessoais sobre a saúde e condições gerais de vida dos indivíduos, sendo este procedimento uma forma de determinação sobre os corpos, práticas e comportamentos considerados saudáveis, ou não, o que torna mais eficiente o processo de opressão às pessoas entendidas como abjetas e contrárias aos pressupostos de uma vida considerada saudável pelos Estados e sociedades (FOUCAULT, 2015, p. 151).

Nos atuais debates sobre diversidade, a ideia de "normatividade" é utilizada para caracterizar a condição imposta por normas sociais e comportamentais que recaem sobre as pessoas como forma de classificá-las como "adequadas", no sentido de atenderem às expectativas construídas historicamente sobre quais corpos e condutas são legítimos, saudáveis e até mesmo humanizados. Nesse cenário, o racismo, sexismo e LGBTfobia ascendem não apenas como formas de opressão, mas de categorização, discriminação e marginalização. Assim, não é difícil imaginar que informações sobre pessoas que historicamente são vigiadas e categorizadas de modo negativo, muitas vezes são tratadas de forma a aumentar a vulnerabilidade dessas populações (COSTA, 2022, p. 61). A LGPD traz a categoria de dados sensíveis, como forma de garantir maior proteção no contexto de tratamento de dados que podem ser manejados de forma potencialmente discriminatória e lesiva. O art. 5º, II, da LGPD define como sensíveis os dados pessoais sobre raça, etnia, religião, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, e dados genéticos ou biométricos, quando vinculados a uma pessoa natural. Desse modo, a criação da categoria de dados sensíveis parte de um processo de observação pragmática acerca dos distintos efeitos causados pelo tratamento desses dados em relação aos demais. Nessa esteira, observa-se igualmente a necessidade de tutela do princípio da igualdade material, como fundamento para a proteção da pessoa (RODOTÀ, 2008, p. 85).

Assim, 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.

Nesse debate, é necessário pensar com o que e como a inteligência artificial é alimentada. Como essas tecnologias são enviesadas? Qual o impacto social disso? Pois, se como Foucault já salientava, nós somos categorizados socialmente como existências legítimas ou ilegítimas, corpos que importam e corpos que não importam, então, quais faces são reconhecidas e sobre que reconhecimento estamos falando quando uma sociedade marcada por discriminações de raça, classe, gênero e orientação sexual implementa tecnologias de vigilância com alto potencial opressivo?

Em um vídeo do TED (conferência *on-line*) de 2017, a cientista da computação, Joy Buolamwini, estudante do MIT (Massachusstes Institute of Technology), mostrou como algumas tecnologias munidas de inteligência artificial não reconheciam seu rosto. Buolamwini é uma pesquisadora que conduz diversos estudos sobre racismo e sexismo em tecnologias digitais. Ela propõe uma análise racializada da tecnologia, como forma de compreensão e correção de máquinas, robôs e ferramentas tecnológicas discriminatórias. A cientista relata sobre seu projeto para auditar algoritmos, chamado *Gender Shades* (*Tons de gênero* em tradução livre), que analisa tecnologias de reconhecimento facial. Segundo ela, "a precisão é menor em faces de mulheres negras". Contudo, o estudo demonstra que o mesmo não acontece quando a visibilidade é negativa, visto que as tecnologias demonstram ser extremamente eficazes para indicar pessoas negras para resultados negativos (BUOLAMWINI, 2017).

Já a pesquisadora Safiya Noble (2018) evidencia como algoritmos discriminam e subalternizam a representação de determinados grupos, especialmente mulheres e mais ainda quando negras, sendo algo perceptível até mesmo na ferramenta de complementação textual do Google, que escancara a misoginia, sexismo e racismo em suas sugestões. A autora indica que essa realidade é um efeito de fortalecimento das estruturas de poder reproduzidas pelas tecnologias e aponta como uma possibilidade de enfrentamento desse problema, a articulação de uma epistemologia feminista, que amplie os sentidos de desenvolvimento e apropriação dessas tecnologias, visto que são embasadas na experiência de homens brancos e burgueses, o que as condiciona a uma compreensão parcial e discriminatória sobre outros grupos sociais (NOBLE, 2018).

