REGULAÇÃO DE SISTEMAS DE RECONHECIMENTO FACIAL PARA FINS DE SEGURANÇA PÚBLICA NO BRASIL: RISCOS E DESAFIOS

REGULATION OF THE USE OF FACIAL RECOGNITION SYSTEMS IN BRAZILIAN PUBLIC SECURITY: RISKS AND CHALLENGES

Alice Azevedo Magalhães [1]
Técio Spínola Gomes [2]

Resumo: *O objetivo deste artigo é explicitar os potenciais riscos que o uso incondicionado de sistemas de reconhecimento facial na segurança pública gera a direitos fundamentais. Questiona-se sobre a necessidade de adoção de mecanismos de governança mediante regulação, assim como de contribuições ao contexto nacional proporcionadas pela discussão normativa no exterior. Trata-se de pesquisa pautada em revisão bibliográfica e fontes documentais primárias e secundárias. Diante do escasso material quantitativo sobre a eficácia do uso desses sistemas no Brasil, conclui-se que sua regulamentação é necessária, sendo imprescindível precedê-la por amplo diálogo com a comunidade acadêmica. Ademais, a Proposta de Lei apresentada pela Comissão Europeia ao Parlamento Europeu equilibra, satisfatoriamente, inovação tecnológica e respeito aos direitos fundamentais, sendo que pode se tornar uma referência para o debate nacional. A regulação de inteligência artificial ainda é experimental. Dessarte, este artigo é relevante ao proporcionar uma base para o aprofundamento do tema em estudos futuros.*
Palavras-chave: *Reconhecimento Facial. Segurança Pública. Inteligência Artificial. Regulação.*

Abstract: *The unconditioned use of facial recognition systems in public security threatens fundamental rights. The objective of this article was to make these potential threats explicit, questioning the need for governance mechanisms through regulation, as well as if the international legal debate could contribute to the Brazilian scenario. The study makes use of bibliographic reviews and primary and secondary documental sources. Given the scarce quantitative research on the effectiveness of these systems in Brazil, it concludes that regulation is necessary. However, it is essential to precede it by a broader dialogue with the academic community. The Regulation of the European Parliament and The Council satisfactorily balances technological innovation and respect for fundamental rights. Thus, it can become a reference for the national debate. The regulation of artificial intelligence is still experimental. Therefore, this article proposes to be relevant as it provides a basis for deepening the theme in future studies.*
Keywords: *Facial Recognition. Public Security. Artificial Intelligence. Regulation.*

[1] Graduanda em Direito pela Universidade Federal da Bahia.
Lattes: http://lattes.cnpq.br/3173151564719542.
ORCID: https://orcid.org/0000-0001-7487-1149.
Email: aliceazmagalhaes@gmail.com

[2] Professor Adjunto da Universidade Federal da Bahia (UFBA). Doutor em Direito Civil pela Universidade de São Paulo (USP). Mestre em Direito pela UFBA. Advogado.
Lattes: http://lattes.cnpq.br/6714227442505483.
ORCID: https://orcid.org/0000-0003-0701-3915.
E-mail: tecio@ufba.br

Introdução

O universo da ficção científica povoou o imaginário popular com imagens de inteligência artificial (IA) e robôs. O escritor Isaac Asimov, nessa esfera, foi um visionário, sendo a ele atribuído um dos primeiros usos do termo "robótica" (ASIMOV, 2019, p.12). Desde 1942, dois aspectos são constantemente reiterados por Asimov: as "Três Leis da Robótica" e a importância da regulação dos denominados "cérebros positrônicos", ou "cérebros" de robôs dotados de IA.

Fora do plano ficcional, a produção regulatória sobre IA se desenvolve gradualmente, encontrando-se em estágio experimental no contexto internacional e nacional (INSTITUTO IGARAPÉ, 2020, p.17). O uso de sistemas de IA pelo Poder Público apresenta capacidade tanto para ampliar a acurácia, justiça, transparência e efetividade das tomadas de decisões (NYE; CHOCHLA; LINDSAY, 2021), quanto para impactar negativamente o exercício de direitos fundamentais, a exemplo dos direitos à igualdade, à proteção contra a discriminação, ao acesso à justiça, à liberdade de expressão, associação e reunião, e à privacidade.

Os algoritmos replicam preconceitos históricos e, nessas circunstâncias, conforme Thieme (2018), a injustiça computacional pode codificar injustiças sociais. Essas dimensões devastadoras e propagadoras de injustiças das tecnologias de IA são, não ocasionalmente, denominadas *weapons of math destruction* (O'NEIL, 2016) ou "armas de destruição matemática".

Apesar da crescente implementação de tecnologias de IA no Brasil, os estudos sobre viés algorítmico são recentes e pouco explorados (SIMÕES-GOMES et al., 2020). A regulação brasileira de sistemas de reconhecimento facial (SRFs) para fins de segurança pública é majoritariamente abordada em nível estadual. No entanto, existem iniciativas no âmbito federal (INSTITUTO IGARAPÉ, 2021, p. 17).

Logo, o objetivo do presente artigo é tornar mais explícitos os potenciais riscos que o uso incondicionado de SRFs na segurança pública gera a direitos e garantias fundamentais, avaliando a necessidade de um debate mais amplo e denso sobre a regulação de SRFs para fins de segurança pública. Ademais, indaga-se como a discussão normativa no exterior pode contribuir para o debate nacional.

Além desta introdução e da metodologia, este artigo é composto por mais três seções. A primeira seção busca delimitar as terminologias de algoritmos, *machine learning* (ML) e inteligência artificial utilizadas. Em seguida, são apontadas as formas pelas quais essas tecnologias podem ser enviesadas, com potencial tanto para propagar injustiças (SAKAI; GALDINO; BURG, 2020) quanto para, por meio de regulação adequada, combatê-las (KLEINBERG; MULLAINATHAN; SUNSTEIN, 2020). A última seção, por sua vez, aborda o uso de SRFs na segurança pública. Por meio dela, são discutidas controvérsias internacionais sobre como o uso desses sistemas, pelas polícias, pode impactar o exercício de direitos. O debate é, então, situado no contexto brasileiro, no qual se percebe flagrante falta de dados e estudos necessários para averiguar a eficácia do uso desses sistemas na prevenção e redução da criminalidade (INSTITUTO IGARAPÉ, 2020, p. 16). Ademais, por meio da análise de projetos de lei, em nível estadual e federal, que versam sobre SRFs para fins de segurança pública, verifica-se que apenas um possui mecanismos para assegurar o uso responsável de SRFs nessas circunstâncias (INSTITUTO IGARAPÉ, 2020, p. 17).

Conclui-se que, diante dos potenciais riscos do uso de SRFs para fins de segurança pública, a regulamentação dessas tecnologias é necessária para impor diretrizes de governança que garantam seu uso responsável. Diante das propostas de regulamentação analisadas, as diretrizes estabelecidas pelo Projeto de Lei apresentado pela Comissão Europeia ao Parlamento Europeu (COMISSÃO EUROPEIA, 2021) são vistas como positivas. Ao fim, é ressaltado o caráter experimental da regulação sobre sistemas de IA (INSTITUTO IGARAPÉ, 2020, p. 17)

Metodologia

O presente artigo realiza um estudo de abordagem qualitativa e elege por metodologia a revisão bibliográfica e fontes documentais primárias e secundárias. Analisaram-se artigos, relatórios e projetos de lei (PL) nacionais e internacionais sobre o SRFs.

