UNIVERSIDADE DE BRASÍLIA

FACULDADE DE DIREITO

PAULO RICARDO DA SILVA SANTANA

RACISMO ALGORÍTMICO: ANÁLISE DOS DESAFIOS DA REGULAÇÃO DAS TECNOLOGIAS DE RECONHECIMENTO FACIAL NO BRASIL

BRASÍLIA

2022

UNIVERSIDADE DE BRASÍLIA

FACULDADE DE DIREITO

PAULO RICARDO DA SILVA SANTANA

RACISMO ALGORÍTMICO: ANÁLISE DOS DESAFIOS DA REGULAÇÃO DAS TECNOLOGIAS DE RECONHECIMENTO FACIAL NO BRASIL

Trabalho de conclusão de curso de graduação apresentado à Faculdade de Direito da Universidade de Brasília, como requisito parcial para a obtenção do grau de Bacharel em Direito.

Orientadora: Professora Doutora Ana Frazão

BRASÍLIA

2022

PAULO RICARDO DA SILVA SANTANA

RACISMO ALGORÍTMICO: ANÁLISE DOS DESAFIOS DA REGULAÇÃO DAS TECNOLOGIAS DE RECONHECIMENTO FACIAL NO BRASIL

Monografia apresentada à Banca Examinadora da Faculdade de Direito da Universidade de Brasília, campus Darcy Ribeiro, como requisito parcial para a obtenção do grau de Bacharel em Direito.

Data da defesa: 18/04/2022.

Resultado: Aprovado.

BANCA EXAMINADORA

_____

Professora Doutora Ana Frazão (FD-UnB)

Orientadora

_____

Professor Doutor Benedito Cerezzo Pereira Filho (FD-UnB)

Examinador

_____

Professora Doutora Bianca Kremer Nogueira Corrêa (IDP)

Examinadora

BRASÍLIA

2022

AGRADECIMENTOS

À Giovanna Milanez, amiga, pela generosidade em compartilhar seu conhecimento e ideias que culminaram na escolha do tema.

Ao Daniel Barbosa, amigo e maior encorajador, também pela importante contribuição com a escolha do tema em momentos de muitas incertezas, mas sobretudo por toda a ajuda com a estrutura do trabalho e a bibliografia. Seguramente este trabalho não se realizaria sem sua contribuição.

Ao Paulo Vitor Lucena, companheiro, por todos os incentivos e por ouvir pacientemente as repetidas leituras de cada capítulo, que muito me ajudaram a reorganizar as ideias.

Ao Pedro Queiroz, amigo, pela cuidadosa revisão do *abstract*.

À professora Ana Frazão, orientadora, que, com precisão, me ajudou a escolher melhores caminhos para a realização da pesquisa.

RESUMO

Este trabalho tem o objetivo de analisar os desafios a serem enfrentados pelo legislador na busca por um modelo regulatório para as tecnologias de reconhecimento facial no Brasil. O ponto de partida foi uma revisão bibliográfica sobre inteligência artificial, algoritmos, big data e reconhecimento facial com o objetivo de esclarecer aspectos técnicos e trazer definições importantes para compreensão do tema. Em seguida, foi realizada uma análise dos principais projetos de lei, bem como de legislações vigentes relacionadas ao reconhecimento facial com o intuito de apontar algumas lacunas normativas. Observou-se que a maioria dos projetos possuem caráter autorizativo do uso das tecnologias de reconhecimento facial, sem definir direitos e obrigações e sem qualquer diálogo com demais normas setoriais importantes. Espera-se que um eventual projeto regulatório, em razão do alto potencial discriminatório dessas tecnologias, busque diálogo com a sociedade, em especial com entidades da sociedade civil na luta por igualdade racial e vise estabelecer um equilíbrio entre privacidade e segurança.

Palavras-chave: Reconhecimento facial; Discriminação; Racismo; Regulação.

ABSTRACT

This work aims to analyze the challenges to be faced by the legislator in the search for a regulatory model for facial recognition technologies in Brazil. The starting point was a literature review on artificial intelligence, algorithms, big data and facial recognition in order to clarify technical aspects and bring important definitions for a better understanding of the topic. Thereafter, an analysis of the main bills was carried out, as well as current legislation related to facial recognition, in order to point out some regulatory gaps. It was observed that most bills are mostly authorizatives to the use of facial recognition technologies, without defining rights and obligations and without any dialogue with other important sectorial legislations. It is expected that an eventual regulatory bill, due to the high discriminatory potential of these technologies, seeks dialogue with society, especially with civil entities that fights for racial equality, and aims to establish a balance between privacy and security.

Keywords: Face Recognition; Discrimination; Racism; Regulation.

