ARTIGOS

POR UM RECONHECIMENTO FACIAL ANTIDISCRIMINATÓRIO: O IMPERATIVO DE ASSEGURAR BANCOS DE ROSTOS DIVERSOS E COMBATER VIESES RACIAIS

DEFENDING AN UNDISCRIMINATING FACIAL RECOGNITION: THE IMPERATIVE OF ENSURING DIVERSE FACES DATABASES AND COMBATTING RACIAL BIASES

Flavianne Fernanda Bitencourt Nóbrega
João Vitor Sales Zaidan

RESUMO: O presente artigo objetiva relacionar a noção de direitos antidiscriminatórios aos possíveis obstáculos técnicos para a sua asseguração concreta em sistemas de reconhecimento facial. Com base na igualdade de direito e da desigualdade material, observa-se que, na esfera do reconhecimento facial, muitos sistemas demonstram ter vieses raciais com menos precisão quando se trata de pessoas não brancas. Necessita-se, pois, que a legislação incorpore a esses os meandros técnicos dessas tecnologias para que se assegure um padrão mínimo ético. Nesse sentido, foi feita uma análise sobre as possibilidades de regulação da solução, em que se constatou laconismo nas propostas legislativas relacionadas ao tema em relação a vieses raciais e questões técnicas, o que pode implicar a falta de efetividade dos direitos fundamentais na esfera dos referidos sistemas.

PALAVRAS-CHAVE: Direito antidiscriminatório. Reconhecimento facial. Padrão ético. Viés racial. Tecnologia.

ABSTRACT: This paper aims to relate the idea of undiscriminating rights to possible technical obstacles to its concrete assurance in facial recognition systems. From the notions of legal equality and material inequalities, one can observe that, in the facial recognition field, many systems seem to have racial biases, with less precision when it comes to non-white people. It is necessary, thus, that legislation incorporates these technologies' technical details in order to ensure a base ethical standard. Hence, na analysis of the possibilities of regulation of this solution was made, in which it was discovered that draft bills related to theme show a lack of themes such as racial biases and technical issues, which can imply in a lack of efectiveness of fundamental rights in the application of those systems.

KEYWORDS: Undiscriminating rights. Facial recognition. Ethical standard. Racial bias. Technology.

1. INTRODUÇÃO

Em dias hodiernos, é notável como avanços promovidos pelas novas tecnologias modificaram diversas sociedades, inclusive a brasileira, chegando-se ao conceito de sociedade da informação (INTERNATIONAL TELECOMMUNICATION UNION, 2014). Essas inovações, assim como os mais distintos fenômenos sociais que foram tendo lugar com o tempo, têm implicações importantes para o direito, na medida em que apresentam novos desafios para a efetividade de normas e princípios já existentes e criam espaços de atuação para que ordenamento jurídico evite a incidência de condutas que vão de encontro ao interesse coletivo. Essas questões geram discussões bastante aprofundadas e necessárias para que sejam geradas inovações legislativas e jurídicas eficientes e eficazes.

Uma das tecnologias que têm um grande potencial tanto de inovação quanto de violação de direitos fundamentais é o reconhecimento facial. Existem várias aplicações para a referida tecnologia, algumas delas já vistas no Brasil (INSTITUTO IGARAPÉ, 2019), mas, de acordo com o Conselho Nacional de Justiça, ainda não se há uso em massa dessas soluções na esfera penal, a qual se configura, em especial, como campo de potenciais violações. Nesse sentido, pode-se observar que o país se encontra em um estágio em que ainda é possível discutir e formular regulamentos para essas tecnologias de modo a evitar que a sua utilização signifique o descumprimento de princípios constitucionais e de direitos fundamentais, notadamente a igualdade e a não discriminação, com consequências severas para a sociedade.

A literatura sobre o reconhecimento facial admite, por exemplo, a face violadora que essa tecnologia pode apresentar, inclusive contra o Estado de Direito como um todo (BARROS e SILVA, 2020). Alguns autores, como Possa (2022), defendem a proibição completa da solução supracitada, dadas as suas ameaças à sociedade em matéria de não consentimento, vigilância em massa, compartilhamento indesejado e privacidade de dados pessoais/biométricos. Essa posição é compartilhada por empresas, como a International Business Machines (IBM).

Apesar de um número significativo de pesquisas sobre essa temática – seguindo os temas mais populares nas áreas de direito digital e governança da internet – ter como foco a questão dos dados e da privacidade, este artigo busca evidenciar o debate sobre os direitos antidiscriminatórios e essas tecnologias. Nesse sentido, o objetivo do estudo é relacionar a noção de direitos fundamentais de igualdade e não discriminação aos possíveis obstáculos técnicos que podem existir para a asseguração concreta dessas garantias em sistemas de reconhecimento facial.

Grande parte dos problemas relacionados a discriminação em sistemas do tipo são gerados por meio dos próprios sistemas, muitas vezes baseados em bancos de dados estrangeiros, em que os algoritmos acabam por gerar vieses, em especial, raciais (GROTHER, QUINN e PHILLIPS, 2011), apresentando um número de falsos positivos muito maior com pessoas negras, por exemplo. Dessa forma, torna-se evidente que o direito precisa incorporar a esses sistemas os meandros técnicos do reconhecimento facial, de modo a criar normas que fixem padrões mínimos éticos, por meio de detalhes do processo de criação desses sistemas, com o objetivo de assegurar direitos antidiscriminatórios.

Entender em detalhes o funcionamento de novas tecnologias é essencial para que as normas jurídicas tenham a eficácia desejada. Mais do que isso, fazê-lo é um dever para que direitos fundamentais já positivados também sejam garantidos de fato e não sejam violados em etapas de funcionamento. Caso contrário, tem-se uma lacuna no ordenamento jurídico, cujo significado prático é uma instituição informal em que as empresas do ramo podem agir como queiram, em detrimento da sociedade, especialmente de grupos marginalizados, constantemente alvo de vieses do reconhecimento facial.

Assim sendo, este artigo apresenta, inicialmente, uma seção sobre os direitos antidiscriminatórios, a questão ética e os direitos humanos no contexto da sociedade da informação, de modo a trabalhar os paradigmas teóricos sobre a igualdade e os marcos em relação à questão no âmbito digital. Outra seção, por sua vez, busca demonstrar como sistemas de reconhecimento facial podem representar violações aos direitos humanos por meio de vieses discriminatórios, sendo espaços em que normas devem incidir para que isso seja evitado. Por fim, são analisadas propostas legislativas sobre o tema ou que interagem com a problemática no Brasil, bem como modelos de outros países, de forma a entender quais são as perspectivas de regulação futura sobre a questão.

2. DIREITOS ANTIDISCRIMINATÓRIOS ANTE A SOCIEDADE DA INFORMAÇÃO

Estão assegurados pela Constituição Federal de 1988 (CF/88), bem como por tratados internacionais, os direitos fundamentais que constituem a dimensão mínima a ser garantida a todos os cidadãos brasileiros, inclusive a dignidade da pessoa humana, conforme art. 1º, III, do texto constitucional, e a igualdade (art. 5, *caput*). Na medida em que são abstratos, esses direitos positivados motivam diversas discussões – que envolvem pontos de vistas diversos – em casos concretos, gerando um acervo jurisprudencial que também é importante para entender como essas garantias podem ser materializadas.

Além disso, o surgimento de novos fenômenos sociais impõe mais um desafio à plena realização dos direitos fundamentais. Uma dessas novidades é, certamente, o reconhecimento facial, do qual já podem ser vistas ameaças (BARROS e SILVA, 2020) em países em que a implementação da tecnologia já está mais avançada, bem como em algoritmos que demonstram vieses raciais. No Brasil, conforme o Conselho Nacional de Justiça (2022), a solução ainda não encontra plena aplicação em esferas penais, o que significa que há uma oportunidade para discutir e legislar sobre o tema evitando que certos impactos negativos evitáveis atinjam a população amplamente.