Internacionalmente, foi enfocada a Comunicação da Comissão Europeia ao Parlamento Europeu: *Laying down harmonized rules on artificial intelligence* (2021), assim como os rela-

tórios apresentados pela organização britânica *Big Brother Watch*, e o estudo estadunidense do *National Institute of Standarts and Technology* (NIST) (2019). No contexto brasileiro, analisaram-se projetos de lei estaduais que versam sobre SRFs: PL 391/2019 MG (MINAS GERAIS, 2019), PL 148/2019 PR (PARANÁ, 2019), PL 342/2019 RJ (RIO DE JANEIRO, 2019), PL 341/2019 RJ (RIO DE JANEIRO, 2019), PL 607/2019 RJ (RIO DE JANEIRO, 2019), PL 853/2019 RJ (RIO DE JANEIRO, 2019), e PL 865/2019 SP (SÃO PAULO, 2019). Analisaram-se também projetos de lei federais sobre o tema: PL n°.4612 de 2019 (BRASIL, 2019) e PL n° 9736/2018 (BRASIL, 2018). Da mesma maneira, é relevante a Portaria n° 4.617, de 6 de abril de 2021 (BRASIL, 2021), a qual institui a Estratégia Brasileira de Inteligência Artificial e a Lei n° 13.709, de 14 de agosto de 2018 (BRASIL, 2018), denominada Lei Geral de Proteção de Dados Pessoais.

O objetivo primário desta investigação é tornar mais explícitos os potenciais riscos que o uso incondicionado de SRFs na segurança pública gera a direitos e garantias fundamentais. Ademais, indaga-se sobre a necessidade de adoção de mecanismos de governança mediante regulação e como a discussão normativa no exterior pode contribuir para o debate nacional.

Frente ao objetivo, optou-se pela investigação descritiva. A análise do objeto de pesquisa foi dividida em diferentes etapas, evidentes na estruturação adotada. Inicialmente, buscou-se definir os conceitos operacionais: "algoritmos", "*machine learning*" e "inteligência artificial". Em seguida, o estudo voltou-se à existência e às formas de manifestação de "vieses algorítmicos" nessas tecnologias. Ao fim, são elencados possíveis riscos oriundos do uso governamental de SRFs na segurança pública, no exterior e no contexto brasileiro, assim como propostas normativas nesse sentido.

Durante o levantamento do referencial teórico, o estudo priorizou fontes oficiais, tanto governamentais quanto produzidas por organizações internacionais, a exemplo da Anistia Internacional, da Comissão Europeia e da Organização para a Cooperação e Desenvolvimento Econômico (OCDE). A seleção de obras específicas foi feita por meio de recursos de busca de palavras-chaves em bases de dados eletrônicos e sistemas de busca eletrônica, como Scielo, Plataforma Sucupira e JSTOR. Outrossim, todo o referencial teórico utilizado foi acessado digitalmente.

As principais obras de referência são os trabalhos do Grupo Independente de Peritos de Alto Nível sobre a Inteligência Artificial (GPAN IA), com destaque para o documento "Orientações éticas para uma IA de confiança" (2019). Solon Barocas e Andrew Selbst (2016) também fornecem importante base para a compreensão de vieses algorítmicos e Jon Kleinberg, Sendhil Mullainathan e Cass R. Sunstein apresentam uma visão transformadora sobre o potencial uso de algoritmos no combate à discriminação, descrito no artigo *Algorithms as discrimination detectors*.

Nacionalmente, além da Estratégia Brasileira de Inteligência Artificial (BRASIL, 2021), outra referência importante para pensar nos riscos a direitos fundamentais oriundos do uso de SRFs na segurança pública é a pesquisa "Recomendações de Governança: Uso de Inteligência Artificial pelo Poder Público", de Juliana Sakai, Manoel Goldino e Tamara Burg.

Definindo: algoritmos, *machine learning* (ML) e inteligência artificial

Ayre e Craner (2018), ao conceituarem algoritmo, utilizam a analogia de uma receita culinária: começando com os ingredientes (input), certas etapas são realizadas em uma determinada ordem (algoritmo), resultando em um prato (output). Assim, de forma simplificada, algoritmos são uma sequência de etapas. Para o propósito deste artigo, porém, é necessário especificar como algoritmos operam em computadores.

Nesse sentido, a definição adotada é a elaborada por Solon Barocas e colegas (BAROCAS et al., 2014, p.3), segundo os quais "algoritmos referem-se a sequências específicas de operações lógicas desenvolvidas para realizar determinada tarefa". Computacionalmente, para resolver um problema, desenvolvedores o "fragmentam em séries de questões que podem ser respondidas por uma particular sequência de operações lógicas e então executadas automaticamente por um computador"

Segundo Becker, Navarro Wolkart e Ferrari (2018, p. 4), os algoritmos podem ser divididos em duas espécies quanto ao funcionamento: i) algoritmos programados e ii) algoritmos

não programados. Os algoritmos programados são aqueles que seguem as operações definidas pelo programador: "a informação 'entra' no sistema (input), o algoritmo faz o que está programado para fazer com ela, e o resultado (output) 'sai' do sistema".

Os algoritmos não programados, também denominados algoritmos inteligentes ou l*earners*, são mais complexos: são algoritmos escritos por outros algoritmos (BECKER; WOLKART; FERRARI, 2018, p. 4). O ML, portanto, muda a lógica tradicional, pois "adentram na máquina tanto o dado como o resultado desejado e o produto é capaz de tornar a relação entre dado e resultado verdadeira" (MENDES; MATTIUZZO, 2019, p. 45).

O ML, ou aprendizado de máquina, ocorre quando computadores são "treinados" a raciocinar (BAROCAS et al., 2014, p. 4). ML "é um tipo de aprendizado via exemplo em que um algoritmo é exposto a uma enorme seleção de exemplos da qual foi instruído a obter lições gerais" (BAROCAS et al., 2014, p. 4). Dessa forma, a partir da análise dos exemplos conhecidos, ele pode, futuramente, classificar dados desconhecidos (AYRE; CRANER, 2018, p. 344).

Uma forma de ilustrar esse processo é pensar em uma criança aprendendo o que é um gato (BAROCAS et al., 2014, p. 4). Esta tecnologia utiliza por exemplo, características dos gatos conhecidos, como ter quatro patas e ter pelos, para reconhecê-los. De maneira similar, computadores testam quais detalhes específicos diferenciam gatos de outros seres para traçar um conceito geral para "gato". Para tanto, dependem de uma diversa e enorme quantidade de exemplos. Esse conjunto de exemplos dos quais o computador extrai os sinais para "gato" pode ser tão complexo que se torna impossível interpretá-lo. Barocas et al. (2014) pontuam que as aplicações mais bem sucedidas dessa tecnologia são, frequentemente, as mais inescrutáveis e, assim, que um aprendizado de sucesso ocorre ao custo de sua compreensão.

Diferentemente das crianças, portanto, um programa de ML necessita de milhões ou bilhões de pontos de dado – os referidos exemplos - para criar seus modelos estatísticos de causa e efeito (O'NEIL, 2016). O sucesso dessas tecnologias deve-se ao fato de que, atualmente, essa quantidade de informação está disponível. Apesar de sua complexidade, esses programas são apenas uma ramificação de uma definição mais ampla: a de Inteligência Artificial (IA).

Não há consenso sobre o conceito de IA. No entanto, para os fins deste artigo, será adotada a definição fornecida pela OCDE (2019), segundo a qual "um sistema de IA é um sistema baseado em máquina que pode, para um determinado conjunto de objetivos definidos pelo homem, fazer previsões, recomendações ou decisões que influenciam ambientes reais ou virtuais." O conceito, posteriormente, reforça que os "sistemas de IA são produzidos para operar com variados níveis de autonomia."

A Comunicação da Comissão ao Parlamento Europeu observa que essas tecnologias podem ser confinadas a um *software*, de forma virtual - como assistentes de voz, sistemas de reconhecimento facial e sistemas de reconhecimento de fala – ou integrados em dispositivos físicos – a exemplo de carros autônomos e utensílios conectados à internet – internet das coisas (2018, p. 1). Quanto ao seu funcionamento, a primeira fase para que um sistema de IA funcione corresponde ao recolhimento de dados, o que pode ocorrer por meio de sensores, por exemplo. A segunda fase é a de raciocínio da informação e tomada de decisões, na qual os dados oriundos dos sensores são utilizados para propor uma ação, visando determinado objetivo. Para que isso ocorra, os dados coletados precisam ser transformados em informação compreensível pelo módulo de processamento. Por fim, uma vez que a ação é decidida, o sistema está pronto para executá-la (GPAN IA, 2019, p. 3).