As pessoas trans também são apontadas como um grupo vulnerável que sofre potenciais violências discriminatórias na implementação de sistemas de inteligência artificial como a TRF. Segundo levantamentos feitos pela Associação Nacional de Travestis e Transexuais (ANTRA) em 2020, foram 175 travestis e mulheres transexuais assassinadas, número que representou alta de 41% em relação ao ano anterior, sendo 78% das vítimas negras e 72% profissionais do sexo (BENEVIDES; NOGUEIRA, 2021).

A informação sobre o gênero de uma pessoa pode parecer não sensível quando pensamos a partir de binarismos homem/masculino e mulher/feminino, já tão fortificados na identificação das pessoas na sociedade. Contudo, o gênero é uma identidade diversa, que identifica também pessoas que não estão conformadas em identidades cisgêneras, sendo o caso de pessoas trans, travestis, não binárias e gênero fluído, por exemplo. Nesse sentido, uma característica tão subjetiva como a identidade de gênero pode ter múltiplas nuances e diferentes recepções e desenvolvimentos sociais e individuais. O tratamento inadequado de informações sobre o gênero de uma pessoa trans pode ocasionar grave violação à personalidade, gerando contextos de discriminação para uma população já extremamente marginalizada. Alguns casos revelam como as tecnologias e o tratamento de dados podem impulsionar violências baseadas na identidade de gênero de populações vulneráveis. As pesquisadoras Mariah Rafaela Silva e Joana Varon desenvolveram um estudo sobre o uso de reconhecimento facial no setor público brasileiro e as identidades trans, no qual alertam sobre os riscos e práticas discriminatórias embutidas na tecnologia e tratamento dos dados, que afetam especificamente a população trans. Isso ainda é agravado pela ausência de transparência, o que dificulta uma mensuração acerca dos efeitos danosos quando avaliadas questões socioeconômicas, raciais e territoriais de pessoas trans (SILVA; VARON, 2021).

Portanto, os dados pessoais sobre identidade de gênero, raça, dados biométricos e outros dados sensíveis tratados e possivelmente cruzados em uma TRF podem gerar uma expansão do contexto discriminatório vivenciado por pessoas trans, tendo em vista dificuldades técnicas de identificação relacionadas aos vieses de produção da tecnologia, além da possibilidade de tratamento discriminatório das informações referentes a essa população. Nessa conjuntura, mesmo que não expressamente presente no art. 5º, II, da LGPD, a identidade de gênero, como informação objetiva ou o conjunto de informações que podem identificar uma pessoa neste aspecto, deve ser interpretada como um dado sensível. Essa interpretação pode ser incluída na perspectiva de que é uma informação pertencente a elementos relacionados à vida sexual, indicados pela LGPD como dados sensíveis, visto que é um dado integrante da ideia de esfera sexual das pessoas, não sendo termo vida sexual restrito à informação sobre orientação sexual. Além disso, o art. 11, §1º, também inclui uma possibilidade de interpretação da identidade de gênero como dado sensível ao abrir margens para aplicação do regime de dados sensíveis em tratamentos de dados que revelem informações sensíveis que podem gerar discriminação e danos aos titulares (COSTA; GAGLIARDI; TORRES, 2022).

Nesse sentido, a identidade de gênero, bem como as informações sobre raça e etnia e os dados biométricos devem ter destaque na análise sobre o tratamento

de dados operados por sistemas de IA em TRF, pois esses dados configuram um conjunto de dados sensíveis altamente capazes de gerarem discriminações negativas a partir de categorizações enviesadas e limitadas às percepções sociais problemáticas no que tange à diversidade. Assim, a vigilância opressiva mobilizada por meio do uso de TRF não está restringida a um tratamento objetivo dos dados biométricos recolhidos em processos de reconhecimento pessoal, mas também nas possibilidades de identificação e categorização das pessoas em outros aspectos, geralmente alinhados a vulnerabilidades expressivas em uma sociedade estruturalmente transfóbica e racista.