Conforme Neves (2006), o fato de a sociedade moderna não mais apresentar a chamada "homogeneidade estratificada" pré-moderna torna a noção de igualdade mais complexa. Nesse sentido, o direito a igualdade só se concretiza de fato com o reconhecimento e a incorporação das diferenças sem privilégios, bem como com "o respeito recíproco e simétrico às diferenças" (NEVES, 2006, p. 167). A realidade social, porém, impõe uma desigualdade fática, o que implica, conforme Luhmann (2016), o conceito de igualdade depender da existência de um outro lado, que é a desigualdade.

Assim sendo, esse princípio só pode ser formulado ao incorporar a desigualdade como um de seus polos, de modo a entendê-lo como um convívio constante entre o igual e o desigual, com o objetivo de proporcionar a igualdade de direito a todos os membros da sociedade (NEVES, 2006). Para tanto, idealiza-se uma esfera pública pluralista, em que haja a neutralização das desigualdades fáticas, de maneira que as diferenças sejam respeitadas de forma recíproca entre os cidadãos. Assim, usando a concepção de Ronald Dworkin, a ideia consiste no direito a ser tratado "como um igual", e não de mero tratamento igual. Essas questões evocam as discussões sobre as políticas públicas de afirmação afirmativa e de discriminação social negativa para concretizar a igualdade jurídica. Pode-se observar tais dimensões também na programação de algoritmos de reconhecimento facial.

Quando um programa destinado a reconhecer rostos usa um banco de dados majoritariamente constituído por faces de pessoas brancas, tacitamente se admite a existência de um "padrão de seres humanos". Como lembra Galindo (2014), essa ideia é bastante perigosa, na medida em que qualquer ideia de "normalidade social" – que

busque estabelecer características aos pertencentes a esse *pool* – não passa de uma forma de discriminação, a qual tenta criar uma espécie de homogeneização da sociedade. É esse o desafio de regulamentos e de políticas públicas que procurem garantir a antidiscriminação: assegurar a igualdade jurídica àqueles entendidos como minorias, os que não têm hegemonia política e são ainda mais dependentes do ordenamento jurídico para verem os seus direitos se materializarem na realidade.

A legislação e as demais normas que se destinem a regular máquinas de reconhecimento facial — que atualmente inexistem nesse nível de especificidade — devem ser desenhadas de modo que a elas seja aplicado o princípio da igualdade. É interessante levar à discussão na sociedade civil e em âmbito legislativo, com ampla participação dos níveis do Estado e de grupos sociais, propostas para positivar uma garantia mínima que se aplique a serviços digitais, em especial aqueles que envolvam reconhecer pessoas, algo com sérias implicações. É necessário que os desenvolvedores e empresas por trás dessas soluções sejam provocados a reverem os seus bancos de dados e demais instâncias dos programas para que se garanta na prática a não existência de discriminação.

Segundo Almeida (2019), o racismo estrutural se dá quando a discriminação racial se manifesta em atitudes em que os autores não as reconhecem como racismo, sendo assim algo tão enraizado ao ponto de se tornar natural, o que torna o combate a tal fenômeno um complexo desafio. Desse modo, entende-se que é preciso determinar que os bancos de dados e de rostos desses programas tenham um mínimo estabelecido de diversidade. Dessa forma, busca-se não apenas a eficiência, mas também o que se chama de *ethics by design*, padrões éticos de desenvolvimento de sistemas (COMISSÃO EUROPEIA, 2021a).

Ainda, é importante ressaltar o que Neves (2014) entende sobre reconhecimento, inclusão e direitos humanos. Com base no proposto por Niklas Luhmann, o autor lembra que a inclusão se refere em especial às "situações em que as pessoas são dependentes das prestações dos sistemas sociais e têm acesso a elas" (NEVES, 2014, p. 4). O problema, porém, é quando as pessoas precisam da atuação do ordenamento na compensação de desigualdades materiais para que haja igualdade de direito, como visto, mas o direito furta-se dessa obrigação. Assim, pode-se constatar um grupo de pessoas subintegradas ou subincluídas que cumprem mais seus deveres com a coletividade do que tem os seus direitos efetivados. Em contrapartida, a parcela sobreintegrada ou sobreincluída tem seus direitos garantidos sem se vincular às responsabilidades jurídicas impostas. Dessa maneira, tem-se uma "fragilidade da esfera pública universalista e pluralista como espaço de heterolegitimação dos procedimentos do Estado constitucional" (NEVES, 2014, p. 7).

Com base nesse cenário, Neves (2014) lembra como os direitos humanos, apesar de terem um caráter universalizante, estão sujeitos ao chamado plano da dupla contingência, caracterizado pela interação entre *ego* e *alter*, estando aquele relacionado à esfera individual e este ao que se apresenta no convívio em sociedade. A negação do reconhecimento do outro ocorre por não suportar sua liberdade, não considerando seu comportamento uma ação, por ser diverso do projeto pelo ego. Apesar de poder haver inclusão sem reconhecimento, a generalização dessa negação torna-se um problema quando ultrapassa os limites da interação concreta e passa para o âmbito estrutural, relegando posições marginalizadas a certos grupos sociais de maneira generalizada.

Esse processo ocorre em diversas áreas da sociedade e pode ser levado com intensidade à seara do reconhecimento facial se as normas que regulam a tecnologia forem construídas com um grau muito grande de generalização e sem se debruçar sobre as minúcias técnicas relevantes. Aceitar algoritmos com vieses raciais, por exemplo, seria reafirmar que existem pessoas subincluídas na sociedade, no caso, na esfera do sistema e do banco de rostos utilizado, como ver-se-á mais à frente, o que não é compatível com um sistema democrático que preza pela igualdade jurídica de seus cidadãos. Assim sendo, não se pode deixar a negação do reconhecimento de certas parcelas da sociedade invadir também essa tecnologia.

Ademais, cumpre lembrar o que diz a Declaração de Princípios de Genebra da Cúpula Mundial sobre a Sociedade da Informação – CMSI (ITU, 2014). Essa reunião, que envolveu a presença de delegações de vários países em Genebra (Suíça), ocorreu no ano de 2003, em um momento em que a internet como se conhece e com o significado que tem hoje estava em processo de formação. O encontro foi bastante marcante, na medida em que se configurou como um marco histórico inicial em matéria de governança da internet. Nesse sentido, houve de fato de uma formulação principiológica que funcionou como carta de intenções de uma invenção da qual não se poderia saber com exatidão os efeitos, os quais são vistos com mais clareza atualmente, tendo em vista o uso em larga escala das tecnologias da informação e comunicação (TICs).

Na Declaração, tem-se uma seção de apenas quatro artigos que tratam das "dimensões éticas da Sociedade da Informação" (ITU, 2014, p. 33). Neles, há o estabelecimento de princípios éticos que devem ser tomados como base no desenvolvimento das atividades informacionais. Incluem-se, por exemplo, valores como a solidariedade, liberdade e igualdade (art. 56), bem como a promoção da justiça, dignidade e valor da pessoa humana (art. 57). Os direitos humanos/fundamentais são igualmente lembrados, bem como garantias, em específico, como a privacidade e a liberdade (art. 58). O art. 59 apresenta, ainda,

algumas medidas que devem ser adotadas de modo a evitar crimes de ódio, discriminação e afins por meio da rede, mas não determina algo especificamente voltado para a ação de empresas que atuam na área.