A partir dos conceitos explicados é possível obter uma melhor compreensão sobre as principais problemáticas associadas do uso dessas tecnologias, tema que será discutido nas próximas seções.

Como algoritmos podem ser injustos

O conhecimento sobre um algoritmo é, frequentemente, baseado no resultado (output) obtido por seu uso (AYRE; CRANER, 2018, p. 343). Assim, por não envolver pessoas nesse processo, há uma tendência em enxergar algoritmos como neutros, objetivos e mais confiáveis do que decisões tomadas por seres humanos. Ayre e Craner (2018, p. 344) pontuam que, na verdade, algoritmos resultam do comportamento humano e de bancos de dados elaborados

por seres humanos, de maneira que podem produzir resultados tão enviesados quanto os de pessoas.

Nesta seção, serão abordadas duas principais maneiras pelas quais o resultado de um algoritmo se torna enviesado. A primeira maneira é durante a programação, na qual pode ocorrer uma replicação das predisposições do programador, seja ela intencional ou não intencional (BAROCAS; SELBST, 2016, p. 678). Como anteriormente mencionado, no processo de elaboração dessa tecnologia, é preciso que um problema seja traduzido para termos compreensíveis pelos computadores.

Nesse sentido, transformar uma questão abstrata em variáveis a serem atingidas (*target variable*) é um processo subjetivo, em que desenvolvedores e programadores podem, até mesmo inconscientemente, interpretar o problema de forma a prejudicar sistematicamente determinadas minorias (BAROCAS; SELBST, 2016, p. 678). Por exemplo, a interpretação humana pode interferir na escolha das variáveis de input consideradas no processamento. O objetivo visado pode depender de categorias facilmente definidas e diferenciadas – como "spam" e "não spam". No entanto, os maiores perigos residem quando a criação de novas categorias é necessária (BAROCAS; SELBST, p. 680). Dessa maneira, indaga-se quais fatores definem categorias subjetivas. Por exemplo, o que caracteriza uma pessoa "digna de crédito" ou com "alto risco de reincidência em crimes"? São questões práticas "respondidas" na elaboração dessas tecnologias.

A segunda forma pela qual o resultado de um algoritmo pode ser considerado enviesado ocorre na utilização de bases de dados corrompidas ou não representativas utilizadas para o treinamento. Conforme supracitado, tecnologias de ML utilizam exemplos para aprender. Destarte, pode-se concluir, de forma intuitiva, que se os exemplos ensinados são discriminatórios, o output será, também, discriminatório, pois o algoritmo irá reproduzir o preconceito anterior.

Ademais, Barocas e Selbst (2016, p. 681) apontam que há discriminação, também, quando esses algoritmos elaboram suas decisões a partir de uma amostra enviesada ou não representativa da população. Portanto, qualquer decisão baseada nas inferências efetuadas por essa tecnologia, usando essas amostras, pode prejudicar sistematicamente aqueles que foram representados em excesso ou em deficiência.

Até mesmo quando a base de dados utilizada para o treinamento de algoritmos reflete a realidade com precisão, é possível que o resultado de seu emprego seja discriminatório, pois ocorre a absorção e replicação de padrões da sociedade. Conforme afirmam Daniel Becker et al, (2018, p. 9), nesse contexto, a utilização dessa tecnologia para a tomada de decisões reforçará circunstâncias sociais desiguais, que urgem serem modificadas.

Um exemplo de situação em que um algoritmo, ainda que não intencionalmente, pode propagar injustiças é o *software* desenvolvido pela PredPol, uma *startup* de Big Data californiana, utilizado para prever a probabilidade de um delito ocorrer em determinado local a partir de dados históricos sobre a criminalidade. Ao comentar o caso, O'Neil (2016, p. 75) aponta que a maioria dos crimes não é de grande magnitude, como assassinato e latrocínio, mas corresponde aos chamados "*nuisance crimes*", ou "crimes de ruído", a exemplo da posse de pequenas quantidades de drogas. Nesse sentido, a autora descreve como o uso dessa tecnologia, considerando os "*nuisance crimes*", cria um ciclo de retroalimentação, no qual a polícia adiciona mais dados que justificam mais policiamento.

Assim, partindo do pressuposto de que os casos retratados acontecem, com frequência, em bairros periféricos, que possuem maiores percentuais de negros e hispânicos em sua população, mesmo que o algoritmo não utilize "raça" como uma variável, o resultado é, inegavelmente, a tendência de prisão de negros e hispânicos. Dessa forma, as pessoas que habitam um ambiente com maior incidência de criminalidade são duplamente prejudicadas, tanto pelo crime quanto pela repressão, enquanto criminosos que habitam locais de menor criminalidade passam despercebidos (O'NEIL, 2016, p. 88).

Ademais, segundo Strandburg (2019, p. 1864), diferentemente dos processos decisórios tradicionais, modelos inescrutáveis de ML não podem ser previamente validados quanto aos seus resultados futuros. Esta opacidade dos "*learners*" deve-se à autonomia desses algoritmos em modificar sua estrutura, de acordo com os dados recebidos (BECKER et al., 2018, p.7). Tal

operação, como anteriormente pontuado, alcança uma complexidade tamanha que até mesmo a observação do output por seu próprio programador torna-se insuficiente para deduzir as decisões internas que proporcionaram esse resultado (BECKER et al., 2018, p. 6). Isto enseja a caracterização desses algoritmos como verdadeiras caixas-pretas.

Destarte, a aplicação de sistemas de IA pelo poder público tem a capacidade de impactar negativamente toda a população, amplificando possíveis discriminações sob o discurso de uma pretensa imparcialidade algorítmica que dificulta a identificação dessas injustiças. "As ferramentas de apoio à tomada de decisões ajudam servidores de órgãos governamentais a tomarem determinadas ações que impactam a vida das pessoas e, de forma direta ou indireta, o exercício de direitos fundamentais" (SAKAI; GALDINO; BURG, 2020, p. 9). Logo, é possível identificar todos os requisitos para caracterizar uma "arma de destruição matemática": opacidade, larga escala e dano (O'NIEL, 2016, p. 33). Todavia, é importante ressaltar que esse contexto não é imutável, e que atualmente existem diversas propostas que objetivam minimizar a presença de vieses em algoritmos e garantir um uso mais ético e seguro dessas ferramentas.

O aprofundamento da discussão sobre práticas de governança aplicadas à Inteligência Artificial não é o objetivo desse artigo. Porém, para melhor compreensão do debate aqui estruturado, serão apresentados, ainda que superficialmente, os critérios de uma IA de confiança. O GPAN IA (2019, p. 2) aponta que sistemas de IA devem seguir os princípios éticos de "respeito à autonomia humana, prevenção de danos, equidade e explicabilidade" e satisfazer os requisitos de "1) ação e supervisão humanas; 2) solidez técnica e segurança; 3) privacidade e governança de dados; 4) transparência; 5) diversidade, não discriminação e equidade. 6) bem-estar ambiental e social; 7) responsabilização."

Strandburg (2019, p. 1873), ao comentar mecanismos de governança, afirma que, apesar da opacidade dos sistemas de ML, existem aspectos de seu desenvolvimento que podem ser explicados de maneira convencional. Exemplos desses aspectos são a separação dos critérios de decisão em aspectos automatizados e não automatizados e a definição das variáveis a serem utilizadas como critério para o resultado. Assim, segundo a autora, para avaliar o impacto desses sistemas, é importante ser preciso sobre o que pode e não pode ser explicado.