Em relação ao contexto de vigilância discriminatória e opressiva, o pesquisador Scott Skinner-Thompson (2021, p. 24) aponta em seus estudos que isso é um processo sistemático que tem sido historicamente destinado às minorias raciais e pessoas LGBTI+, definindo suas condições de vida e sociabilidades. O autor chama de "privacidade nas margens" esse cenário de distanciamento de grupos vulneráveis em relação a direitos fundamentais como liberdade e privacidade, apontando que pessoas negras e trans, por exemplo, são pessoas perseguidas nas sociedades, sendo empregados métodos de categorização e vigilância sobre essas pessoas, retirando delas aspectos essenciais de dignidade humana.

Conforme apontado por Simone Browne (2015), a vigilância não é uma novidade para pessoas negras, é um controle estabelecido pelo sistema antinegritude. A autora chama de "vigilância racializante" o processo de vigilância de pessoas negras não apenas como uma ferramenta de monitoramento e controle social, mas também para a produção da "negritude" como categoria, permitindo ainda mais o monitoramento e a categorização com base na divisão racial. Assim, atos de vigilância reificam as fronteiras ao longo das linhas raciais, reificando assim a raça, tendo como resultado disso um tratamento frequentemente discriminatório e violento para pessoas negras. A vigilância ajuda a estruturar as relações sociais por perspectivas raciais que privilegiam a branquitude em estruturas sociais marcadas pelo racismo (BROWNE, 2015, p. 10).

Diante dos contextos abordados, podemos vislumbrar, em alguma medida, como populações vulneráveis potencialmente sofrem significativos danos à personalidade em tratamentos indevidos e abusivos de dados. Nesse sentido, é necessário observar a diversidade em um processo de efetivação do tratamento de dados sensíveis e da forma como essas informações são utilizadas em processos automatizados com o uso de inteligência artificial, como é o caso da TRF. O direito também precisa ser mobilizado para a aplicação dos princípios da igualdade e não discriminação, rompendo "com o manto da desigualdade formal, e a perversa utilização de características étnico-raciais, sexuais e de gênero como mecanismos de exclusão" (MULHOLLAND; KREMER, 2019, p. 580). A transparência sobre a

criação e funcionamento dessas tecnologias também é um princípio basilar para o uso de tecnologias como a TRF, pois esses sistemas de IA são munidos de *machine learning* – aprendizado de máquinas –, sendo de extrema relevância a compreensão da sociedade sobre como essas tecnologias são operadas, como os dados que as alimentam são tratados. Essas explicações são necessárias para que possamos entender de modo transparente quais o métodos utilizados e, consequentemente, os resultados alcançados. Sem essa compreensão o que temos é uma opacidade típica de sistemas autoritários não regulados (MULHOLLAND; FRAJHOF, 2019, p. 273).

Ainda no debate sobre transparência, as possibilidades regulatórias de sistemas de IA precisam estar em diálogo com outras legislações, especialmente a LGPD, que inclusive dispõe ao longo de seu art. 20 sobre direitos de titulares relacionados ao contexto de tratamentos de dados de modo automatizado. O dispositivo destaca que o titular tem direito de solicitar a revisão de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem seus interesses, incluindo diversas dinâmicas como perfilamento pessoal, profissional, de consumo e de crédito. Essa garantia concedida ao titular de dados é relevante na articulação sobre os direitos dados às pessoas diante das tecnologias de IA, como a TRF, que pode gerar resultados enviesados de forma automatizada. Contudo, é necessário que haja intervenção humana no processo de revisão para que seja dado protagonismo a um debate crítico sobre as decisões automatizadas, os dados que as alimentaram e os usos que são feitos da tecnologia. Dessa forma, é preciso refletir sobre uma estratégia, que tem sido observada em normas de outros países, que é a promoção de um direito que integre a participação humana nos processos decisórios de sistemas de IA, ou seja, garantir que as pessoas não estejam sujeitas às decisões tomadas unicamente por mecanismos automatizados. Essa possibilidade pode ser contemplada por um direito à revisão humana e até mesmo por um direito a uma explicação, compreensível por seres humanos, quanto aos seus principais critérios e parâmetros (WIMMER; DONEDA, 2021, p. 3).