Novas menções à questão ética são feitas no Plano de Ação de Genebra (ITU: 2014), que estabelece metas e orientações para que os pontos estabelecidos na Declaração possam ser postos em prática. A Linha de Ação C10 trata das dimensões éticas da sociedade da informação e, apesar de mencionar a necessidade de aumentar a pesquisa e a consciência em relação à questão, apenas reforça que "todos os protagonistas da sociedade da informação" (p. 59) devem zelar por basicamente os mesmos princípios definidos nos arts. de 56 a 59 da Declaração, com ênfase no combate a crimes cibernéticos e às más práticas de usuários. É possível notar, pois, como a noção de empresas enquanto violadoras é algo distante da mente das delegações na CMSI.

É ainda mais restrito o espaço dedicado às questões éticas no Compromisso de Túnis, produto de outra Cúpula, que ocorreu em 2005 na capital da Tunísia. Há apenas uma menção, no art. 9º do texto (ITU, 2014, p. 69), quanto a continuar buscando "abordar as dimensões éticas da sociedade da informação", assim como na Agenda de Túnis para a sociedade da informação, a qual faz referência à seção da Declaração de Genebra. Nesse sentido, apesar de ambos os documentos estabelecerem e referendarem princípios importantes, é fundamental situar resoluções internacionais e ordenamentos jurídicos nacionais de modo a estimular que o desenvolvimento de novas tecnologias atue diretamente ao encontro da asseguração material da não discriminação.

Atualmente, existem iniciativas que buscam criar padrões mínimos que desenvolvedores devem seguir ao criar plataformas e sistemas que envolvam soluções como inteligência artificial e reconhecimento facial. Busca-se, assim, conscientizar empresas e atores do campo da tecnologia a não só não violarem direitos fundamentais, mas incluírem um padrão ético como base de seus sistemas. Protocolos como o da Comissão Europeia (2021a), por exemplo, partem dos mesmos princípios dos documentos apresentados, mas vão além, descrevendo mais o que deve ser feito. Aponta-se, ainda, para a importância de garantir transparência sobre os efeitos de algoritmos e mecanismos de *accountability* para assegurar o cumprimento das disposições.

Todavia, vale ressaltar que esse tipo de conjunto de regramentos ainda se encontra em grande medida restrito à esfera recomendatória, dependendo da adoção voluntária de empresas e desenvolvedores e/ou da pressão de organizações da sociedade civil para que encontrem algum vigor material. Desse modo, é importante que o direito se aproprie dessas exigências, coloque-as em discussão — inclusive com os seus principais destinatários — e faça com que, de recomendações, regras mais detalhadas tornem-se normas jurídicas. É imperativo que isso ocorra para que se possa entender que direitos antidiscriminatórios estão assegurados de maneira concreta na legislação no que se refere a tecnologias de reconhecimento facial e sistemas afins.

No Brasil, há principalmente duas leis que têm como objeto central questões relativas a internet e a proteção de dados em sistemas digitais. A primeira delas é a Lei n. 12.965/2014, que ficou conhecida como Marco Civil da Internet. Além de contar com algumas disposições de caráter técnico-organizacional, é notável como, nessa norma, predomina uma hermenêutica contratual, com um certo foco em relações de consumidor. É verdade que se observam garantias de direitos, incluindo uma menção genérica a "direitos humanos" (art. 2º, II), além da liberdade de expressão (art. 2º, *caput*) e até mesmo a pluralidade e a diversidade (art. 2º, III). Todavia, é notável como os direitos fundamentais são encaixados em uma única categoria, e não detalhados de maneira mais extensiva, além de não haver repercussões desses princípios em outros dispositivos da lei.

A segunda norma é a Lei n. 13.709/2018, conhecida como Lei Geral de Proteção de Dados (LGPD), tem como foco a proteção de dados de cidadãos, ante uma clara necessidade de se estabelecer limites nessa questão considerando ameaças à privacidade das pessoas por parte de grandes empresas de tecnologia. Essa legislação tem inspiração tanto no Marco Civil da Internet quanto no Regulamento Geral de Proteção de Dados da União Europeia, considerado marco normativo mundial nessa esfera.

Apesar de não se referir com aprofundamento a questões relacionadas a direitos antidiscriminatórios ou algoritmos relacionados ao reconhecimento facial, o art. 4º, inciso III, da LGPD exclui a sua vigência para o tratamento de dados para fins exclusivamente de segurança pública, do Estado, da defesa nacional ou de "atividades de investigação e repressão de infrações penais". Isso cria uma lacuna de suma importância na legislação, a qual tem o potencial de abrir brechas para a violação de direitos fundamentais na esfera da segurança pública (SILVA e SILVA, 2019), área em que se podem observar violações generalizadas (SOUZA, 2015).

Nesse sentido, é importante sistematizar quais são as principais mudanças na legislação que podem ocorrer, assim como em que estágio estão as discussões sobre proteção de dados e limitação ao reconhecimento facial em diversas esferas, com ênfase no processo legislativo. Também é importante recorrer a modelos de regulação e/ou protocolo já existentes, de modo a compreender o que a legislação brasileira pode incorporar, bem como o que é particular do país de forma a exigir que uma disposição legal assegure certa regra em razão de uma especificidade, como é o caso da diversidade étnico-racial brasileira.

3. AS TECNOLOGIAS DE RECONHECIMENTO FACIAL E SUAS POTENCIAIS AMEAÇAS AOS DIREITOS FUNDAMENTAIS

A tecnologia que permite uma máquina reconhecer rostos, sem dúvidas, representa o alto grau de desenvolvimento tecnológico atingido pelo mundo, em especial pelos países mais desenvolvidos. Diversas implicações sociais, porém, são geradas a partir dessas criações, como a desinformação nas redes sociais, que geram posteriores discussões em âmbito social, legislativo e judiciário no sentido de como não permitir que a tecnologia vá de encontro a direitos fundamentais estabelecidos.

Dessa forma, enquanto o ordenamento jurídico não formula entendimentos sobre a matéria, vigora o costume, cuja majoritária fonte são as grandes empresas do ramo de tecnologia da informação, conhecidas como *big techs*, mas também companhias menores que têm sistemas de reconhecimento facial, matéria tratada neste artigo. Dada a ausência ou insuficiência de regulação, esse costume muitas vezes age em substituição ou competição com preceitos fundamentais, utilizando a classificação proposta por Helmke e Levitsky (2004). É dizer, como, na prática, as instituições formais não se imperam de maneira forte o suficiente, uma vez que a vontade da indústria é o que realmente vigora.

Para melhor compreender como exatamente essas tecnologias podem representar ameaças aos direitos humanos, cumpre fazer uma análise de como elas e os algoritmos de reconhecimento facial funcionam. Trata-se de uma maneira de observar possíveis lacunas éticas na programação desses sistemas, assim como — e especialmente — de espaços técnicos que as normas jurídicas não atingem. Promover entendimento amplo do funcionamento técnico desses programas é uma maneira de melhor traçar formas de regulá-los, inclusive descobrindo o que necessita ser modificado para não ir de encontro à legislação.

De acordo com Ruback, Ávila e Cantero (2021), o reconhecimento facial consiste em uma tecnologia que tem como base o aprendizado de máquina, utilizando algoritmos programados para realizar identificações a partir da extração de padrões de grandes volumes de dados inseridos. A mecânica dos sistemas é analisar a geometria da face, com base nos chamados pontos nodais, de modo a criar uma espécie de assinatura facial, armazenada em bancos de dados. São analisadas, no processo, características, como idade, gênero e estado emocional. Esses dados, junto ao algoritmo e ao modo de funcionamento dos sistemas, são cruciais para determinar como eles trabalharão e quais serão seus resultados e impactos. Por mais que se defenda que essas máquinas são "neutras", é notável que elas apresentam uma subjetividade em seus resultados, a depender de como foram programadas, conforme Rosa, Pessoa e Lima. (2020), o que pode causar efeitos danosos em matéria de discriminação, principalmente étnico-racial.