Kleinberg et al. (2020) defendem, ainda, que dado o alto nível de especificidade dos algoritmos – muito maior do que aquele envolvido nos processos decisórios realizados por pessoas – estes podem, com regulamentação adequada, tornar mais fácil a identificação de discriminação e, logo, preveni-la. Apontam, como exemplo, uma denúncia sobre uma seleção de emprego discriminatória com mulheres. Assim, alegam ser muito mais fácil identificar as variáveis utilizadas, o banco de dados de treinamento etc. de um sistema baseado em algoritmos do que provar em juízo que as convicções pessoais machistas de um entrevistador influenciaram a contratação. Assim, algoritmos apresentam o potencial de atuar como poderosos detectores de discriminação humana, oferecendo transparência sobre as motivações das decisões, desde que com a devida regulamentação.

Esse entendimento pode ser validado pela possibilidade de se periciar um algoritmo. No Brasil, por exemplo, já há decisão que determina a realização de perícia técnica em dados de algoritmos utilizados em atividade empresarial, desde que, claro, esses dados não sejam expostos publicamente (TRIBUNAL REGIONAL DO TRABALHO DA 1ª REGIÃO, 2021).

Controvérsias sobre o uso de tecnologias de reconhecimento facial na segurança pública: riscos aos direitos fundamentais

Dentre os principais perigos apontados quanto à existência de vieses algorítmicos, destaca-se o uso de SRFs para fins de segurança pública. O alto risco dessas tecnologias decorre do impacto direto à vida de pessoas e ao exercício de direitos fundamentais, notadamente, o direito à igualdade, à proteção contra a discriminação, à privacidade, à liberdade de expressão, e à liberdade de reunião (SAKAI; GALDINO; BURG, 2020, p. 3).

Nesse sentido, um estudo federal estadunidense, realizado pelo *National Institute of Standarts and Technology* (2019), avaliou 189 algoritmos de 99 desenvolvedores diferentes, examinando a eficácia dos *softwares* de reconhecimento facial em identificar pessoas de dife-

rentes idades, sexo e raças. Entre as conclusões, destaca-se que, nas correspondências de um para um, as taxas de falsos positivos eram de 10 até 100 vezes maiores para asiáticos e afro-americanos do que para caucasianos.

Outrossim, resultado semelhante foi encontrado por Boulamwini e Gebru (2018, p. 8), ao avaliarem SRFs da Microsoft, IBM e Face ++. Em sua totalidade, esses sistemas apresentaram melhores *performances* em rostos masculinos do que em rostos femininos (8.1% - 20.6% de diferença entre as taxas de erro); e em pessoas de pele clara, quando comparadas àquelas de pele escura (11.8% - 19.2% de diferença entre as taxas de erro).

A violação ao princípio da igualdade aqui apontada segue os critérios indicados por Celso Antônio Bandeira de Mello (2008, p. 21), para identificação do desrespeito à isonomia: (i) a investigação do que é adotado como critério discriminatório; (ii) a análise de justificativa racional para a desigualdade adotada; e (iii) se essa justificativa racional é harmônica com os valores do sistema normativo constitucional. Nos casos supracitados, as diferenças na eficácia dos SRFs foram baseadas em raça e gênero. Não há fundamento lógico que justifique interesses nessa diferenciação e, ademais, a discriminação por motivos de raça e gênero é condenada tanto internacionalmente, quanto nacionalmente, no caso brasileiro, nos Arts. 3°, IV e 5°, I, XLI e XLII da Constituição Federal (BRASIL, 2019).

A organização *Big Brother Watch* (2020), à vista disso, prega o fim do uso do "*live facial recognition*", ou reconhecimento facial ao vivo, em tradução livre, pelas forças policiais do Reino Unido. Esse sistema, associado a câmeras, escaneia, em tempo real, os dados biométricos de todas as pessoas visíveis, os compara às imagens em um banco de dados e armazena aquelas que obtiveram "correspondência" com o banco de dados analisado (BIG BROTHER WATCH, 2020). O próprio recolhimento - mesmo que temporário - sem consentimento, de um dado biométrico tão sensível quanto as características do rosto de alguém, por si só, já é um recurso de uso delicado, em se tratando de direito à privacidade.

Adicionalmente, o SRF empregado pela Metropolitan Police - *NeoFace Watch* - em 98% dos casos identificou pessoas inocentes erroneamente (BIG BROTHER WATCH, 2018, p. 3). O monitoramento, para fins de segurança pública, de pessoas inocentes é, inclusive, interpretado por pesquisadores como uma violação ao princípio da presunção da inocência, uma vez que toda investigação que impacte direitos deve partir de uma suspeita fundada (SAKAI; GALDINO; BURG, 2020, p. 15).

A organização, ademais, aponta que essas tecnologias ameaçam a liberdade de expressão e a liberdade de reunião e defende que o uso de reconhecimento facial em manifestações e eventos pode dissuadir pessoas a participarem. Portanto, a prática, potencialmente, impediria as pessoas de expressarem suas ideias e opiniões nesses espaços, caso sejam vigiadas (BIG BROTHER WATCH, 2020, p.13). Essa preocupação é partilhada pela Anistia Internacional (2021), a qual afirma que "sistemas de reconhecimento facial são uma forma de vigilância de massa que viola o direito à privacidade e ameaça os direitos à liberdade de reunião pacífica e de expressão."

Como exemplo, cita-se o uso da tecnologia pelo Departamento de Polícia de Nova York de SRFs, durante os protestos do movimento *Black Lives Matters*, em 2020, e a tentativa de prisão do ativista Derrick Ingram por, supostamente, ter ameaçado um policial ao gritar em um megafone. A correspondência do reconhecimento facial do manifestante foi feita por meio de uma foto retirada de sua conta privada em uma rede social (AMNESTY INTERNATIONAL, 2021). Esse caso indica que a referida tecnologia pode ser empregada de forma autoritária como instrumento de perseguição política.

Algumas cidades estadunidenses, como São Francisco, Oakland e Alameda, diante desse contexto, optaram por banir o uso de SRFs para fins de segurança pública, sob o fundamento de que danos podem ser causados "à privacidade, à liberdade de expressão e de associação em espaços públicos" e "(...) ameaça ao devido processo legal, pois invertem o princípio da presunção da inocência" (IGARAPÉ, 2020, p. 17).

A Comissão Europeia, por outro lado, apresentou uma proposta intermediária de regulação ao Parlamento Europeu (2021, p.12). A comissão estabelece uma abordagem regulatória proporcional ao nível dos riscos de cada uso de sistemas de IA aos direitos fundamentais.

Nesse sentido, os classifica em: "i) risco inaceitável, ii) alto risco e iii) risco baixo ou mínimo." (COMISSÃO EUROPEIA, 2021, p.12).

O uso de SRFs, aqui abordado, é enquadrado em duas dessas categorias: de risco inaceitável e de alto risco. Essa distinção perpassa pelo entendimento de que a obtenção de dados biométricos se desdobra em captura: i) "*real time*", em tempo real, e ii) "*post*", posterior. Nos sistemas "*real time*" - também denominados "*live facial recognition*", conforme supracitado – "a captura dos dados biométricos, a comparação e identificação ocorrem instantaneamente, quase que instantaneamente ou em qualquer período sem um atraso significante (COMISSÃO EUROPEIA, 2021, p. 20)." Esses sistemas envolvem a análise de material ao vivo. Nos sistemas "*post*", diferentemente, o material analisado é preexistente, os dados biométricos foram previamente capturados, e a comparação e identificação ocorre apenas após um período significativo (COMISSÃO EUROPEIA, 2021, p. 20).

A Comissão Europeia caracteriza os SRFs "*real time*" para fins de segurança pública como de risco inaceitável e defende a sua proibição, exceto em três definidas e limitadas situações, diante de interesses públicos substanciais, a saber: busca por vítimas de crimes, certas ameaças à vida ou à integridade física, localização identificação ou persecução de perpetradores de cometer crimes, ataques terroristas.