Vale destacar que o PL 21/2020 estabelece como princípios a transparência e explicabilidade, que determina a possibilidade de divulgação de conhecimento sobre a inteligência artificial, mas também indica observação sobre os segredos comercial e industrial. Assim, fica evidente a necessidade de uma maior elaboração sobre os direitos que as pessoas podem mobilizar diante de tratamento de dados realizado por tecnologias de IA. Ademais, quando falamos de tratamentos massivos de dados sensíveis por sistemas de IA, como no caso das tecnologias de reconhecimento facial, cabe uma maior atenção sobre como essas tecnologias são potencialmente falíveis e enviesadas e sobre como as falhas técnicas em

decisões automatizadas não podem ser definidas como resultados neutros. Isso porque essas tecnologias são produzidas, desenvolvidas e destinadas a finalidades de grande impacto individual e coletivo para a população, portanto, em casos de uso indevido, os potenciais danos recebem dimensões maiores de acordo com a vulnerabilidade das pessoas diante de um processo automatizado, sobre o qual pouco conhecem e pouco podem se proteger no cenário atual.

Considerações finais

Este trabalho teve o objetivo central de pensar sobre como as tecnologias de reconhecimento facial estão sendo implementadas no Brasil e em outros países e partiu de um processo de tensionamento crítico quanto aos efeitos sociais dessas tecnologias, especialmente para populações vulneráveis. Foram levantadas considerações atualizadas na literatura do tema. A discussão dos aspectos analisados demonstrou que pensar sobre um processo regulatório de sistemas baseados em IA, como a TRF, demanda um processo de participação popular e discussão pública, em que seja possível demarcar elementos sociais estruturais que definem muito sobre a forma como esses sistemas serão implementados e sobre como podem gerar danos significativos aos cidadãos.

O reconhecimento facial é uma tecnologia de identificação biométrica realizada a partir da coleta de dados faciais, que podem ser provenientes de fotografias ou segmentos de vídeos. Ele tem sido uma ferramenta de reprodução e potencialização de opressões já existentes na sociedade, pois, ao delegar aos algoritmos a tarefa de identificar e apontar suspeitos, confere-se à seletividade penal uma aparência de suposta neutralidade e afastamento da discriminação racial em abordagens policiais. Nesse sentido, é importante considerar que o Brasil é marcado por violências sistemáticas a grupos minoritários, inclusive perpetradas pelo Poder Público ou em nome de uma suposta segurança pública, que na verdade demarca quais faces são verdadeiramente reconhecidas para serem violadas e perseguidas, ao mesmo tempo que são desconhecidas em termos de acesso a direitos fundamentais e dignidade humana.

As tecnologias de reconhecimento facial têm ocasionado uma série de ameaças, abusos e violações a direitos humanos em todo o mundo. No caso brasileiro, elas vêm sendo implementadas desde 2019 por vinte estados das cinco regiões do país (VENTURA, 2021), e têm sido objeto de promessas tentadoras do setor privado e da Administração Pública, especialmente quando adotadas para fins de policiamento e segurança pública, ao argumento de mitigação da impunidade e aumento da eficiência do trabalho policial. O Brasil é o terceiro país que mais

encarcera pessoas em todo mundo (CONECTAS, 2020) e que mais mata pessoas transexuais (PINHEIRO, 2022). As tecnologias de reconhecimento facial reforçam esse cenário já, há muito, preocupante. Haja vista seu funcionamento binário e baseado em estereótipos, que não reconhecem e reforçam a diferença à diversidade de corpos, identidades e expressões a partir da construção de padrões de classificação.