LISTA DE ABREVIATURAS E SIGLAS

ACLU	União Americana por Liberdades Civis
ADM	Armas de Destruição em Massa
ANPD	Agência Nacional de Proteção de Dados
CCPA	*California Consumer Private Act*
CDC	Código de Defesa do Consumidor
CFTV	Circuito Interno Fechado de Televisão
EDPB	*European Data Protection Board*
EDPS	*European Data Protection Supervisor*
EUA	Estados Unidos da América
FBI	*Federal Bureau of Investigation*
GDPR	*General Data Protection Regulation*
IA	Inteligência Artificial
IBM	*International Business Machines*
INMETRO	Instituto Nacional de Metrologia, Qualidade e Tecnologia
IRIS	Instituto de Referência em Internet e Sociedade
LAPIN	Laboratório de Políticas Públicas e Internet
LGPD	Lei Geral de Proteção de Dados
NIST	*National Institute of Standards and Technology*
ONU	Organização das Nações Unidas
PEC	Proposta de Emenda à Constituição
PL	Projeto de Lei
SEPEC	Secretaria Especial de Produtividade e Competitividade
TRF	Tecnologia de Reconhecimento Facial

LISTA DE FIGURAS

INTRODUÇÃO

Sociedade da informação, sociedade dos dados, sociedade em rede, capitalismo de vigilância, sociedade da caixa preta, sociedade do controle, *dataísmo*, *datificação*. Em que sociedade estamos vivendo afinal? As ciências sociais se esforçam para explicar tempestivamente o mundo de hoje frente a uma sociedade que mal consegue acompanhar os avanços impostos pela tecnologia. Tecnologias surgem e envelhecerem antes mesmo que a sociedade consiga entender os seus efeitos sobre ela.

A vigilância, seja estatal, seja privada, aos poucos ajudou a moldar um mundo cada vez mais pautado pela extração e pelo processamento de dados sobre tudo e todos, fazendo emergir questões importantes acerca do equilíbrio entre os seus benefícios e a deterioração dos direitos fundamentais e da democracia. Como uma das facetas da vigilância, as Tecnologias de Reconhecimento Facial (TRFs) ajudaram a conduzir a promessa por um mundo mais seguro e mais justo, aumentando a capacidade e a eficiência nos processos de identificação e reconhecimento e superando os problemas decorrentes da subjetividade humana.

Contudo, a tecnologia também se mostrou capaz de ser etarista, homofóbica, misógina e racista, colocando em xeque a fé na sua suposta objetividade. Com isso, muito vem se debatendo acerca da ampla utilização da tecnologia para fins e vigilância, sobretudo as biométrico-faciais, que lidam com dados pessoais estreitamente conectados com práticas discriminatórias.

No Brasil, as controvérsias em torno das TRFs ganharam evidência com as primeiras prisões realizadas pela segurança pública utilizando-se de software de reconhecimento facial e têm crescido com a sua utilização em outros contextos, como transporte público e privado.

Nos últimos anos, surgiram alguns projetos de lei estaduais e federais relacionados à regulação das TRFs, variando, em alguma medida, o seu alcance e, por vezes, até regulando tecnologias correlacionadas. Contudo, até o presente momento, nenhum projeto federal foi aprovado. Nesse recorte, este trabalho se propõe a analisar os desafios da regulação das tecnologias de reconhecimento facial no Brasil, país historicamente marcado pelo racismo e pela discriminação.

Considerando o tema exposto, a principal pergunta de pesquisa deste trabalho é:

Quais são os principais problemas que deverão ser enfrentados pelo legislador brasileiro na busca por um modelo regulatório das tecnologias de reconhecimento facial?

Para responder à questão acima, as seguintes perguntas secundárias devem ser endereçadas:

1. Quais são os contornos atuais da vigilância e quais são os seus impactos na sociedade democrática?

2. O que é o reconhecimento facial e como ele se insere no contexto de vigilância atual?

3. Quais os riscos envolvidos na sua utilização pelo poder público e por agentes privados?

O Capítulo I desenvolve a pergunta secundária 1, apresentando os contornos atuais da vigilância privada e estatal, seus efeitos na sociedade e os riscos gerais da vigilância para o estado democrático de direito, elencando direitos fundamentais ameaçados pelo abuso no uso de tecnologias de vigilância, em especial a privacidade.

O Capítulo II, por sua vez, visa esclarecer aspectos técnicos relacionados às tecnologias de reconhecimento facial, demonstrando suas etapas básicas de funcionamento e os problemas de ordem técnica comuns na sua implementação e utilização e suas repercussões em uma sociedade marcada pelo racismo.

O Capítulo III realiza uma exploração dos projetos de leis federais e estaduais relacionados ao reconhecimento facial, destacando alguns aspectos positivos e negativos. A seguir, é realizada uma análise do Projeto de Lei nº 4.619/19, único projeto de lei federal voltado especificamente para a regulação do uso e desenvolvimento de tecnologias de reconhecimento facial. A partir desses apontamentos são delimitados os problemas que devem ser debatidos pelo legislador na elaboração de um projeto regulatório abrangente para as tecnologias de reconhecimento facial.

Por fim, na Conclusão são reunidos os elementos bases para fornecer uma resposta à pergunta de pesquisa principal.

A pesquisa foi elaborada por meio de um estudo bibliográfico referente a vigilância, inteligência artificial, big data, algoritmos, reconhecimento facial e suas conexões com a erosão de direitos fundamentais e, ainda, de que forma o racismo se perpetua por meio da tecnologia, sobretudo as de reconhecimento facial. Também foram analisados relatórios de observatórios e entidades atuantes nos direitos humanos e igualdade racial bem como projetos de lei nacionais e internacionais sobre a regulação do reconhecimento facial.