A Decisão Quadro do Conselho Europeu 2002/584/JHA (2002, p. 3) aborda o mandado de detenção europeu e os processos de entrega entre os Estados-Membros. O documento lista 32 fatos puníveis, que, verificadas certas condições, ensejam a aplicação do mandado de detenção europeu, como tráfico de seres humanos, corrupção e homicídio doloso. A longa lista pode gerar a preocupação de que as exceções, na realidade, são abrangentes em demasia. Entretanto, cada uso de sistemas de identificação biométrica "*real time*" em locais públicos para propósitos de persecução penal deve ser condicionado a uma autorização expressa e específica de autoridades judiciárias ou de autoridade administrativa independente em Estados-Membros. Tais autorizações devem ser obtidas previamente ao uso da tecnologia, exceto em situações justificáveis de urgência (COMISSÃO EUROPEIA, 2021, p. 23).

Os sistemas reconhecimento posteriores, por sua vez, são classificados como de alto risco (COMISSÃO EUROPEIA, 2021, p. 26). A Comissão Europeia condiciona o uso desses sistemas de IA a altas práticas de governança, como a requisição de transparência, instruções de uso e documentação sobre possíveis riscos aos direitos fundamentais e discriminação, a divulgação aos usuários do nível de precisão e eficácia, cybersegurança etc. Isso requer a realização de registros "incluindo características gerais, capacidades e limitações do sistema, algoritmos, dados, treinamento, processos de testagem e validação utilizados, assim como documentação sobre os riscos do sistema" (COMISSÃO EUROPEIA, 2021, p.30).

A aprovação dessa proposta depende de um debate exaustivo entre os membros do Parlamento Europeu. Entretanto, esta aprovação se apresenta como uma alternativa adequada, embora possua desvantagens, à proibição por completo dessas tecnologias. Permite, logo, por meio da gradação dos riscos, que haja equilíbrio entre o desenvolvimento tecnológico, inovação e respeito a direitos fundamentais.

Uso de tecnologias de reconhecimento facial na segurança pública brasileira

No Brasil, não há regulação de uso de SRFs para fins de segurança pública em nível federal, como indicado pela Estratégia Brasileira de Inteligência Artificial (BRASIL, 2021, p. 28). A Lei Geral de Proteção de Dados (LGPD) (BRASIL, 2018), como expressamente disposto no inciso III de seu artigo 4°, não se aplica ao tratamento de dados pessoais para fins exclusivos de segurança pública. Essa matéria, consoante parágrafo 1° do referido artigo, deve ser regida por lei específica (BRASIL, 2018).

Segundo o mesmo dispositivo, ainda, as hipóteses do inciso III devem obedecer aos critérios de proporcionalidade, necessidade ao atendimento do interesse público, devido processo legal, princípios gerais de proteção e os direitos do titular estabelecidos na Lei. n° 13.709 de 14 de agosto de 2018 (BRASIL, 2018). Outrossim, de acordo com o parágrafo 3°, nessas hi-

póteses, a Agência Nacional de Proteção de Dados (ANPD) deve solicitar relatórios de impacto aos responsáveis pela proteção dos dados pessoais (BRASIL, 2018).

Ademais, os dados biométricos são enquadrados pela LGPD na categoria de dado pessoal sensível, conforme o inciso II de seu artigo 5° (BRASIL, 2018). O reconhecimento facial, segundo a cientista de dados, Nina da Hora (2021), é um método biométrico, em que a identificação envolve a comparação dos traços de um rosto contra vários rostos em um banco de dados, buscando uma associação. Aponta, ainda, a existência de problemas de reconhecimento de padrão visual, pois o rosto, representado como um objeto tridimensional sujeito a variações de pose, iluminação etc., é identificado com base em imagens adquiridas, bidimensionais (HORA, 2021).

Portanto, apesar da inexistência de lei específica, não se pode afirmar que existe uma lacuna normativa, pois o país possui um amplo arcabouço jurídico que protege os direitos individuais, desde a Constituição até a LGPD. No entanto, não obstante, verifica-se ausência de dados sobre o número de falsos positivos nas implementações de SRFs nas cidades brasileiras. Além disso, há falta de estudos sistemáticos sobre a eficiência desses sistemas na prevenção e redução da criminalidade (IGARAPÉ, 2019). Ou seja, não há informações necessárias para averiguar se essas tecnologias estão de acordo com os princípios da transparência, necessidade, proporcionalidade e não discriminação. Logo, atualmente o "sucesso" do reconhecimento facial tem sido julgado apenas com base no critério da quantidade de prisões decorrentes de seu uso (IGARAPÉ, 2019).

SRFs vêm sendo utilizados no Brasil desde 2011 (IGARAPÉ, 2019). O Instituto Igarapé mapeou que, dos 48 casos de uso desses sistemas – reportados pelo setor público, contemplando 30 cidades em 15 estados – 13 são no setor da segurança pública. Apenas no período de março a outubro de 2019, nos estados da Bahia, Rio de Janeiro, Santa Catarina e Paraíba, essas tecnologias foram decisivas nas prisões de 151 pessoas, segundo dados do Centro de Estudos de Segurança e Cidadania (CESeC) (NUNES, 2019, p. 89). Esses números, analisados individualmente, são insuficientes para estimar eficácia. Deve ser considerado, ainda, que o grau de semelhança fixado como necessário para emitir um alerta para os agentes da polícia pode ser alterado e, portanto, variar (NUNES, 2019, p. 88).

Nesse sentido, é pertinente exemplificar com a análise feita pelo CESeC (NUNES, 2019, p. 88), com base nos dados do monitoramento na cidade de Feira de Santana, durante quatro dias da micareta de 2019: dos alertas emitidos, mais de 96% eram falsos. Foram 1,3 milhões de pessoas com seus rostos capturados, que geraram 903 alertas, dos quais resultou o cumprimento de 18 mandados de prisão e prisão de 15 pessoas. O alto índice de falsos positivos é alarmante e causa questionamentos sobre a eficiência na aplicação dessas tecnologias. Ademais, a abordagem adotada a partir dessas correspondências pode contribuir na propagação de injustiças.

A escala da utilização dos SRFs pelos municípios e estados para fins de segurança pública, aliada à pouca transparência sobre sua aquisição, implementação e funcionamento, indicam que o atual arcabouço normativo tem sido insuficiente para coibir eventuais riscos aos direitos fundamentais da população. O debate regulatório nacional sobre essa matéria e sua instrumentalização, portanto, representa um ponto crucial na escolha pela manutenção ou mitigação dos riscos, ou, até mesmo, pela proibição do uso dessas tecnologias.

Assim, nos próximos parágrafos, são apresentadas algumas iniciativas brasileiras de regulamentação sobre SRFs para fins de segurança pública, tanto em âmbito estadual quanto federal. Posteriormente, são tecidas considerações sobre como essa discussão normativa no exterior pode contribuir para o debate nacional.

Um relatório elaborado em parceria entre o Instituto Igarapé e o Data Privacy Brasil Research (2020, p. 17) aponta que, no cenário brasileiro, tem-se optado por uma regulação nos âmbitos estaduais. Essa abordagem, apesar de permitir "maior experimentação" e garantir "que os entes federativos incorporem suas particularidades na observância dos princípios", apresenta como ônus da ausência de uma legislação única a maior dificuldade na observância de princípios. Disto decorre a possibilidade de que violações a direitos e garantias individuais não sofram a devida responsabilização (IGARAPÉ, 2020, p. 17).

A partir desse relatório, foram elencados sete projetos de lei (PL) estaduais: PL 391/2019 MG (MINAS GERAIS, 2019), PL 148/2019 PR (PARANÁ, 2019), PL 342/2019 RJ (RIO DE JANEIRO, 2019), PL 341/2019 RJ (RIO DE JANEIRO, 2019), PL 607/2019 RJ (RIO DE JANEIRO, 2019), PL 853/2019 RJ (RIO DE JANEIRO, 2019), e PL 865/2019 SP (SÃO PAULO, 2019), que abordam, ainda que indiretamente, o reconhecimento facial para fins de segurança pública. Dois desses projetos, o PL n° 391/2019, de Minas Gerais (MINAS GERAIS, 2019) e o PL. n° 148/2019, do Paraná (PARANÁ, 2019), dispõem sobre implementação de tecnologias de reconhecimento facial em locais públicos em geral. Os projetos não apresentam delimitação, nos respectivos âmbitos estaduais, sendo que, neste, essa implementação tem caráter obrigatório, enquanto naquele, apresenta caráter permissivo. Os demais projetos abordam a adoção desses sistemas em estações e meios de transporte, como metrô, trens, embarcações e terminais rodoviários. Há predominância pela obrigatoriedade, pois apenas um projeto, o PL n° 853/2019 (RIO DE JANEIRO, 2019), tem "caráter permissivo".