Há uma tendência internacional ao banimento do uso de tecnologias de reconhecimento facial, especialmente nos Estados Unidos. Na cidade de São Francisco, seu uso foi banido em razão do alto potencial de uso abusivo e instauração de um estado de vigilância opressiva e massiva, além de uma baixa acurácia na identificação, sobretudo de pessoas negras e mulheres. A tendência foi também seguida nas cidades de Portland, Mineápolis, Cambridge, Oakland, Nova Orleans e dezenas de outros municípios. Além das recomendações do *AI Act*, promovida pela Autoridade Europeia de Proteção de Dados, em prol do banimento de tecnologias de reconhecimento facial em todo o bloco europeu.

Não há transparência no cenário brasileiro em relação aos contratos de fornecimento desses sistemas, nem mesmo se sabe ao certo quais são os critérios utilizados para reconhecimento de padrões faciais por essa tecnologia, ou como funcionam os *inputs* nos bancos de dados (*Datasets)*. Para agravar ainda mais a situação, sequer existe uma regulamentação específica de como essa tecnologia pode ser implementada de maneira a assegurar direitos e garantias fundamentais para aferição dos riscos de sua ampla adoção. Por essas razões, aliadas aos diversos relatos de violência promovida por essa ferramenta no campo da segurança pública, nunca foi tão importante efetivar o banimento do uso desta tecnologia. Além disso, os recentes debates sobre a construção de uma minuta de substitutivo aos PLs de Inteligência Artificial, dentre eles o PL 21/2020, pretende colaborar para a constituição de uma espécie de Marco regulatório da IA no Brasil. Seus antecessores apresentavam falhas estruturais no que diz respeito à ausência de consulta pública e maior discussão de seu texto e propostas regulatórias. Contudo, é importante que a Comissão de Juristas designada para esta função em abril de 2022 se comprometa a uma necessária análise sociojurídica e multissetorial sobre tecnologias de vigilância, sobretudo aquelas que detêm alto potencial opressivo como o reconhecimento facial, guiando as soluções jurídicas necessárias por meio de debates públicos e estudos que contemplem a realidade social radicada na experiência brasileira. A implementação de tecnologias de reconhecimento facial envolve o tratamento massivo de dados sensíveis como dados biométricos, raciais e outras informações identitárias, que impactam em dimensões sociais de discriminação e marginalização de pessoas. Diante disso, antes mesmo de pensarmos em processos regulatórios devemos nos perguntar

sobre como os fatores humanos impactam o uso dessas tecnologias e quais os reais objetivos de sua implementação.

Assim, uma via relevante para a proteção de grupos vulneráveis nesse contexto é o banimento de qualquer sistema de IA que implique processos discriminatórios e que amplie problemas estruturais que afastam pessoas negras, mulheres, pobres e LGBTI+ e outros grupos vulneráveis de seus direitos fundamentais, aumentando o abismo entre as populações localizadas nas margens da "evolução tecnológica" e aquelas detentoras de privilégios e controle sobre os rumos de tecnologias de vigilância.

Artificial intelligence and discrimination: challenges and perspectives for the protection of vulnerable groups in facial recognition technologies context

Abstract: This research analyzes the ways facial recognition technologies impact fundamental rights, especially of vulnerable groups in Brazil. Thus, it starts by questioning how these technologies impact the social reality of these groups and how it is possible to protect them from oppressive and discriminatory digital surveillance. The article uses a methodological process based on bibliographic review and document analysis of legislation and bills in Brazil. The paper explores Brazilian and international cases in the search for critical aspects about the implementation of facial recognition technologies, as well as presents perspectives on the banning of discriminatory technologies that can increase the context of vulnerability of black and trans people.

Keywords: Artificial Intelligence. Discrimination. Facial Recognition. Sensitive Data. Vulnerable Populations.