Mister destacar que esta pesquisa não tem o objetivo de examinar o racismo no Brasil, suas bases e suas imbricações, mas sim, a partir do reconhecimento de que o racismo permeia as estruturas da sociedade brasileira, suas instituições e seu processo político, analisar de que forma a tecnologia integra esse fenômeno, particularmente as tecnologias de reconhecimento facial.

CAPÍTULO I – VIGILÂNCIA

I.1 – VIGILÂNCIA E PRIVACIDADE

1984, romance distópico de George Orwell, vem sendo relido como uma espécie de profecia em relação às questões referentes à privacidade. Figura onipresente na trama, o vigilante Grande Irmão é frequentemente utilizado como metáfora para se compreender os problemas relacionados à privacidade nos tempos atuais. Essa visão é criticada por Daniel Solove, segundo o qual a metáfora orwelliana está concentrada na vigilância, carregada de impessoalidade, por meio de máquinas e câmeras, o que resulta em um ambiente em que a privacidade parece não estar ameaçada, tornando a vigilância menos invasiva.

Solove entende que, a partir da metáfora orwelliana, o indivíduo não se importa com o fato de que saibam sobre ele informações aparentemente irrelevantes, como o modelo de seu carro ou hotel de preferência, mas sim, apenas se tiver feito algo errado.[1] Não é à toa que discussões atuais sobre privacidade e proteção de dados abarcam até mesmo os dados aparentemente inofensivos, como comentários e curtidas em fotos nas redes sociais.

A conclusão inicial de Solove é de que a metáfora do Grande Irmão é melhor para explicar a vigilância estatal sobre os indivíduos ou a vigilância no meio digital. Em *1984*, os indivíduos são constantemente vigiados pelo Grande Irmão, por meio de dispositivos bidirecionais, as *teletelas*.[2] A vigilância é de tal modo liquefeita na sociedade atual que a interação dos usuários, por diversos dispositivos eletrônicos conectados em rede com suas aplicações digitais, cria uma atmosfera de fluxo bidirecional de informações entre os indivíduos e os agentes de vigilância, tal como ocorre com as *teletelas* de Orwell.

Para Solove, buscar entender os problemas relacionados à privacidade a partir da obra de Orwell apenas ajuda a reforçar a narrativa de que não há nada a temer com relação à vigilância, desde que o indivíduo não tenha feito nada de errado.[3] Por fim, Solove defende que a privacidade importa, mesmo quando não há nada a esconder.

---

[1] SOLOVE, Daniel J. *The Digital Person*: technology and privacy in the information age. Ex. Machina. 2004. p. 27 – 34.
[2] As *teletelas* eram dispositivos similares a monitores de televisão utilizados para transmitir e receber simultaneamente informações dos cidadãos, isto é, ver e ouvir tudo no seu campo de visão. Ver mais em: ORWELL, George. 1984. Tradução de Claudio Carina, Sonia Carvalho. São Paulo: Citadel, 2021. pp.46 e 47.
[3] SOLOVE, Daniel J. *Why Privacy Matters Even if You Have "Nothing to Hide*. The Chronicle of Higher Education, 15 maio 2011. Disponível em: http://www.uvm.edu/~dguber/POLS21/articles/solove.htm. Acesso em: 16 out. 2021.

Para chegar a essa conclusão, o autor propõe uma alternativa à metáfora orwelliana: uma análise a partir da obra *O Processo*, romance de Franz Kafka que narra a história de um personagem em investigação misteriosa, sem informações sobre o motivo, enfrentando uma forte burocracia, munida de informações das pessoas para tomar decisões importantes sobre elas e negando-lhes a capacidade de participar do modo como suas informações são usadas.

Nessa perspectiva, Solove afirma que a metáfora de Kafka captura melhor o escopo, a natureza e os efeitos do tipo de relação de poder criada pelos bancos de dados.[4] Assim, o problema não estaria propriamente na coleta de informações, como em Orwell, mas sim na maneira como o processo burocrático trata os indivíduos e suas informações.[5]

Solove não nega os paralelos entre a distopia de Orwell, publicada em 1949, e a realidade atual.[6] A vigilância se tornou uma dimensão central da modernidade, que demanda incessantemente por mais segurança. Aliás, a visão do autor sobre a metáfora do Grande Irmão vai ao encontro do conceito de vigilância líquida de Zygmunt Baumam, vigilância diluída na onipresença da segurança.[7]

Embora a vigilância, de maneira geral, seja antiga e se refira a processos de coleta de informação das mais diversas fontes, é preciso reconhecer que nada mais a simboliza melhor, nos dias de hoje, do que as câmeras de monitoramento. Como veremos mais adiante, a evolução tecnológica nos dispositivos de captação de imagem ajudou a aprimorar e intensificar o monitoramento dos indivíduos nos permitindo abandonar, em parte, os chamados circuitos fechados de TV (CFTV)[8] e adotar, aos poucos, soluções robustas de videomonitoramento equipadas com algoritmos de inteligência artificial, conectados a bases de dados e com o poder de reconhecer automaticamente os rostos dos indivíduos.