Assim como foi averiguado pelo Instituto Igarapé, em parceria com a Data Privacy Brasil Research (2020, p. 17), é preocupante a ausência de menção a mecanismos de governança nesses projetos de lei. O argumento de inevitabilidade do avanço tecnológico é, em três estados, apresentado como justificativa para a implementação desses sistemas – PL n°148/2019 (PARANÁ, 2019), PL n° 391/2019 (MINAS GERAIS, 2019) e PL n° 607/2019 (RIO DE JANEIRO, 2019). A partir dessas colocações, pode-se inferir a errônea concepção de que o desrespeito a direitos e garantias fundamentais representa o custo da evolução na segurança pública e tecnologia, afinal, argumenta-se, ela é inevitável (PARANÁ, 2019).

Outrossim, em nenhum dos projetos elencados é manifesta a preocupação com princípios para o uso, proteção dos dados dos cidadãos, privacidade ou medidas de averiguação e/ou prevenção de discriminação. Apesar disso, em alguns casos, está prevista correção de desvios de finalidade, por meio medidas adequadas – PL n° 148/2019 (PARANÁ, 2019) e PL n° 391/2019 (MINAS GERAIS, 2019). Entretanto, não é analisado que mesmo o uso dessas tecnologias para a finalidade planejada, "garantir a segurança" dos cidadãos, representa riscos aos direitos e garantias fundamentais, caso não sejam adotadas medidas de governança.

Em âmbito federal, são apresentados os projetos de lei n° 4612 de 2019 (BRASIL, 2019) e n° 9736/2018 (BRASIL, 2018). Este visa tornar obrigatória a identificação biométrica de custodiados pelo Estado, por meio de SRFs, novamente, sem análise dos riscos oriundos de seu uso. Aquele, por sua vez, destaca-se positivamente por estabelecer pressupostos para o uso dessas tecnologias: a) "acesso à informação"; b) "definição multissetorial de boas práticas e padrões técnicos, éticos de segurança garantidores dos direitos dos cidadãos"; c) "transparência quanto aos parâmetros para a tomada de decisão automatizada, observados os segredos comercial e industrial"; entre outros. Além da proibição do tratamento discriminatório e do uso dessas tecnologias para o estabelecimento de contínua vigilância massiva.

O projeto de lei n° 4612/2019 (BRASIL, 2019), portanto, é o que mais se aproxima das diretrizes estabelecidas pela Estratégia Brasileira de Inteligência Artificial (EBIA) (BRASIL, 2021), a qual tem, entre seus objetivos, "contribuir para a elaboração de princípios éticos para o desenvolvimento e uso de IA responsáveis.". Nesse sentido, a EBIA aponta que:

> Qualquer movimento ao encontro de regulamentação, devem ser seguidos princípios, tais como: (i) desenvolver estruturas legais existentes; (ii) adotar uma abordagem regulatória baseada em princípios e resultados; (iii) fazer um "teste de equilíbrio de riscos e benefícios centrado no indivíduo humano e (iv) fazer avaliação de impacto contextual (BRASIL, 2021).

Ademais, assim como a proposta elaborada pela Comissão Europeia, a EBIA (BRASIL, 2021) afirma que essa intervenção regulatória deve ser proporcional aos riscos associados a suas aplicações e suas limitações devem se restringir a usos específicos. A necessidade de gradação é, também, contemplada pelo PL n° 4.612/2019 (BRASIL, 2019), a partir da proibição de

"contínua vigilância massiva".

Essa expressão é definida no parágrafo único do artigo 2° do referido dispositivo como sendo: "a atividade exercida sem pausas e sobre toda a população indiscriminadamente, sem restrição a local ou período". Apesar de interessante, a expressão é menos rigorosa do que a proposta de proibição das tecnologias de reconhecimento facial "*real time*" para segurança pública, apresentada pela Comissão Europeia. Isso porque bastaria que se estabelecesse um local, independentemente de sua abrangência, para que o uso do SRF fosse permitido. Logo, dentre as propostas analisadas em âmbitos estadual, nacional e internacional, a Comissão Europeia destaca-se positivamente como a organização que melhor equilibra o desenvolvimento tecnológico e a inovação com o respeito a direitos fundamentais.

Notas conclusivas

O uso de sistemas de inteligência artificial pelo poder público apresenta potencial tanto para ampliar a acurácia, justiça, transparência e efetividade nas tomadas de decisões quanto para tornar-se uma arma de destruição matemática, intensificando a discriminação e infringindo direitos. A escolha pela concretização deste ou daquele potencial, por sua vez, depende da identificação dos riscos decorrentes do uso irresponsável dessas tecnologias e da minimização desses por meio de mecanismos de governança.

A Inteligência Artificial é uma ferramenta. Como tal, ela pode ser instrumentalizada tanto para o bem, por exemplo, como uma forma de combater preconceitos, conforme defendido por Kleinberg et al. (2020), quanto para o mal, ainda que inconscientemente, conforme observado nas várias maneiras pelas quais algoritmos tornam-se enviesados e propagam preconceitos.

Nesse sentido, a regulação se apresenta como uma forma de impor o uso responsável desses sistemas. Como foi observado, essas tecnologias têm sido usadas por estados e municípios brasileiros há uma década, sem que haja estudos que comprovem sua eficácia no combate à criminalidade ou transparência quanto aos dados produzidos. As propostas analisadas, com exceção de uma, evidenciam negligência quanto à identificação e combate aos potenciais riscos oriundos da utilização de SRFs para fins de segurança pública.

No entanto, apesar de inexistir regulação nacional, conforme apontado pela Estratégia Brasileira de Inteligência Artificial, o tema não deve ser regulamentado precipitadamente e de forma dissociada da comunidade acadêmica. O país, consoante anteriormente exposto, dispõe de um amplo arcabouço jurídico que protege os direitos individuais, enquanto as discussões sobre a elaboração de norma específica são devidamente amadurecidas.

A escassez de pesquisas qualitativas sobre SRFs no Brasil não possibilitou que fosse realizada, neste artigo, uma ponderação entre os riscos e benefícios obtidos pelo emprego do reconhecimento facial na segurança pública. Tal problemática, não obstante, tem potencial para fomentar estudos, visando ao preenchimento dessa lacuna.

Internacionalmente, tem-se adotado iniciativas pela regulamentação, tanto no sentido de proibição geral, como ocorre em cidades e estados estadunidenses, quanto em vias de proibição condicionada a alguns usos. Deve-se observar, no entanto, que a proibição irrestrita desestimula a evolução dessas tecnologias e sua possível aplicação no combate a preconceitos, de forma que é uma opção com muitas limitações.

O projeto de lei proposto pela Comissão Europeia ao Parlamento Europeu, dentre os aqui analisados, foi o que apresentou melhores soluções sobre o uso de tecnologias de reconhecimento facial para fins de segurança pública e, logo, pode contribuir como referência na discussão normativa no contexto brasileiro. As limitações propostas permitem que o desenvolvimento tecnológico e aperfeiçoamento dessas tecnologias não seja interrompido, assim como oferecem medidas rigorosas de controle e uso responsável.