Summary: Introduction – **1** Discussion about Face Recognition Technology and its implementation in Brazil – **2** Faces of Discrimination: Oppressive Technologies and Risks for Vulnerable Groups – Final considerations – References

Referências

ARTIGO 19. Organizações se unem em chamada para banimento global de usos de reconhecimento facial e biométrico. *Artigo19*, 09 jun. 2021. Disponível em: https://artigo19.org/2021/06/09/21413/.

BARROS, Marina; VENTURINI, Jamila. Os desafios do avanço das iniciativas de cidades inteligentes nos municípios brasileiros. *In*: MAGRANI, Eduardo (Org.). *Horizonte presente*: debates de tecnologia e sociedade. Rio de Janeiro: Letramento, v. 1, 2018.

BENEVIDES, Bruna; NOGUEIRA, Sayonara. *Dossiê dos assassinatos e da violência contra travestis e transexuais brasileiras em 2020*. São Paulo: Expressão Popular, ANTRA, IBTE, 2021.

BRASIL. *Projeto de lei nº 21 de 2020*. Disponível em: https://www.camara.leg.br/propostas-legislativas/2236340.

BRASIL. Assembleia Legislativa. Lei 13.709/2018. *Lei Geral de Proteção de Dados Pessoais*. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato20152018/2018/Lei/L13709.htm. Acesso em: 15 dez. 2021.

BROWNE, Simone. *Dark Matters*: On the Surveillance of Blackness. Durham: Duke University Press Books, 2015.

BUOLAMWINI, Joy. *Como eu luto contra o preconceito em algoritmos. TED*. Vídeo. 2017. Disponível em: https://www.ted.com/talks/joy_buolamwini_how_i_m_fighting_bias_in_algorithms.

CONECTAS Direitos Humanos. Brasil se mantém como 3º país com maior população carcerária do mundo. *Conectas*, 18 fev. 2022. Disponível em: https://www.conectas.org/noticias/brasil-se-mantem-como-3o-pais-com-a-maior-populacao-carceraria-do-mundo/.

CONGER, Kate; FAUSSET, Richard; KOVALESKI, Serge. San Francisco Bans Facial Recognition Technology. *The New York Times*, 14 mai. 2019. Disponível em: https://www.nytimes.com/2019/05/14/us/facialrecognitionbansanfrancisco.html?utm_source=The+Hack&utm_campaign=d2697daeccThe_Hack_0123&utm_medium=email&utm_term=0_060634743e-d2697daecc-206979693.

COSTA, Eduarda; REIS, Carolina. Histórico da LGPD penal: o que foi feito até aqui e quais são os próximos passos? *Blog Lapin*, 16 abr. 2021. Disponível em: https://lapin.org.br/2021/04/16/lgpd-penal-o-que-foi-feito-ate-aqui-e-quais-sao-os-proximos-passos/#.

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.

COSTA, Ramon; GAGLIARDI, Marília; TORRES, Lívia. Gender Identity, Personal Data and Social Networks: An analysis of the categorization of sensitive data from a queer critique. *Revista Direito e Práxis*, Ahead of print, Rio de Janeiro, 2022.

DONEDA, Danilo. *Da privacidade à proteção de dados pessoais*. São Paulo: Revista dos Tribunais, 2019.

DONEDA, Danilo *et al*. Considerações iniciais sobre inteligência artificial, ética e autonomia pessoal. *Pensar*, Fortaleza, v. 23, n. 4, p. 1-17, out./dez. 2018.

EDRI. Italy introduces a moratorium on vídeo surveillance systems that use facial recognition. *EDRI.* 15 dez. 2021. Disponível em: https://edri.org/our-work/italy-introduces-a-moratorium-on-video-surveillance-systems-that-use-facial-recognition/. Acesso em: 15 maio 2022.

FOUCAULT, Michel. *História da Sexualidade 1*: a vontade de saber. 3. ed. São Paulo: Paz e Terra, 2015.

GOMES, Sheley. Europa avança para o banimento do reconhecimento facial. *Carta Capital*, 29 jun. 2021. Disponível em: https://www.cartacapital.com.br/blogs/intervozes/europa-avanca-para-o-banimento-do-reconhecimento-facial/.