Nesse contexto, vigilância líquida se refere à sociedade moderna, marcada pela vigilância constante, seja no meio físico ou digital, suportada por câmeras, dispositivos biométricos, celulares e algoritmos equipados com inteligência artificial, e por uma sociedade que não compreende completamente o fluxo de informações coletadas por esses aparatos tecnológicos.[9]

---

[4] SOLOVE. Daniel. Op. cit., 2004. p. 37.
[5] Ibid. p. 38.
[6] Ibid. p. 31. O brilhantismo da obra de Orwell não é descartado por Solove, que entende que a metáfora do Big Brother entende a privacidade em termos de poder, e vê a privacidade como uma dimensão essencial da estrutura política da sociedade.
[7] BAUMAN, Zygmunt. LYON, David. *Vigilância líquida:* diálogos com David Lyon. *Zahar*. 2014. p. 5 a 17.
[8] Segundo Herman Kruegle (2007, p. 9), o objetivo de um CFTV é fornecer olhos remotos a um operador de segurança. Kruegle (2007, pp. 14-16) explica ainda que as versões mais simples desses sistemas são compostas por câmera, gravador de vídeo e monitor de TV, por onde o operador monitora a cena gravada pelas câmeras. KRUEGLE, Herman. *CCTV surveillance:* analog and digital video practices and technology. 2ª ed. Elsevier, 2007. p. 9 e 14-16
[9] SOLOVE. Daniel. Op. cit., 2004. p. 75.

As bases matemáticas do reconhecimento facial moderno surgiram dez anos após a publicação de *1984*. Hoje, essa tecnologia é tão amplamente difundida que vem embutida em aparelhos de uso diário, como celulares e computadores, por exemplo, reforçando a tese da vigilância líquida de Baumam. Seu uso tem permitido situações muito similares à metáfora kafkiana analisada por Solove.

Não faltam registros de pessoas apreendidas injustamente por crimes que não cometeram, envoltas em circunstâncias em que não conseguem obter informações sobre as decisões que as conduziram a essas situações. A diferença curiosa em relação à metáfora de Kafka é que o tribunal do mundo real tem sido ocupado por algoritmos inteligentes. Nesse recorte, da mesma forma que ajudou a aprimorar a vigilância, o reconhecimento facial também foi responsável por originar novas questões concernentes à privacidade, às quais veremos com mais detalhes no próximo capítulo.

I.2 – VIGILÂNCIA NO CONTEXTO DO BIG DATA

Os anos 2000 foram marcados por muitas mudanças tecnológicas. No início da década, menos de 500 milhões de pessoas no mundo tinham acesso à Internet. Até o final dos anos 2000, este número chegaria a 2 bilhões de pessoas.[10] Neste mesmo período, surgiram gigantes da tecnologia como *Facebook*, *Youtube*, *Wikipedia* e *Twitter*, empresas que ajudaram a transformar a Internet em uma plataforma provedora de diversos serviços digitais, a chamada *WEB* 2.0,[11] resultando em grande produção de dados em relação aos anos anteriores. É nesse contexto que surge o *big data*, termo criado pelo pesquisador Doug Laney como um novo paradigma na era da informação, caracterizado por grande volume de dados, maior velocidade e variedade.[12]

A evolução das máquinas e de sua capacidade de armazenamento e processamento resultaram no crescimento exponencial da produção de dados. Potencializados pela internet, os dados foram se tornando centrais na sociedade. Todas as informações possíveis passaram a ser registradas, até mesmo as aparentemente sem valor, sendo posteriormente transformadas em formatos de dados quantificados

---

[10] Informações extraídas do site *Our world in data* no gráfico *Internet users by world region*. Disponível em: https://ourworldindata.org/grapher/internet-users-by-world-region?time=1990..latest&country=Europe+%26+Central+Asia~East+Asia+%26+Pacific~Latin+America+%26+Caribbean~South+Asia~North+America~Middle+East+%26+North+Africa~Sub-Saharan+Africa. Acesso em: 15 jun. 2021

[11] O'REILLY, Tim. *What Is Web 2.0:* Design Patterns and Business Models for the Next Generation of Software. O 'Reilly, 30 de set. de 2005. Disponível em: https://www.oreilly.com/pub/a/web2/archive/what-is-web-20.html?page=1. Acesso em: 21 out. 2021

[12] Em 2001, no artigo *3D Data Management: Controlling Data Volume, Velocity, and Variety*, o responsável pelo termo *big data*, Doug Laney, o definiu como gerenciamento de dados a partir de 3 dimensões: volume, velocidade e variedade de dados. Em publicação posterior ele incluiu novos V's: veracidade, valor, validade, virtual.

e permitindo o uso da informação de várias novas maneiras, incluindo o monitoramento em tempo real e a análise preditiva. Keneth Cukier e Viktor Mayer-Schönberger se referem a esse processo como *datificação* da sociedade.[13]