No desfecho deste artigo, é importante reforçar que as regulamentações de IA são experimentais, o que limita a obtenção de resultados conclusivos, uma vez que seus impactos ainda não são compreendidos em sua totalidade. Esta pesquisa, ao fim, cumpre seu objetivo de difusão dos potenciais riscos que o uso incondicionado de sistemas de reconhecimento facial na segurança pública gera a direitos e garantias fundamentais. Sendo assim, almeja-se

que esta forneça os conceitos e problemáticas introdutórias para a compreensão do tema no contexto nacional.

Referências

AMNESTY INTERNATIONAL. **Ban dangerous facial recognition technology that amplifies racist policing**. 2021. Disponível em: https://www.amnesty.org/en/latest/news/2021/01/ban-dangerous-facial-recognition-technology-that-amplifies-racist-policing/. Acesso em: 03 mai. 2021.

AYRE, Lori; CRANER, Jim. Algorithms: avoiding the implementation of institutional biases. Technology Column. v. 37, n. 3, 2018. Disponível em: https://www.researchgate.net/publication/327806571_Algorithms_avoiding_the_implementation_of_institutional_biases. Acesso em: 14 abr. 2021.

BAROCAS, Solon; ROSENBLAT, Alex; BOYD, Danah; GANGADHARAN, Seeta Peña; YU, Corrine. **Data & Civil Rights: Technology Primer**. Data & Civil Rights Conference. Out. 2014. Disponível em: https://datasociety.net/wp-content/uploads/2014/10/Technology.pdf. Acesso em: 17 abr. 2021.

_____; SELBST, Andrew D. Big data's disparate impact. **California Law Review**., v.104, p.671-732, 2016. Disponível em: http://www.californialawreview.org/wp-content/uploads/2016/06/2Barocas-Selbst.pdf. Acesso em: 19 abr. 2021.

BECKER, Daniel; WOLKART, Erik Navarro; FERRARI, Isabela. Arbitrium ex machina: panorama, riscos e a necessidade de regulação das decisões informadas por algoritmos. **Revista dos Tribunais**, v. 995, p.1-16, set, 2018. Disponível em: http://governance40.com/wp-content/uploads/2018/11/ARBITRIUM-EX-MACHINA-PANORAMA-RISCOS-E-A-NECESSIDADE.pdf. Acesso em: 10 abr. 2021.

BIG BROTHER WATCH. **Briefing on facial recognition surveillance**. Londres. 2020. Disponível em: https://bigbrotherwatch.org.uk/wp-content/uploads/2020/06/Big-Brother-Watch-briefing-on-Facial-recognition-surveillance-June-2020.pdf. Acesso em: 29 abr. 2021.

_____. **Executive Summary**. Londres. 2018. Disponível em: https://bigbrotherwatch.org.uk/wp-content/uploads/2018/05/Face-Off-final-digital-1.pdf. Acesso em: 25 abr 2021.

BOULAMWINI, Joy; GEBRU, Timnit. **Gender Shades**: Intersectional Accuracy Disparities in Commercial Gender Classification. Conference on Fairness, Accountability, and Transparency. p. 1 – 15. 2018. Disponível em: https://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf. Acesso em 29 abr. 2021.

BRASIL. [Constituição (1988)]. Constituição da República Federativa do Brasil: promulgada em 5 de outubro de 1988. 2. ed. São Paulo: Rideel, 2019.

_____. **Lei n° 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais. Brasília, DF: Presidência da República, 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 15 de abr. 2021.

_____. Congresso Nacional. Câmara dos Deputados**. Projeto de Lei da Câmara n° 4612, de 2019.** Dispõe sobre o desenvolvimento, aplicação e uso de tecnologias de reconhecimento facial e emocional, bem como outras tecnologias digitais voltadas à identificação de indivíduos ou análise de comportamentos. Sr. Bibo Nunes. Brasília, DF: Disponível em: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=1794019&filename=PL+4612/2019. Acesso em 29 abr. 2021.

_____. Congresso Nacional. Câmara dos Deputados**. Projeto de Lei da Câmara n° 9736, de 2018**. Acrescenta dispositivo à Lei n° 7.210, de 11 de julho de 1984, para incluir a previsão de identificação por reconhecimento facial. Sr. Julio Lopes. Brasília, DF: Disponível em: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=1643053&filename=PL+9736/2018. Acesso em 29 abr. 2021.

_____**. Decreto n° 8.771, de 11 de maio de 2016.** Regulamenta a Lei nº 12.965, de 23 de abril de 2014, para tratar das hipóteses admitidas de discriminação de pacotes de dados na internet e de degradação de tráfego, indicar procedimentos para guarda e proteção de dados por provedores de conexão e de aplicações, apontar medidas de transparência na requisição de dados cadastrais pela administração pública e estabelecer parâmetros para fiscalização e apuração de infrações. Brasília, DF: Presidência da República, 2016. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2016/decreto/D8771.htm. Acesso em 15 abr. 2021.

_____. Ministério da Ciência, Tecnologia e Inovações. **Portaria n° 4.617, de 6 de abril de 2021**. Institui a Estratégia Brasileira de Inteligência Artificial e seus eixos temáticos. Brasília, DF: Ministério da Ciência, Tecnologia e Inovações, 2021. Disponível em: https://www.in.gov.br/en/web/dou/-/portaria-gm-n-4.617-de-6-de-abril-de-2021-*-313212172. Acesso em 15 abr. 2021.

_____. Tribunal Regional do Trabalho da 1ª Região. Mandado de Segurança. Agravo Regimental. Plataforma digital. Vínculo de emprego. Perícia em dados de algoritmo. Necessidade, possibilidade e limites. Juiz natural. Independência. Princípio democrático fundante. Transcendência do caso. Produção antecipada de prova e contenção a litigiosidade. Acórdão em mandado de segurança n. 0103519-41.2020.5.01.0000-RJ. Uber do Brasil Tecnologia LTDA e Carlos Cesar Goncalves Ventura. Relatora: Raquel de Oliveira Maciel. 22 abr. 2021.

HORA, Nina da. O que é Reconhecimento facial? Uma introdução técnica. 2021. Disponível em: https://www.ninadahora.dev/post/reconhecimento-facial-introdu%C3%A7%C3%A3o. Acesso em 10 mai. 2021.

NUNES, Pablo. Novas ferramentas, velhas práticas: reconhecimento facial e policiamento no Brasil. In: CENTRO DE ESTUDOS DE SEGURANÇA E CIDADANIA (CESeC). **Retratos da violência**: cinco meses de monitoramento, análises e descobertas. p. 67- 70. 2019. Disponível em: http://observatorioseguranca.com.br/wp-content/uploads/2019/11/1relatoriorede.pdf. Acesso em 03 mai. 2021.

EUROPEAN COMMISSION, Regulation of the European Parliament and of The Council – Laying down harmonized rules on artificial intelligence (artificial intelligence act) and amending certain Union legislative acts. **COM (2021) 206**. Bruxelas, 2021. Disponível em: https://digital-strategy.ec.europa.eu/en/library/proposal-regulation-laying-down-harmonised-rules-artificial-intelligence. Acesso em: 22 abr. 2021.

EUROPEAN COUNCIL. Council Framework Decision on the European arrest warrant and the surrender procedures between Member States. **JHA (2002) 584**. Bruxelas. 2002. Disponível em: https://www.gov.uk/government/publications/framework-decision-on-the-european-arrest-warrant. Acesso em: 29 abr. 2021.

GRUPO INDEPENDENTE DE PERITOS DE ALTO NÍVEL SOBRE A INTELIGÊNCIA ARTIFICIAL (GPAN IA). **Orientações éticas para uma IA de confiança**. Abr. 2019. Disponível em: https://ec.europa.eu/futurium/en/ai-alliance-consultation#:~:text=The%20Ethics%20Guidelines%20for%20Trustworthy,strategy%20announced%20earlier%20that%20year. Acesso em 17 de abr. 2021.

_____. **Uma definição de IA: Principais capacidades e disciplinas científicas**. Abr. 2019. Dis-

ponível em:https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai. Acesso em: 20 abr. 2021.