GUIMARÃES, Hellen. Nos erros de reconhecimento facial, um "caso isolado" atrás do outro. Presos por engano, cientista de dados, mototaxista e motorista têm algo mais em comum: são negros. *Piauí*, 24 set. 2021. Disponível em: https://piaui.folha.uol.com.br/nos-erros-de-reconhecimento-facial-um-caso-isolado-atras-do-outro/.

HARTZOG, Woodrow; SELLINGER, Evan. Facial Recognition is the perfect tool for opression. *Medium*, 2 ago. 2018. Disponível em: https://medium.com/s/story/facial-recognition-is-the-perfect-tool-for-oppression-bc2a08f0fe66.

INOCENTE preso por erro de reconhecimento facial vive traumas. *R7,* Brasília, 15 dez. 2021. Dsiponível em: https://noticias.r7.com/brasilia/videos/inocente-preso-por-erro-de-reconhecimento-facial-vive-traumas-15122021. Acesso em: 15 maio 2022.

INSTITUTO IGARAPÉ. *Reconhecimento Facial no Brasil*. 2019. Disponível em: https://igarape.org.br/infografico-reconhecimento-facial-no-brasil/.

KREMER, Bianca. Reconhecimento facial no Brasil: uma perspectiva de gênero e raça. *Medium Coding Rights*. 7 fev. 2022. Disponível em: https://medium.com/codingrights/reconhecimento-facial-no-brasil-uma-perspectiva-de-ra%C3%A7a-e-g%C3%AAnero-9fe027c3a176. Acesso em: 15 maio 2022.

LEMOS, Marcela. Polícia admite erro e cientista de dados da IBM preso por 22 dias é solto. *Uol Notícias*, Rio de Janeiro, 9 set. 2021. Disponível em: https://noticias.uol.com.br/cotidiano/ultimas-noticias/2021/09/09/policia-admite-erro-e-cientista-de-dados-da-ibm-preso-por-22-dias-e-solto.htm. Acesso em: 15 maio 2022.

LOURENÇO, Gabriel. Brasil é o 5º país com mais redes de câmeras de vigilância com reconhecimento facial no mundo. *Olhar Digital*, 25 nov. 2021. Disponível em: https://olhardigital.com.br/2021/11/25/seguranca/brasil-cameras-reconhecimento-facial/. Acesso em: 21 maio 2022.

MCCARTHY, J. *What is artificial intelligence*? Stanford, 2000. Disponível em: http://www-formal.stanford.edu/jmc/whatisai.pdf.

MELO, Paulo Victor. A serviço do punitivismo, do policiamento preditivo e do racismo estrutural. *Diplomatique*, 18 mar. 2021. Disponível em: https://diplomatique.org.br/a-servico-do-punitivismo-do-policiamento-preditivo-e-do-racismo-estrutural/. Acesso em: 20 maio 2022.

MULHOLLAND, Caitlin; FRAJHOF, Isabella Z. Inteligência artificial e a Lei Geral de Proteção de Dados Pessoais: breves anotações sobre o direito à explicação perante a tomada de decisões por meio de *machine learning*. *In*: FRAZÃO, Ana; MULHOLLAND, Caitlin (Org.). *Inteligência artificial e Direito*: ética, regulação e responsabilidade. São Paulo: Thomson Reuters Brasil, 2019.

MULHOLLAND, Caitlin; KREMER, Bianca. Responsabilidade civil por danos causados pela violação do princípio da igualdade no tratamento de dados pessoais. *In*: SILVA, Rodrigo da Guia; TEPEDINO, Gustavo (Org.). *O Direito Civil na era da inteligência artificial*. São Paulo: Revista dos Tribunais, 2020, p. 565-584.

NEGRI, Sergio; OLIVEIRA, Samuel; COSTA; Ramon. O Uso de Tecnologias de Reconhecimento Facial Baseadas em Inteligência Artificial e o Direito à Proteção de Dados. *Revista Direito Público.* Brasília, Volume 17, n. 93, 82-103, maio/jun. 2020.