O paradigma do *big data* empoderou ainda mais a vigilância à medida em que possibilitou mecanismos para se tentar traduzir o homem físico para o meio digital, não só pela agregação de seus dados de identificação tradicionais como também de suas vozes, personalidades e emoções. Inclusive, em *A era do Capitalismo de Vigilância*, Shoshana Zuboff descreve uma nova forma de capitalismo que reivindica de maneira unilateral a experiência humana como matéria-prima gratuita para a tradução em dados comportamentais.[14]

O mercado não assistiu desinteressado o Estado produzir e manipular dados para atingir seus objetivos. Já em 1991, em artigo publicado pelo *The New York Times*, o jornalista John Markoff afirmava que o Grande Irmão de George Orwell teria se tornado um homem de negócios, enfatizando que as grandes corporações representavam uma ameaça maior à privacidade que o Estado, muito em razão da capacidade que elas detém de compilar dossiês detalhados sobre os consumidores.[15] O que para Markoof, foi possível graças ao desenvolvimento de tecnologias de computação e comunicação cada vez mais poderosas.

Esse movimento perigoso das grandes corporações ainda ocorre atualmente. Não por outro motivo, quase três décadas mais tarde, Frank Pasquale afirmaria que o mercado aumenta as apostas no jogo dos dados conforme a tecnologia avança. Para Pasquale, a cada ano, câmeras de vigilância se tornam mais baratas, sensores são implementados em mais lugares, celulares rastreiam movimentos, programas registram o uso dos teclados e novos softwares prometem cópias quantificadas dos indivíduos gerando uma vasta quantidade de dados usada para alimentar bancos de dados, reunidas em perfis de profundidade e especificidade sem precedentes.[16]

Esses perfis de indivíduos compõem a base de produtos de predição, comercializados em um novo tipo de mercado denominado por Zuboff de *Mercado de Comportamento Futuro*, pois são produtos que antecipam o que um indivíduo faria agora, daqui há pouco ou mais tarde.[17] Os governos têm

---

[13] MAYER-SCHÖNBERGER, Viktor. CUKIER, Keneth. *Big Data:* the essential guide to work, life and learning in the age of insight. Londres: John Murray Publishers, 2017. *E-book*.
[14] ZUBBOF, Shoshana. *A Era do Capitalismo de Vigilância*. 1 ed. Editora Intrínseca, 2021. p.18.
[15] MARKOFF, John. *Remember Big Brother? Now he's a company man*. The New York Times, 31 jan 1991. Disponível em: https://www.nytimes.com/1991/03/31/weekinreview/ideas-trends-remember-big-brother-now-he-s-a-company-man.html. Acesso em: 15 mar. 2022.
[16] PASQUALE, Frank. *The black box society*: the secret algorithms that control money and information. London: Harvard University Press, 2015. p. 4.
[17] ZUBBOF, Shoshana. Op. Cit., 2021. p.19.

explorado bem os produtos desse mercado para aprimorar ainda mais seu aparato de vigilância de modo que não é mais suficiente poder identificar e reconhecer os indivíduos suspeitos, é preciso poder dizer o que eles serão capazes de fazer. Assim, o mundo real deixa para traz a distopia de Philip K. Dick, *Minority Report*. Adaptada para os cinemas em 2020 com título homônimo, a obra retrata uma sociedade em que o Estado prevê a atuação de um crime e age contra o suposto criminoso antes da concretização do ato.

A tecnologia, assim, foi capaz de superar os limites do imaginário da ficção científica, pois em *Minority Report* os crimes são previstos por seres mutantes com poder de previsão, chamados de *precogs*. Talvez o autor da obra que inspirou a adaptação cinematográfica jamais teria imaginado que o papel desempenhado pelos *precogs*, em poucas décadas, seria realizado por algoritmos computacionais inteligentes empoderados por gigantescas bases de dados.

I.3 – INDO ALÉM DA PRIVACIDADE

O *big data* tornou indispensável a informação para o funcionamento da sociedade e de suas instituições e crucial para o exercício de direitos fundamentais. Nesse sentido, Laura Schertel afirma que na sociedade contemporânea, caracterizada pelo fluxo intenso de informações a partir de uma moderna infraestrutura de comunicação e informação, muitos direitos tendem a ser afetados ou influenciados pelo fenômeno da informação.[18]

Como vimos nos tópicos anteriores, a vigilância se estendeu para além das atividades de controle, investigação e inteligência estatal. O mercado incorporou elementos da vigilância estatal no desenvolvimento de produtos e de novos modelos de negócio, moldando o próprio Capitalismo. Liquefeita na sociedade, a vigilância passou a ser um atributo da realidade contemporânea, de forma que somos vigiados não só pelo Estado, mas também pelo mercado. Schertel aponta como consequência disso a classificação das pessoas em categorias de acordo com a avaliação de seus riscos e a discriminação do acesso a determinados bens e serviços, de modo a afetar significativamente as suas chances de vida.[19]

Os algoritmos exercem um papel importante no processo de violação de direitos fundamentais, pois conforme aponta Ana Frazão, alimentados por bases de dados cada vez maiores, no atual contexto

---

[18] MENDES. Laura Schertel. *Privacidade, Proteção de dados e defesa do consumidor:* linhas gerais de um novo direito fundamental. São Paulo: Ed. Saraiva, 2014. *E-book.* n.p.
[19] Ibid. n.p.