Sistemas de aprendizado de máquina — como os de reconhecimento facial — funcionam por meio de algumas etapas (RUBACK; ÁVILA e CANTERO, 2021). Inicia-se com uma coleta de dados e com uma classificação, que é uma maneira de o sistema atribuir faces identificadas a uma classe ou a um rótulo. Assim, utilizam-se dados de teste para observar o nível de falhas que o algoritmo apresenta, tabulando-os no que se chama de matriz de confusão. Há resultados positivos e negativos, sendo eles verdadeiros ou falsos. Pode-se dizer que essa etapa oferece a possibilidade de estabelecer padrões mínimos objetivos para que um sistema de reconhecimento facial tenha a permissão de uso. É justamente um número muito grande de falsos positivos que representa uma afronta a direitos fundamentais (BARROS e SILVA, 2020).

Para além de falsos positivos e negativos, porém, é importante ressaltar outro fenômeno que apresenta sérias ameaças aos direitos antidiscriminatórios: o chamado viés, em especial o viés racial (BUOLAMWINI e GEBRU, 2018), presente em algoritmos de aprendizado de máquina e, por conseguinte, no reconhecimento facial. Em razão de o sistema fazer predições com base nos dados inseridos nele, é justamente essa base de dados que cria certas tendências nesses sistemas, as quais costumeiramente são em prejuízo de pessoas negras. Silva (2022) mostra, por exemplo, como os mais diversos programas, por não se atentarem à necessidade de garantir o respeito à diversidade, acabam por funcionar quase sem considerar a existência de pessoas não brancas, como é o caso de câmeras que alertam que pessoas amarelas estariam com os olhos fechados ou de carros autônomos melhor treinados para identificar pessoas de pele clara.

Um diagnóstico cuidadoso das etapas que envolvem a construção de algoritmos usados no reconhecimento facial (coleta, avaliação e processamento de dados) revela como esses vieses podem surgir. Inicialmente, a própria coleta de dados já pode ser bastante problemática, tendo em vista que comumente são utilizados bancos pré-existentes (RUBACK; ÁVILA e CANTERO, 2021), inclusive muitas vezes feitos por grupos estrangeiros. Esse é um espaço claro para a atuação de regulações ou mesmo de um banco de rostos público e nacional que deva ser usado em sistemas feitos para o Brasil: é necessário que os rostos sejam representativos da composição étnica da população brasileira de modo a evitar desvios apriorísticos (SURESH e GUTTAG, 2019).

Tem-se, ainda, as etapas de pré-processamento — em que os dados são filtrados e partidos em dados de treinamento e de teste —, de criação do modelo — quando vários algoritmos são testados, o que determina como o sistema usa os dados — e, por fim, de avaliação do modelo e de pós-processamento. De acordo com Ruback,

Ávila e Cantero (2021), os dados de teste são dados não utilizados antes na construção do sistema, de modo a ser uma maneira mais confiável de observar como o sistema está se comportando. Outros utilizados são os dados de referência, cujos modelos existentes disponíveis, em grande parte oriundos de instituições e de grupos dos Estados Unidos da América, o que também demonstra afastar sistemas criados da realidade brasileira e de países do Sul global.

Com base nessas etapas, Suresh e Guttag (2019) identificaram seis vieses que podem estar presentes nas máquinas de reconhecimento facial. O primeiro deles é o histórico, que se manifesta antes mesmo da própria criação dos sistemas, para reafirmar discriminações presentes na sociedade. Tem-se, então, o de representação, que se refere ao problema de a amostra não ser representativa em relação à população a que o algoritmo se destina; o de avaliação, relacionado à etapa de teste e às discussões sobre como metrificar os resultados do sistema a contento; e o de interpretação humana, que tem como origem a relação das pessoas com a tecnologia, na fase de pós-processamento dos dados. Outros dois vieses apontados são o de agregação, que consiste em desconsiderar as diferenças entre grupos sociais distintos; além do de aprendizado, quando escolhas de modelagem amplificam disparidades nos dados.

Esses vieses podem ser usados como guias para uma discussão sobre essa problemática com vistas à produção de regulação sobre o reconhecimento facial. Pode-se entendê-los como problemas já conhecidos da referida tecnologia e que precisam de uma regulação clara que obrigue desenvolvedores a de fato tentarem evitá-los de modo objetivo. Uma lacuna, portanto, é o de permitir que violações continuem acontecendo, além de depender da iniciativa voluntária de empresas que desenvolvem essas tecnologias no respeito a padrões éticos mínimos, o que não parece razoável em um Estado de Direito.

Grother, Quinn e Phillips (2011), por exemplo, mostram como esses vieses podem estar associados ao local de desenvolvimento de algoritmos de reconhecimento facial. Rosa, Pessoa e Lima (2020) "reforça[m] o elemento de raça enquanto relacional e circunscrito" (p. 6), na medida em que mostram como cada país desenvolve sistemas que se adequam melhor aos fenótipos da etnia da maioria das suas respectivas populações. Na China, no Japão e na Coreia do Sul, as tecnologias reconheciam melhor amarelos, enquanto na Alemanha e nos Estados Unidos, os sistemas tinham melhores resultados com caucasianos.

Vale lembrar que a pesquisa do National Institute of Technology (GROTHER; QUINN e PHILLIPS, 2011) foi feita quase dez anos depois de um primeiro levantamento e, comparando ambos, pôde-se notar como a problemática em relação a pessoas não brancas não apenas continua existindo como se agravou. O número de falsos positivos que envolve negros, asiáticos e centro-americanos, segundo a pesquisa, é especialmente alto, enquanto os falsos positivos em relação a brancos dos EUA ou da Europa não são tão numerosos. Também se constatou que esse desempenho está diretamente ligado ao banco de dados usado para treinar a máquina. Em uma população tão miscigenada e diversa como a brasileira, é essencial que os dados também incorporem essa diversidade.

É importante ressaltar potenciais violações a direitos, como o de imagem, conforme ressaltam Conceição, Viana e Rocha (2019). De acordo com os autores, é essencial considerar um conflito entre interesses públicos e privados no uso do reconhecimento, com a supremacia, de modo geral, dos públicos. No caso da utilização da tecnologia em matéria de segurança, pode-se observar que as pessoas estão sendo constantemente vigiadas, o que traz implicações em matéria de direito de imagem, bem como de privacidade, embora a atividade esteja sendo feita em nome do interesse público. Dessa forma, destaca-se que a ação do Estado também deve ser regulada, de modo a não haver excessos e violações de direitos dos cidadãos, que devem ser protegidos pela organização estatal.

Ainda, existem posições que entendem que os vieses presentes em sistemas de reconhecimento facial e questões relacionadas à privacidade e ao tratamento correto de dados impedem totalmente a utilização desses sistemas em razão dos riscos sistemáticos de violações de direitos humanos. Para Possa (2022), o uso desse tipo de tecnologia reforça o chamado Estado de Coisas Inconstitucional (STF, 2015), na medida em que tira das pessoas o poder sobre os dados que estão sendo coletados sobre si. A empresa International Business Machines (IBM) também já se manifestou taxativamente contra o emprego de criações desse tipo na área da segurança pública pelos riscos de discriminação, após desenvolver um estudo sobre a questão, mostrando a seriedade dessas preocupações (POSSA, 2022).