NOBLE, Safiya Umoja. *Algorithms of Oppression: How search engines reinforce racism*. NYU Press, 2018.

NOYAN, Oliver. New German government to ban facial recognition and mass surveillance. Euractiv, 26 nov. 2021. Disponível em: https://www.euractiv.com/section/data-protection/news/new-german-government-to-ban-facial-recognition-and-mass-surveillance/. Acesso em: 16 maio 2022.

NUNES, Pablo. O algoritmo e racismo nosso de cada dia. *Revista Piauí*, 02 jan. 2021. Disponível em: https://piaui.folha.uol.com.br/o-algoritmo-e-racismo-nosso-de-cada-dia/.

OLIVEIRA, Samuel. *Sorria, você está sendo filmado!* Repensando direitos na Era do reconhecimento facial. São Paulo: Thomson Reuters Brasil, 2021.

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.

PINHEIRO, Ester. Há 13 anos no topo da lista, Brasil continua sendo o país que mais mata pessoas trans no mundo. *Brasil de Fato*, 23 jan. 2022. Disponível em: https://www.brasildefato.com.br/2022/01/23/ha-13-anos-no-topo-da-lista-brasil-continua-sendo-o-pais-que-mais-mata-pessoas-trans-no mundo#. Acesso em: 18 maio 2022.

RAMOS, Lucas Cabral de Souza. *Reconhecimento Facial*: do uso privado aos blocos de carnaval. 2021. 39 f. Trabalho de Conclusão de Curso (Análise e Desenvolvimento de Sistemas) – Faculdade de Educação Tecnológica do Estado do Rio de Janeiro, 2021. Disponível em: https://bityli.com/YaFcj.

RODOTÀ, Stefano. *A vida na sociedade da vigilância*: a privacidade hoje. Rio de Janeiro: Renovar, 2008.

SILVA, Mariah Rafaela; VARON, Joana. *Reconhecimento facial no setor público e identidades trans*: tecnopolíticas de controle e ameaça à diversidade de gênero em suas interseccionalidades de raça, classe e território. Rio de Janeiro: Codin Rights, 2021. Disponível em: https://codingrights.org/docs/rec-facial-id-trans.pdf. Acesso em: 29 dez. 2021.

SILVA, Tarcízio. Racismo Algorítmico em Plataformas Digitais: microagressões e discriminação em código. *Anais do VI Simpósio Internacional Lavits*. Salvador, 2019. Disponível em: https://lavits.org/anais-do-vi-simposio-internacional-lavits-assimetrias-e-invisibilidades-vigilancia-genero-e-raca/?lang=pt Acesso em: 12 jan. 2022.

SKINNER-THOMPSON, Scott. *Privacy at margins*. Cambridge: Cambridge University Press, 2021.

VENTURA, Layse. Tecnologia de reconhecimento facial chega a 20 estados. *Olhar Digital*, 10 jul. 2021. Disponível em: https://olhardigital.com.br/2021/07/10/seguranca/tecnologia-de-reconhecimento-facial-chega-a-20-estados/. Acesso em: 15 maio 2022.

WIMMER, Miriam; DONEDA, Danilo. "Falhas de IA" e a Intervenção Humana em Decisões Automatizadas: Parâmetros para a Legitimação pela Humanização. *Revista Direito Público*. Brasília, V. 18, n. 100, p. 374-406, out./dez. 2021.

ZUBOFF, Shoshana. *A Era do Capitalismo de Vigilância*: a luta por um futuro humano na nova fronteira do poder. Rio de Janeiro: Intrínseca, 2020.

Informação bibliográfica deste texto, conforme a NBR 6023:2018 da Associação Brasileira de Normas Técnicas (ABNT):

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.

Recebido em: 21.03.2022
Pareceres: 12.04.2022, 17.04.2022
Aprovado em: 01.09.2022