do *big data*, eles têm sido utilizados para decisões e tarefas que envolvem análises qualitativas e subjetivas, comumente marcadas por alta carga valorativa, tal como acontece nos julgamentos para classificação, ranqueamento e criação de perfis das pessoas.[20]

Nesse contexto, é possível depreender que não só a privacidade se encontra ameaçada pelo uso de TRFs, mas também direitos fundamentais já há muito tempo consolidados. *Softwares* com reconhecimento facial utilizados na contratação de empregados, por exemplo, apresentam o risco de discriminação por idade, sexo e cor da pele. O caso mais famoso já registrado foi o do *Rekognition*, desenvolvido pela *Amazon*, em que se registrou discriminação por sexo e pela cor da pele nas escolhas de candidatos realizadas pelo algoritmo.[21] Casos como esse demonstram que essas tecnologias podem afetar diretamente a dignidade da pessoa humana, igualdade e liberdade de exercício de trabalho.

Schertel também exemplifica outras possíveis violações, como a limitação da liberdade de reunião em espaços públicos, em que os participantes são filmados e registrados sem justificativa, e a liberdade de ir e vir, que pode ser limitada nos casos de proibição de embarque em aeronaves de passageiros registrados equivocadamente em lista de terroristas.[22] Questão importante, tendo em vista que o reconhecimento facial tem sido largamente utilizado, não só para fins de segurança nos aeroportos, mas também no processo de identificação de passageiros.

Para alguns autores, os riscos vão além dos direitos fundamentais. Como bem observa Samuel Oliveira, além das violações sistemáticas a direitos fundamentais, do emprego maciço de inovações tecnológicas também decorrem outras questões preocupantes, como a consolidação da vigilância e a erosão da confiabilidade nos governos e nas instituições.[23] Um caso que ilustra bem isso é o da entrega de informações sobre atividades online de usuários pela *Yahoo* ao governo chinês, em 2005, ocasionando a condenação de jornalistas a 10 anos de prisão. Durante o processo, houve denúncias de diversas violações de direitos humanos, incluindo tortura.[24]

---

[20] FRAZÃO, Ana. *Discriminação algorítmica.* Compreendendo o que são os julgamentos algorítmicos e o seu alcance na atualidade. Parte I. JOTA, 16 jun. 2021. Disponível em: https://www.jota.info/opiniao-e-analise/colunas/constituicao-empresa-e-mercado/discriminacao-algoritmica-16062021?amp. Acesso em: 26 out. 2021.

[21] AMAZON *face-detection technology shows gender and racial bias, researchers say*. CBS News, 25 jan. 2019. Disponível em: https://www.cbsnews.com/news/amazon-face-detection-technology-shows-gender-racial-bias-researchers-say/. Acesso em: 26 out. 2021.

[22] MENDES, Laura Schertel. Op. cit., 2014. n.p.

[23] OLIVEIRA, Samuel R. *Sorria, você está sendo filmado!* Repensando direitos na era do reconhecimento facial. São Paulo: Thomson Reuters, 2021. p. 29.

[24] RESOURCE CENTRE. *Yahoo! lawsuit (re China)*. Business & Human Rights, 1 abr. 2007. Disponível em: https://www.business-humanrights.org/en/latest-news/yahoo-lawsuit-re-china. Acesso em: 11 fev. 2022.

Robert Reich lembra que parte da argumentação da *Yahoo* em relação ao caso foi a de que a presença da empresa na China impulsionava o país para a democracia.[25] Diferente das pessoas naturais, as empresas não são competentes para julgamento moral ou participar de decisões democráticas. Aliás, Reich afirma que grandes empresas, como a *Yahoo*, não possuem expertise em avaliações morais e nem são autorizadas a equilibrar lucros e interesse público.[26] Obstinadas na busca por lucros, essas empresas são reflexos do que o autor chama de *supercapitalismo*.[27]

O escândalo *Cambridge Analytica* é também um caso que nos permite compreender bem os riscos que essas tecnologias trazem aos indivíduos, à coletividade e à democracia. Nesse caso, dados pessoais de milhões de usuários da rede social *Facebook*, coletados sem consentimento, foram utilizados para influenciar a decisão dos cidadãos americanos nas eleições de 2018 e dos cidadãos britânicos no plebiscito que decidiu a saída da Grã-Bretanha da União Europeia, o *Brexit*.

O caso *Yahoo* envolveu o fornecimento de informações privadas dos seus usuários. Já o *Cambridge Analytica* acende uma preocupação ainda maior, pois ocorreu com base na coleta, sem o consentimento, de dados tornados publicamente pelos próprios usuários, de aparente insignificância. Nas duas situações, as ameaças à democracia estão muito além de justiça em disputas eleitorais.