Apesar dessa posição da IBM, é importante considerar o que destaca Canto (2019), que grandes empresas do ramo da tecnologia lançam padrões éticos a serem seguidos por elas próprias, embora isso apenas constitua o que a autora chama de narrativa ética, ou seja, por mais que mostrem alguma preocupação – ainda que formal – com a definição de limites para suas inovações, não o aplicam na prática. A Microsoft, por exemplo, ainda que defenda a criação de princípios éticos para o uso do reconhecimento facial, "continua trabalhando junto ao setor militar em diversos países ao redor do globo" (CANTO, 2019, p. 13). Essa dinâmica mostra a necessidade de o direito incorporar essas questões e fazer valer de fato, nessa esfera, os direitos fundamentais já positivados.

Nesse sentido, é fato que é desejável que o reconhecimento facial seja discutido no Legislativo, incluindo as suas implicações em âmbito social e jurídico, de modo a formular entendimentos que sejam transformados em

regulações. Dessa forma, é importante entender que no Brasil já se regula de alguma maneira a criação tecnológica supracitada, assim como as perspectivas normativas para o futuro no país em relação ao tema. Também se deve explorar propostas e ideias colocadas por grupos ou outros países, bem como normas em vigor em outras nações, de modo a situar o estado da arte da problemática.

4. PERSPECTIVAS DE REGULAÇÃO DO RECONHECIMENTO FACIAL NO BRASIL

Ainda que não sejam muito usadas no Brasil (CNJ, 2022), já existem tecnologias de reconhecimento facial em diversas áreas. De acordo com o Instituto Igarapé (2019), há uso desse tipo de tecnologia em áreas, como educação, transporte, controle de fronteiras e segurança pública. Como lembram Barros e Silva (2020), algumas empresas usam câmeras em meios de transporte públicos para evitar fraudes com bilhetes, além das controversas utilizações para busca de suspeitos de crimes e foragidos da Justiça.

Segundo Nunes (2019), 90,5% das pessoas identificadas como suspeitas de delitos por um sistema de reconhecimento facial usado pelo governo da Bahia eram negras, o que mostra a urgência em formular regramentos e padrões éticos mínimos a serem seguidos.

Uma norma que mostra o perigo de regras muito abstratas e sem um nível mínimo de detalhamento é a Portaria n. 793, de 24 de outubro de 2019, do Ministério da Justiça e Segurança Pública, que regulamenta o incentivo financeiro das ações do programa Eixo Enfrentamento à Criminalidade Violenta. Em seu art. 4º, § 1º, inciso III, alínea *b*, há previsão de "fomento à implantação de sistemas de videomonitoramento com soluções de reconhecimento facial, por *Optical Character Recognition* – OCR, uso de inteligência artificial ou outros" (BRASIL, 2019). Ainda que se possa utilizar soluções do tipo, a falta de um padrão abre bastante margem para abusos com a tecnologia e em uma área que já padece de uma situação grave em se tratando de violações.

Existem algumas iniciativas legislativas que buscam regular tecnologias que interagem com o reconhecimento facial, ainda que não haja nenhum projeto que tenha como objeto a tecnologia em específico. Diante das limitações impostas pelo art. 4º da LGPD, a Câmara dos Deputados criou um Grupo de Juristas (CÂMARA DOS DEPUTADOS, 2019) destinado a redigir um "anteprojeto de legislação específica para o tratamento de dados pessoais no âmbito da segurança pública, investigações penais e repressão de infrações penais". Note-se que a segurança de Estado e a defesa nacional não foram abrangidas pelo trabalho do grupo. No fim de 2020, após algumas renovações do período de trabalho do grupo, foi apresentado o Anteprojeto de Lei de Proteção de Dados para segurança pública e persecução penal (2020). Em seus arts. de 42 a 44, ele trata de "tecnologias de monitoramento e tratamento de dados de elevado risco", entre as quais figura o reconhecimento facial.

O anteprojeto apresenta alguns pontos importantes em matéria de asseguração de padrões éticos mínimos e de direitos fundamentais. O art. 42, por exemplo, estabelece que deve haver uma avaliação de risco prévia ao uso de tecnologias de monitoramento, a qual, de acordo com o § 1º, inciso VI, do artigo deve considerar "a possibilidade de tratamento discriminatório". Outro aspecto de destaque é o art. 43, que veda a utilização do reconhecimento facial na segurança pública "diretamente acrescida de técnicas de identificação de pessoas indeterminadas em tempo real e de forma contínua quando não houver a conexão com a atividade de persecução penal individualizada e autorizada por lei e decisão judicial". Caso mantido como está e aprovado, tem-se uma garantia sólida no âmbito da segurança pública, um tema que é palco de violações recorrentes.

É importante, contudo, sublinhar possíveis limitações que a atual redação do anteprojeto pode conter. Conforme ressaltam Lemos *et al.* (2021), o texto deixa dúvidas em relação ao sentido de persecução penal individualizada. Os autores apresentam como exemplo um sistema que, ainda que esteja buscando uma ou algumas pessoas contra quem há mandados de prisão, façam-no por meio de uma varredura contínua, com o uso de bancos de dados com milhões de rostos, ou mesmo com a análise de rostos de transeuntes de algum local. Suscita-se, então, questionamentos com relação ao que pode ser considerado individual. Também não é muito claro o que se considera como contínuo, o que novamente pode trazer insegurança jurídica na regulação dessas tecnologias (LEMOS *et al.*, 2021).

Há, ainda, o Projeto de Lei n. 21/2020, de autoria do Deputado Federal Eduardo Bismarck (PDT/CE), que tem o objetivo de estabelecer regulação para a inteligência artificial. Existem, nesse sentido, alguns pontos que interessam à seara do reconhecimento facial, como o estabelecimento da não discriminação como um princípio do desenvolvimento de sistemas do tipo (art. 5º, III) e da necessidade de mitigar vieses "contrários ao disposto na legislação vigente" (art. 5º, IV). É questionável, porém, o que o projeto prevê quanto à intervenção subsidiária do poder público, ao versar que "regras específicas deverão ser desenvolvidas para os usos de sistemas de inteligência artificial apenas quando absolutamente necessárias [...]", o que pode ocasionar lacunas sensíveis.

Ainda assim, o PL aborda diversos pontos relevantes, tais como participação social, atuação setorial, gestão baseada em risco e monitoramento do impacto. Ressalta-se também quão relevante é disciplinar as atribuições tanto do poder público como um ator de monitoramento quanto com relação aos limites de uso de tecnologias do tipo em políticas públicas e na segurança pública. Tendo

em vista que o Estado tem uma grande capacidade de executar algumas aplicações em larga escala do reconhecimento facial, notadamente na esfera da segurança pública, é essencial que a administração pública seja limitada a não o fazer de maneira discriminatória e com uso de sistemas enviesados.

Outro ato normativo relevante para a discussão ora proposta é o PL n. 1.515/2022, de autoria do Deputado Federal Coronel Armando (PL/SC), que tem como objetivo preencher a lacuna da LGPD nas áreas de defesa nacional, segurança pública e investigação e repressão penais. Ele inclui a não discriminação no rol de princípios (art. 4º, IX) que devem ser seguidos pelas atividades de tratamento e compartilhamento de dados nos referidos campos, mas a autodeterminação informativa (SANTARÉM *et al.*, 2022), que consiste no direito de controle sobre seus dados, não se encontra presente no projeto. Ainda, é notável como as referências a tecnologias de monitoramento/reconhecimento facial foram suprimidas desse PL, de modo que simplesmente não há referência direta a essas tecnologias, além de haver não haver ênfase à necessidade de análise de impacto. Esses pontos assinalam o projeto como um retrocesso em matéria da proteção de direitos antidiscriminatórios.