HIDVEGI, Fanny; MASSÉ, Estelle. **Mapping artificial intelligence strategies in Europe:** a new report by Access Now. 2018. Disponível em: https://www.accessnow.org/mapping-artificial--intelligence-strategies-in-europe/. Acesso em: 17 abr. 2021.

INSTITUTO IGARAPÉ. **Infográfico reconhecimento facial no Brasil**. 2019. Disponível em: https://igarape.org.br/infografico-reconhecimento-facial-no-brasil/. Acesso em: 03 mai. 2021.

_____. **Regulação do reconhecimento facial no setor público.** 2020. Disponível em: https://igarape.org.br/wp-content/uploads/2020/06/2020-06-09-Regula%C3%A7%C3%A3o-do-reconhecimento-facial-no-setor-p%C3%BAblico.pdf. Acesso em: 03 mai. 2021.

_____. **Webreport videomonitoramento**. 2019. Disponível em: https://igarape.org.br/videomonitoramento-webreport/. Acesso em: 03 mai. 2021.

KLEINBERG, Jon; MULLAINATHAN, Sendhil; SUNSTEIN, Cass R. **Algorithms as discrimination detectors**. PNAS. vol. 117, n. 48, dez. 2020. p. 30097 – 30100. Disponível em: https://www.pnas.org/content/117/48/30096. Acesso em: 24 abr. 2021.

MELLO, Celso Antônio Bandeira de. **O conteúdo jurídico do princípio da igualdade**. 3 ed. São Paulo: Malheiros, 2008.

MINAS GERAIS. Assembleia Legislativa. **Projeto de Lei n° 391, de 2019**. Dispõe sobre a obrigatoriedade da implantação de tecnologia de reconhecimento facial em locais públicos no âmbito do Estado de Minas Gerais. Deputado Carlos Henrique. Belo Horizonte, MG. Disponível em: https://www.almg.gov.br/atividade_parlamentar/tramitacao_projetos/texto.html?a=2019&n=391&t=PL. Acesso em 29 abr. 2021.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST). NIST Study Evaluates Effects of Race, Age, Sex on Face Recognition Software. 2019. Disponível em: https://www.nist.gov/news-events/news/2019/12/nist-study-evaluates-effects-race-age-sex-face-recognition-software. Acesso em: 03 mai. 2021.

O'NEIL, Cathy. **Weapons of math destruction**: how big data increases inequality and threatens democracy. 1 ed. Nova Iorque: Crown Publishers, 2016.

ORGANIZATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT (OECD). **OECD/LEGAL/0449**: Recommendation of the Council on Artificial Intelligence. 2019. Disponível em: https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449. Acesso em: 17 abr. 2021.

PARANÁ. Assembleia Legislativa. **Projeto de Lei n° 148, de 2019**. Dispõe sobre a permissão de implantação de tecnologia de reconhecimento facial em locais públicos. Deputado Subtenente Everton. Curitiba, PR. Disponível em: http://portal.alep.pr.gov.br/modules/mod_legislativo_arquivo/mod_legislativo_arquivo.php?leiCod=82332&tipo=I. Acesso em 29 abr. 2021.

RIO DE JANEIRO. Assembleia Legislativa. **Projeto de Lei n° 341, de 2019**. Dispõe sobre a obrigatoriedade de concessionários do serviço público de administração de terminais rodoviários, instalação de câmeras de segurança com tecnologia de reconhecimento facial de suspeitos e procurados da justiça nos locais que determina e dá outras providências. Deputado Vandro Familia. Rio de Janeiro, RJ. Disponível em: http://alerjln1.alerj.rj.gov.br/scpro1923.nsf/0c5bf5cde95601f903256caa0023131b/5db5f3d2098193ca832583d100739827?OpenDocument&Highlight=0,341%2F2019. Acesso em 29 abr. 2021.

_____. Assembleia Legislativa. **Projeto de Lei n° 342, de 2019**. Dispõe sobre a obrigatoriedade de concessionários do serviço público de metrô, trens e barcas, instalação de câmaras de segurança com tecnologia de reconhecimento facial de suspeitos e procurados da justiça nos locais que determina e dá outras providências. Deputado Vandro Familia. Rio de Janeiro, RJ. Disponível em: http://alerjln1.alerj.rj.gov.br/scpro1923.nsf/e00a7c3c8652b69a83256cca00646ee5/ea3643862a7c5ce2832583d100740275?OpenDocument. Acesso em 29 abr. 2021.

_____. Assembleia Legislativa. **Projeto de Lei n° 607, de 2019**. Torna obrigatória a instalação de câmeras de monitoramento com reconhecimento facial em todas as praças de pedágios, no âmbito do estado do Rio de Janeiro. Deputado Sergio Louback. Rio de Janeiro, RJ. Disponível em: http://alerjln1.alerj.rj.gov.br/scpro1923.nsf/e00a7c3c8652b69a83256cca00646ee5/051ddc6638919505832584010064da36?OpenDocument, Acesso em 29 abr. 2021.

_____. Assembleia Legislativa. **Projeto de Lei n°853, de 2019**. Veda a negociação e comercialização de produtos e serviços no interior dos vagões e embarcações dos transportes públicos do Estado do Rio de Janeiro na forma que menciona. Deputado Anderson Moraes. Rio de Janeiro, RJ. Disponível em: http://alerjln1.alerj.rj.gov.br/scpro1923.nsf/18c1dd68f96be3e7832566ec0018d833/85f4bde0acc7c0f783258426006119f4?OpenDocument. Acesso em 29 abr. 2021.

SAKAI, Juliana; GALDINO, Manoel; BURG, Tamara. **Recomendações de Governança**: Uso de Inteligência Artificial pelo Poder Público. 2020. Disponível em: https://www.transparencia.org.br/downloads/publicacoes/Recomendacoes_Governanca_Uso_IA_PoderPublico.pdf. Acesso em: 20 mar 2021

SÃO PAULO. Assembleia Legislativa**. Projeto de Lei n° 865, de 2019**. Torna obrigatória a instalação de câmeras de reconhecimento facial em todas as estações do Metrô e da CPTM, bem como no interior dos vagões das composições. Deputado Rodrigo Gambale. São Paulo, SP. Disponível em: https://www.al.sp.gov.br/propositura/?id=1000278098. Acesso em 29 abr. 2021.

SIMÕES-GOMES, Letícia; ROBERTO, Enrico; MENDONÇA, Jônatas. **Viés algorítmico - um balanço provisório.** Estud. sociol., Araraquara, v. 25, n. 48, jan/jun, 2020. Disponível em: https://periodicos.fclar.unesp.br/estudos/article/view/13402. Acesso em: 10 abr. 2021.

STRANDBURG, Katherine J. Rulemaking and inscrutable automated decision tools. **Columbia Law Review**, v. 119, n. 7, p. 1851-1886, 2019. Disponível em: https://www.jstor.org/stable/26810852?seq=1. Acesso em: 11 abr. 2021.

THIEME, Nick. **We are Hard-Coding Injustices for Generations to Come**. 2018. Disponível em: https://undark.org/2018/02/20/ai-watchdog-computational-justice/. Acesso em: 17 abr. 2021.

THOMAS, Nye; CHOCHLA, Erin; LINDSAY, Susie. **Law Commission of Ontario, Regulating AI**: Critical Issues and Choices. Toronto. 2021. Disponível em: https://www.lco-cdo.org/wp-content/uploads/2021/04/LCO-Regulating-AI-Critical-Issues-and-Choices-Toronto-April-2021-1.pdf. Acesso em 10 mai. 2021.

UE. Comunicação da Comissão ao Parlamento Europeu, ao Conselho Europeu, ao Conselho, ao Comité Económico e Social Europeu e ao Comité das Regiões — Inteligência artificial para a Europa, Bruxelas, **25.4.2018 [COM(2018) 237 final]**. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:52018DC0237&from=EN. Acesso em 29 abr. 2021.

Recebido em 25 de maio de 2021
Aceito em 14 de junho de 2021