Com a evolução da Inteligência Artificial, a abundante produção de dados e sua alta disponibilidade na rede criaram um terreno fértil para a proliferação de algoritmos de classificação, análise preditiva e de influência no comportamento dos indivíduos, o que Stefano Rodotá chama de maré tecnológica, a qual as autoridades nacionais e internacionais nem sempre são capazes de controlar adequadamente.[28]

O *Mercado de Comportamento Futuro*[29] tem movimentado as autoridades de diversos países para estabelecer limites mínimos ao seu poder,[30] mas enquanto isso não acontece, valores democráticos e até a personalidade dos indivíduos são postos à prova por julgamentos algorítmicos.[31]

---

[25] REICH, Robert B. *Supercapitalismo*: como o capitalismo tem transformado os negócios, a democracia e o cotidiano. Rio de Janeiro: Elsevier, 2008. p. 203.
[26] Ibid. 2008. p. 202.
[27] Ibid. 2008. p. 49.
[28] RODOTÀ, Stefano. *A vida na sociedade de vigilância* – a privacidade hoje. Organização, seleção e apresentação de Maria Celina Bodin de Moraes. Tradução: Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008. p. 14.
[29] Ver nota 17.
[30] Ver nota 181.
[31] Existem algoritmos de Inteligência Artificial capazes de afirmar sobre a orientação sexual de alguém e até mesmo sua orientação política. Ver mais em: LEVIN, Sam. *New AI can guess whether you're gay or straight from a photograph*. The Guardian, 8 set. 2017. Disponível em: https://www.theguardian.com/technology/2017/sep/07/new-artificial-intelligence-can-tell-whether-youre-gay-or-straight-from-a-photograph. Acesso em: 15 mar. 2022; E ainda: GABBATT, Adam. MORRIS, Sam. *AI can tell Republicans from Democrats* – but can you? Take our quiz. The Guardian, 12 set. 2017. Disponível em:

Ana Frazão alerta para o fato de que o futuro das pessoas e das próprias democracias pode estar atrelado a julgamentos algorítmicos já que, no contexto atual, não só a economia é movida a dados, mas também a sociedade e a política.[32] Aliás, nessa mesma direção, Rodotá afirma que uma forte proteção de dados pessoais continua a ser uma utopia necessária para garantir a natureza democrática dos sistemas políticos.[33]

I.4 – VIGILÂNCIA E RACISMO

Como visto no tópico I.2, a vigilância serve para atender tanto aos interesses do Estado quanto aos de agentes econômicos. Nesse contexto, não há como fugir de um debate sobre a questão racial, pois o racismo, assim como a vigilância, permeia todas as estruturas da sociedade, também ameaçando direitos fundamentais e, por consequência, a própria democracia.

A vigilância comercial tem como principais insumos os ativos de vigilância, descritos por Shoshana Zuboff como superávit comportamental humano utilizado como matéria-prima para a busca por receita de vigilância e sua conversão em capital de vigilância.[34] Em termos práticos, grandes companhias como o *Google*, *Facebook* e *Amazon* se aproveitam da vastidão de dados (vozes, personalidades e emoções) para produzir conhecimento sobre o comportamento humano ao mesmo tempo em que o molda, visando aperfeiçoar produtos e aumentar seus lucros.

De acordo com Zuboff, essas companhias, as *big techs*, detêm um poder que não deve ser negligenciado, o instrumentarismo. Para a autora, esse poder tem a capacidade de fazer valer a sua vontade, sem precisar de armamentos e exércitos, através do meio automatizado de uma arquitetura computacional cada vez mais ubíqua, composta por dispositivos, coisas e espaços inteligentes conectados em rede.[35]

As *big techs* concentram cada vez mais o fluxo de dados à medida em que se expandem. Seus negócios são primariamente baseados em algoritmos computacionais projetados para maximizar as vendas. Esses algoritmos, da mesma forma que humanos, podem apresentar comportamentos discriminatórios nos seus julgamentos. Equipados com Inteligência Artificial e conectados a grandes

---

https://www.theguardian.com/technology/2017/sep/12/artificial-intelligence-republicans-democrats-quiz. Acesso em: 15 mar. 2022.

[32] FRAZÃO, Ana. Op. cit., 2021. n.p.

[33] RODOTÀ, Stefano. Op.cit., 2008. p. 15.

[34] ZUBBOF, Shoshana. Op. Cit., 2021. p.114.

[35] Ibid. p.19.

bases de dados, eles terminam por reforçar as mesmas desigualdades do mundo real: de idade, gênero, raça, lugar de origem, local de moradia etc. Esse processo é chamado por Safiya Noble de opressão algorítmica.[36]

Ana Frazão observa que os julgamentos realizados por algoritmos permitem aos agentes econômicos diversas possibilidades de ação, inclusive no que diz respeito a diferenciar consumidores, seja para cobrar distintos preços, seja para negar acesso a determinados serviços ou condições específicas.[37] Assim, se estabelecem condições para que uma categoria muito particular de racismo se manifeste: o racismo algorítmico.