De todo modo, vale reconhecer que as propostas legislativas expostas anteriormente não têm como foco exatamente a questão do reconhecimento facial, de modo que a análise buscou extrair de projetos de temas relacionados o que eles tratam que também pode ter repercussões em relação ao tipo de tecnologia que é o foco da pesquisa. Isso mostra como o reconhecimento facial pode não estar mobilizando tanto o debate público quanto outros temas correlatos, a exemplo da inteligência artificial e das lacunas da LGPD — ao menos no âmbito legislativo. Caso comprovada, essa diferença na intensidade das discussões sobre o tema no país pode abrir margem para que a legislação se mantenha lacônica e não incorpore regulações que são importantes para assegurar o combate a vieses raciais nessas inovações.

Também podem ser exploradas regulações e propostas de regramentos adotadas ou sugeridas em outros países, alguns com uso do reconhecimento facial mais avançado, a fim de buscar aprender com outras experiências, sempre respeitando as especificidades de cada realidade. Na União Europeia (UE), considerada pioneira nas discussões e regulação em matéria de privacidade de dados e questões digitais de modo geral, alguns princípios importantes foram formulados. Em um relatório (COMISSÃO EUROPEIA, 2021a) que formula bases para o desenvolvimento da inteligência artificial no bloco que segue o modelo de *ethics by design* — ou seja, que parte da perspectiva ética —, podem ser observadas duas dimensões importantes.

A primeira delas é a da autonomia, em que sistemas que usam a IA não podem restringir a liberdade das pessoas de seguirem suas vidas conforme suas expressões culturais diversas, as quais precisam ser consideradas no desenvolvimento dessas tecnologias. Quando isso não é feito e se considera que as pessoas são homogêneas, restringem-se as possibilidades de opções dessas tecnologias, além de abrir-se margem para vieses discriminatórios. A segunda é a dignidade, chamando a atenção para o fato de que os seres humanos não podem ser "instrumentalizados, objetificados ou desumanizados" (COMISSÃO EUROPEIA, 2021a, p. 6), de modo que esses sistemas precisam respeitar essa dimensão em todas as instâncias.

Outro ponto importante proposto pela UE é a questão do risco, também contemplada em propostas legislativas brasileiras. Conforme lembram Chen e Wang (2022), uma proposição da Comissão Europeia (2021b) estabelece uma abordagem baseada no risco, com classificações de inaceitável, alto e baixo ou médio risco, com base em como a tecnologia interage com a sociedade. Dessa forma, propõe-se que sejam banidos sistemas de identificação biométrica em tempo real, bem como aqueles de "crédito social" baseados em IA, além de se lembrar da necessidade de fortalecer restrições a aplicações de alto risco de inteligência artificial. O anteprojeto de lei formulado no Brasil com relação à segurança pública apresenta uma formulação semelhante, embora contenha exceções, como visto.

Um relatório do Serviço de Estudos do Parlamento Europeu (MADIEGA e MILDEBRATH, 2021) ressalta, ainda, a questão dos vieses e do potencial discriminatório de tecnologias de reconhecimento facial. Nele, os autores também lembram das questões anteriormente trabalhadas nesta pesquisa em relação a falsos positivos e negativos, assim como de dados de treino insuficientes como uma das causas de vieses algorítmicos, o que tem um impacto sensível na asseguração de direitos fundamentais. Um ponto importante indicado é que a alta incidência de falsos positivos nos Estados Unidos, por exemplo, altera a noção de presunção de inocência ao impor a necessidade de provar que sistemas enviesados estão errados. Expõe-se, ainda, a preocupação de que a referida tecnologia pode intensificar injustiças contra grupos que já têm uma posição marginalizada.

Alguns casos concretos de empresas que foram punidas em razão de sistemas de reconhecimento facial, conforme Chen e Wang (2022), na China, nos Estados Unidos e na União Europeia, mostram que o tema central ainda é a privacidade. Nos três casos analisados pelos autores, empresas coletaram dados sem a autorização dos usuários e foram condenadas a fazer reparações, bem como tiveram de apagar os dados. A questão dos dados é com certeza a que mais mobiliza discussões em matéria de governança da internet e regulação dessa área, todavia, não se pode esquecer dos potenciais impactos negativos que podem ter algoritmos programados sem

a necessidade de levar em consideração a diversidade étnico-racial das sociedades.

Na América Latina, conforme análise de Silva, Franqueira e Hartmann (2021), a legislação concernente ao reconhecimento facial tem como foco, de maneira geral, questões ligadas ao consentimento em relação às pessoas que estão sendo gravadas, além de haver diferenciação nas regulações ligadas à segurança pública — como no Brasil. Notam-se também preocupações com uma questão recorrente na discussão sobre proteção de dados, que é o compartilhamento de informações pessoais/biométricas sem o devido consentimento, em especial em hipóteses ligadas à segurança pública, em que são suscitados debates em relação a direitos individuais e interesses coletivos.

Alguns pontos observados pelos autores, que defendem um reconhecimento facial essencialmente antidiscriminatório, são, por exemplo, a falta de um marco legal sobre o tema em vários países, abrindo margem para aplicações desreguladas da tecnologia, além da necessidade de mecanismos de *accountability*, também importantes para barrar e/ou desestimular usos arbitrários da tecnologia. Outra questão que é de competência da execução de políticas públicas é a escolha pela localização desses mecanismos de identificação, que muitas vezes também podem reproduzir intenções de discriminar (BOTELLO, 2016). Fussey e Murray (2019) também apontam para a necessidade de realizar treinamentos para melhor aplicação da referida inovação.

Ainda, Morales (2021) aponta para alguns tipos de discriminação que podem incidir sobre a LGPD, também podendo ser pensados no âmbito do reconhecimento facial. Há a discriminação por associação, que ocorre em razão da aproximação de pessoas a grupos que são alvos da prática em razão de critérios que promovem esse fenômeno, algo que pode ocorrer com a classificação em rótulos dos referidos sistemas. Há, ainda, a indireta, que, conforme trabalhado na seção sobre direitos antidiscriminatórios, acontece com a pressuposição de neutralidade, a qual não considera as necessidades materiais que existem para uma real promoção da igualdade de direito. Por fim, a autora aponta a discriminação inconsciente, na esteira do que Almeida (2019) define como racismo estrutural, um preconceito tão disseminado e naturalizado que deixa de ser assim reconhecido, e como Neves (2014) trabalha a questão da exclusão. Todos esses fenômenos sociais podem ser refletidos no desenvolvimento de sistemas de identificação facial se não houver um padrão mínimo a ser seguido nesse processo.

5. CONSIDERAÇÕES FINAIS

Como pôde ser visto, inovações em matéria de tecnologia implicam também inovações sociais e jurídicas. É necessário que a igualdade de direito se materialize no desenvolvimento de algoritmos de reconhecimento facial; caso contrário, essas inovações estimularão a discriminação. A fim de que isso não ocorra, as normas jurídicas precisam contar com um grau de especificidade necessário para que não deixe margem, por exemplo, para a existência de vieses raciais. O reconhecimento desses fenômenos por parte das normas jurídicas, pois, é vital para a concretização de direitos antidiscriminatórios nessa esfera.

A maneira que os *softwares* de reconhecimento facial **são desenvolvidos abre bastante margem para que** se reproduza padrões de discriminação, conforme também se mostrou ao longo do texto. De modo frequente, os chamados vieses são inseridos nos meios de funcionamento desses sistemas de forma que, por mais que não sejam intencionais, envolvem a desconsideração de necessidades importantes para que as tecnologias sejam verdadeiramente inclusivas.

Reconhecer o direito à igualdade significa, muitas vezes, não agir simplesmente de maneira neutra, mas corrigir desigualdades materiais para que todos possam ter seus direitos igualmente respeitados. Não usar bancos de dados que incluam rostos tão diversos como a população brasileira, por exemplo, em se tratando de um sistema a ser usado no Brasil, é sinal do que Neves (2014) chama de negação generalizada do reconhecimento, direcionada a pessoas já marginalizadas pela sociedade. Dessa forma, **é** imperativo que bancos de dados sejam diversos de modo a evitar os vieses.

É verdade que algumas empresas vêm se posicionando publicamente em relação à problemática e reconhecendo a questão. Todavia, conforme Canto (2019), não é possível confiar unicamente na atuação das empresas. Ainda que se formulem padrões como o *ethics by design* (COMISSÃO EUROPEIA, 2021a), não se pode apenas esperar que desenvolvedores o adotem voluntariamente. É necessário, por meio de um diálogo multissetorial, adotar um regulamento com força de lei para que não seja permitido o uso de sistemas de reconhecimento facial que não adotem padrões mínimos antidiscriminatórios.

A análise do estado da discussão legislativa sobre o reconhecimento facial no Brasil mostra que existe uma pequena inserção da temática em proposições legislativas recentes, notadamente de princípios antidiscriminatórios. Todavia, é necessário que haja não apenas uma norma dedicada ao reconhecimento facial, mas que aborde a questão dos vieses e que conte com uma definição de padrões técnicos mínimos com garantias éticas e antidiscriminatórias.

Assim sendo, cabe também à sociedade civil exercer o papel de pressionar legisladores para que esses elementos possam ser tema de legislações futuras. O conhecimento sobre essas questões é fundamental para que isso possa acontecer, de modo que o presente artigo se coloca como mais um ponto no debate teórico e jurídico que objetiva

assegurar um reconhecimento facial antidiscriminatório. É por meio deste que poderão ser vistas mudanças no ordenamento que impactem a sociedade e não permitam a reprodução de padrões de exclusão e discriminação com populações que já enfrentam tais problemáticas na sociedade brasileira e no mundo.

REFERÊNCIAS

ALMEIDA, Silvio. **Racismo estrutural**. São Paulo: Jandaíra, 2019. 256 p.

ANTEPROJETO DE LEI DE PROTEÇÃO DE DADOS PARA SEGURANÇA PÚBLICA E PERSECUÇÃO PENAL. **Comissão de Juristas instituída por Ato do Presidente da Câmara dos Deputados de 26 nov. 2019**. Presidente: Min. Néfi Cordeiro. Disponível em: https://static.poder360.com.br/2020/11/DADOS-Anteprojeto-comissao-protecao-dados-seguranca-persecucao-FINAL.pdf. Acesso em: 9 jun. 2023.

BARROS, Isabela Maria Pereira Paes; SILVA, Isabela Inês Bernadino de Souza. Utilização do reconhecimento facial por empresas para identificação de suspeitos: segurança ou violação do Estado Democrático de Direito? **Revista Transgressões**, Natal, v. 8, n. 1, p. 57-76, 2020. Disponível em: https://periodicos.ufrn.br/transgressoes/article/view/19909. Acesso em: 9 jun. 2023.

BOTELLO, Nelson Arteaga. Regulación de la videovigilancia en Mexico: gestión de la ciudadanía y acceso a la ciudad. **Espiral**, Guadalajara, v. 23, n. 66, maio/ago. 2016. Disponível em: https://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S1665-05652016000200193. Acesso em: 10 mar. 2023.

BRASIL. **Lei n. 12.965, de 23 de abril de 2014.** Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Brasília: Presidência da República, 2014. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 9 jun. 2023.

BRASIL. **Lei 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília: Presidência da República, 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 9 jun. 2023.

BRASIL. Ministério da Justiça e Segurança Pública. **Portaria n. 793**, de 24 de outubro de 2019. Brasília: Imprensa Nacional, [2019]. Disponível em: https://www.in.gov.br/en/web/dou/-/portaria-n-793-de-24-de-outubro-de-2019-223853575. Acesso em: 2 mar. 2023.

BUOLAMWINI, Joy; GEBRU, Timnit. Gender shades: intersectional accuracy disparities in commercial gender classification. **Proceedings of Machine Learning Research**, v. 81, p. 1-15, 2018. Disponível em: http://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf. Acesso em: 3 mar. 2023.

CÂMARA DOS DEPUTADOS. **Ato do Presidente de 26 de nov. 2019**. Institui Comissão de Juristas destinada a elaborar o anteprojeto de legislação específica para o tratamento de dados pessoais no âmbito da segurança pública, investigações penais e repressão de infrações penais, conforme o disposto no artigo 4º, inciso III, alíneas "a" e "d" da Lei n. 13.709, de 14 de agosto de 2018. Brasília: Câmara dos Deputados, 2019.

CANTO, Mariana. Made in surveillance: a regulação da importação e do uso de tecnologias de vigilância estrangeiras e a relativização dos direitos fundamentais e da soberania estatal. In: SIMPÓSIO INTERNACIONAL LAVITS, 6, 2019, Salvador. **Anais** [...]. Salvador: LAVITS, 2019. Disponível em: http://lavits.org/wp-content/uploads/2019/12/Canto-2019-LAVITS.pdf. Acesso em: 9 mar. 2020.

CHEN, Wenhao; WANG, Min. Regulating the use of facial recognition technology across borders: a comparative case analysis of the European Union, the United States, and China. **Telecommunications Policy**, vol. 47, n. 2, mar. 2022. Disponível em: https://doi.org/10.1016/j.telpol.2022.102482. Acesso em: 11 fev. 2023.

CONCEIÇÃO, V. S.; VIANA, C. C.; ROCHA, A, M. Reconhecimento Facial e a relativização do direito de imagem. **Revista Ingi**, Aracaju, v. 3, n. 3, p. 436-450, jul./set., 2019.

COMISSÃO EUROPEIA. **Ethics by design and ethics of use approaches for artificial intelligence.** Bruxelas: European Commission, 2021a. Disponível em: https://ec.europa.eu/info/funding-tenders/opportunities/docs/2021-2027/horizon/guidance/ethics-by-design-and-ethics-of-use-approaches-for-artificial-intelligence_he_en.pdf. Acesso em: 20 fev. 2023.

COMISSÃO EUROPEIA. **Proposal for a regulation of the european parliament and of the council**: laying down harmonised rules on artificial intelligence (artificial intelligence act) and amending certain union legislative acts. Bruxelas: European Commission, 2021b. Disponível em: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52021PC0206. Acesso em: 9 jun. 2023.

CONSELHO NACIONAL DE JUSTIÇA. Departamento de Monitoramento e Fiscalização do Sistema Carcerário e do Sistema de Execução de Medidas Socioeducativas. **Grupo de Trabalho Reconhecimento de Pessoas**. Brasília: CNJ, 2022. Disponível em: https://www.cnj.jus.br/wp-content/uploads/2022/12/relatorio-final-gt-sobre-o-reconhecimento-de-pessoas-conselho-nacional-de-jusica.pdf. Acesso em: 9 jun. 2023.

FUSSEY, Pete; MURRAY, Daragh. **Independent Report on the London Metropolitan Police Service's Trial of Live Facial**

Recognition Technology. Essex: ESRC, Human Rights Center, University of Essex, 2019. Disponível em: https://repository.essex.ac.uk/24946/1/London-Met-Police-Trial-of-Facial-Recognition-Tech-Report-2.pdf. Acesso em: 10 mar. 2023.

GALINDO, Antonella. O direito antidiscriminatório entre a forma e a substância: igualdade material e proteção de grupos vulneráveis pelo reconhecimento da diferença. *In*: FERRAZ, Carolina Valença; LEITE, Glauber Salomão (orgs.). **Direito à diversidade**. São Paulo: Atlas, 2014, p. 43-60.

GROTHER, Patrick J.; QUINN, George W.; PHILLIPS, P. Johathon. **Report on the Evaluation of 2D Still-Image Face Recognition Algorithms**: NIST Interacy Report 7709. [s.l]: NIST, 2011. Disponível em: https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=905968. Acesso em: 12 mar. 2023.

HELMKE, Gretchen; LEVITSKY, Steven. Informal Institutions and Comparative Politics: a research agenda. **Perspectives on Politics**, v. 2, n. 4, dez. 2004, p. 725-740. Disponível em: https://wcfia.harvard.edu/files/wcfia/files/883_informal-institutions.pdf. Acesso em: 20 fev. 2023.

INSTITUTO IGARAPÉ. **Reconhecimento facial no Brasil**, 2019. Rio de Janeiro: Instituto Igarapé, 2019. Disponível em https://igarape.org.br/infografico-reconhecimento-facialno--brasil. Acesso em: 25 fev. 2023.

INTERNATIONAL TELECOMMUNICATION UNION (ITU). **Documentos da Cúpula Mundial sobre a Sociedade da Informação**: Genebra 2003 e Túnis 2005. Tradução Marcelo Amorim Guimarães. São Paulo: Comitê Gestor da Internet no Brasil, 2014. *E-book*.

LEMOS, A.; FERNANDES; E.; MEDEIROS, J; GUEDES, P.; SILVA, P. **Comentários ao Anteprojeto de Lei de Proteção de Dados para a Segurança Pública: Tecnologia de Reconhecimento Facial**. Rio de Janeiro: ITS Rio, 2021. Disponível em: https://itsrio.org/wp-content/uploads/2021/04/UK-Comentarios_LGPDPenal.pdf. Acesso em: 4 mar. 2023.

LUHMANN, Niklas. **O Direito da Sociedade**. São Paulo: Martins Fontes, 2016.

MADIEGA, T.; MILDEBRATH, H. **Regulating facial recognition in the EU. In-Depth Analysis**. Bruxelas: Serviço de Estudos do Parlamento Europeu, 2021.

MORALES, L. X. Tutela antidiscriminatória na Lei Geral de Proteção de Dados: problemáticas e alternativas. **Internet & Sociedade**, São Paulo, v. 2, n. 2, p. 67-89, dez. 2021. Disponível em: https://revista.internetlab.org.br/wp-content/uploads/2022/03/Tutela-antidiscriminatoria-na-Lei-Geral-de-Protecao-de-Dados-problematicas-e-alternativas.pdf. Acesso em: 9 jun. 2023.

NEVES, Marcelo. **Entre Têmis e Leviatã: uma relação difícil**. São Paulo: Martins Fontes, 2006.

NEVES, Marcelo. Direitos Humanos: inclusão ou reconhecimento? *In*: FERRAZ, Carolina Valença; LEITE, Glauber Salomão (orgs.). **Direito à diversidade**. São Paulo: Atlas, 2014, p. 3-17.

NUNES, Pablo. Novas ferramentas, velhas práticas: reconhecimento facial e policiamento no Brasil. *In:* RAMOS, Silvia (coord.). **Retratos da violência**: cinco meses de monitoramento, análises e descobertas. Rio de Janeiro: Rede de Observatórios de Segurança, 2019. Disponível em: https://cesecseguranca.com.br/wp-content/uploads/2019/11/Rede-de-Observatorios_primeiro-relatorio_20_11_19.pdf. Acesso em: 9 jun. 2023.

POSSA, Alisson. O reconhecimento facial como instrumento de reforço do Estado de Coisas Inconstitucionais no Brasil. **IDP Law Review**, Brasília, v. 1, n. 2, p. 131-146. abr. 2022. Disponível em: https://www.portaldeperiodicos.idp.edu.br/lawreview/article/view/5943/2553. Acesso em: 9 jun. 2023.

ROSA, Alex da; PESSOA, Sara de Araújo; LIMA, Fernanda da Silva. Neutralidade tecnológica: reconhecimento facial e racismo. **Vírus**, São Paulo, v. 21, n. 2, dez. 2020. Disponível em: http:// www.nomads.usp.br/virus/virus21/?sec=4&item=9&lang=pt. Acesso em: 2 mar. 2023.

RUBACK, Lívia; ÁVILA, Sandra; CANTERO, Lúcia. Vieses no aprendizado de máquina e suas implicações sociais: um estudo de caso no reconhecimento facial. *In:* Workshop sobre as Implicações da Computação na Sociedade, 2, 2021. **Anais** [...]. Porto Alegre, XLI Congresso da Sociedade Brasileira de Computação, 2021, p. 90-101. Disponível em: https://doi.org/10.5753/wics.2021.15967. Acesso em: 9 jun. 2023.

SILVA, Lorena Abbas da; FRANQUEIRA, Bruna Diniz.; HARTMANN, Ivar. A. O que os olhos não veem, as câmeras monitoram: reconhecimento facial para segurança pública e regulação na América Latina. **Revista Digital de Direito Administrativo**, São Paulo, v. 8, n. 1, p. 171-204, 2021. Disponível em: 10.11606/issn.2319-0558.v8i1p171-204. Acesso em: 2 mar. 2023.

SILVA, R. L.; SILVA, F. S. R. da. Reconhecimento facial e segurança pública: os perigos do uso da tecnologia no sistema penal seletivo brasileiro. *In:* CONGRESSO INTERNACIONAL DE DIREITO E CONTEMPORANEIDADE: MÍDIAS E DIREITOS DA SOCIEDADE EM REDE, 5, 2019, Santa Maria. **Anais** [...]. Santa Maria: UFSM, 2019. Disponível em: https://www.ufsm.br/cursos/pos-graduacao/santa-maria/ppgd/congresso--de-direito-5a-edicao. Acesso em: 1º mar. 2023.

SILVA, Tarcízio. Linha do tempo do racismo algorítmico. *In:* SILVA, Tarcízio. **Blog do Tarcizio Silva**: pesquisa métodos

digitais, ciência, tecnologia e sociedade, 2022. Disponível em: https://tarciziosilva.com.br/blog/posts/racismo-algoritmico-linha-do-tempo. Acesso em: 18 fev. 2023.

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

SOUZA, M. **Dos espaços de controle de territórios dissidentes**. Rio de Janeiro: Consequência Editora, 2015.

SURESH, Harini; GUTTAG John Guttag. A Framework for Understanding Sources of Harm throughout the Machine Learning Life Cycle. *In*: **EAAMO: Equity and Access in Algotithms, Mechanisms, and Optimization**, 23, 2021, New Iorque. Anais [...]. EAAMO, Nova Iorque, p. 1-9, out. 2021. Disponível em: https://doi.org/10.1145/3465416.3483305. Acesso em: 1º mar. 2023.

SUPREMO TRIBUNAL FEDERAL. **ADPF 347 MC/DF**. Medida cautelar na arguição de descumprimento de preceito fundamental 347. Relator: Min. Marco Aurélio, 9 de setembro de 2015. Disponível em: https://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=TP&docID=10300665 . Acesso em: 1º mar. 2023.

Flavianne Fernanda Bitencourt Nóbrega
Doutora em Direito pela Universidade Federal de Pernambuco. Professora de Teoria Política e do Estado da Faculdade de Direito do Recife – UFPE e da Pós-Graduação. Coordenadora do Programa de Extensão "Acesso ao Sistema Interamericano de Direitos Humanos (ASIDH)".

João Vitor Sales Zaidan
Graduando em Direito pela Faculdade de Direito do Recife – Universidade Federal de Pernambuco. Pesquisador na área de Direitos Humanos e membro do Programa de Extensão "Acesso ao Sistema Interamericano de Direitos Humanos (ASIDH)".