Os algoritmos são utilizados para decidir questões importantes da vida humana, que vão desde o conteúdo que um usuário consome nas redes sociais a análises de crédito. Dando espaço para correlações indevidas e generalizações, cada sociedade olha para o passado ao lançar mão de algoritmos para tomada de decisões automatizadas. Assim, é fácil supor que na sociedade americana, por exemplo, latinos, negros e povos do oriente médio seriam os mais afetados por essas decisões automatizadas. No Brasil, é fato que principalmente os negros são os mais afetados.[38]

Esses grupos marginalizados no mundo real são, portanto, transplantados para o mundo digital, resultando no que Virginia Eubanks denomina de *digital poorhouses* (casas de abrigos digitais – tradução livre).[39] A autora observa que a população pobre e a classe trabalhadora dos Estados Unidos, durante o século XIX, foram isolados em casas de abrigos. No século XX, foram investigados por assistentes sociais e tratados como criminosos em julgamento. No século XXI, bancos de dados, algoritmos e modelos de risco resultaram no surgimento de verdadeiros abrigos digitais.[40]

A vigilância estatal, representada principalmente pelo sistema criminal, é também fortemente marcada pela disparidade racial. Diferente da vigilância comercial, as questões raciais em torno da vigilância estatal não são recentes e são, há muito tempo, debatidas no âmbito do policiamento, na execução de política de drogas, sistema punitivo etc.

---

[36] NOBLE, Safiya. *Algorithms of oppression:* how search engines reinforce racism. Nova York: New York University Press, 2018. p 4.
[37] FRAZÃO, Ana. Op. cit., 2021. n.p.
[38] RAMOS, Silvia (coord.). *Retratos da Violência* – Cinco meses de monitoramento, análises e descobertas. Rio de Janeiro: Rede de Observatórios da Segurança/CESeC, nov. 2019. p. 69.
[39] EUBANKS, Virginia. *Automating Inequality:* How High-Tech Tools Profile, Police, and Punish the Poor. St. Martin's Press, 2018. n.p
[40] Ibid.

Tomando como exemplo os Estados Unidos, país com a maior população carcerária do mundo,[41] a União Americana por Liberdades Civis (ACLU) apontou, em relatório de abril de 2020, que apesar das taxas comparáveis de uso de maconha entre brancos e negros, este último grupo tem 3,64 mais chances de ser preso por porte de maconha. A disparidade racial se manteve mesmo nos estados americanos que legalizaram a maconha.[42] O exemplo americano é pertinente, pois o Brasil, país com a terceira maior população carcerária do mundo,[43] trilha o mesmo caminho percorrido pelos Estados Unidos, executando uma política de encarceramento dos mais vulneráveis, sobretudo das pessoas negras.

A vigilância estatal também se beneficia das descobertas do Capitalismo de Vigilância, sendo ela a principal cliente das *big techs* na compra de tecnologias de vigilância, especialmente as voltadas para o reconhecimento facial. Veremos mais adiante o quanto essas tecnologias vêm sendo progressivamente empregadas pela segurança pública no mundo todo com o fim de monitoramento e controle. O problema dessa relação entre a vigilância estatal e comercial é que ela decorre de um sistema racista que flerta cada vez mais com tecnologias de alto potencial discriminatório.

Por fim, é importante pontuar que esse sistema racista é fruto de uma disparidade racial que também ocorre no processo político. Djamila Ribeiro pontua que a população negra é utilizada como uso político, como beneficiária de políticas públicas e não como sujeitos políticos que ajudam a pensar as políticas públicas. Por isso, a autora é categórica ao afirmar que discutir democracia é necessariamente discutir o antirracismo.[44]

---

[41] Segundo o *World Prison Brief*, os Estados Unidos possuem a maior população carcerária do mundo, com mais de 2 milhões de presos. Ver mais em: *Highest to Lowest* - Prison Population Total. WPB – World Prison Brief. Disponível em: https://www.prisonstudies.org/highest-to-lowest/prison-population-total?field_region_taxonomy_tid=All. Acesso em: 11 fev. 2022.

[42] NEW *ACLU Report:* Despite Marijuana Legalization Black People Still Almost Four Times More Likely To Get Arrested. ACLU, abr. 2020. Disponível em: https://www.aclu.org/press-releases/new-aclu-report-despite-marijuana-legalization-black-people-still-almost-four-times. Acesso em: 29 out. 2021.

[43] Segundo o *World Prison Brief*, o Brasil possui a 3ª maior população carcerária do mundo, com mais de 800.000 de presos. Ver mais em: *Highest to Lowest* - Prison Population Total. WPB – World Prison Brief. Disponível em: https://www.prisonstudies.org/highest-to-lowest/prison-population-total?field_region_taxonomy_tid=All. Acesso em: 11 fev. 2022.

[44] Entrevista concedida por Djamila Ribeiro no programa Roda Viva, TV Cultura, em 09 de nov. de 2020. *Djamila Ribeiro no Roda Viva:* "Discutir democracia é discutir antirracismo". Disponível em: https://www.youtube.com/watch?v=jn1AtnzTql8. Acesso em: 29 out. 2021.

CAPÍTULO II – RECONHECIMENTO FACIAL E RACISMO ALGORÍTMICO

II.1 – BREVE HISTÓRICO SOBRE AS TECNOLOGIAS DE RECONHECIMENTO FACIAL

No mesmo período em que importantes estudos na área de Psicologia foram realizados sobre o rosto humano e suas expressões[45] foram lançadas as bases para o reconhecimento facial moderno. Enquanto o homem ainda descobria os segredos escondidos nas linhas do rosto humano, também, tentava ensinar as máquinas a fazê-lo com a mesma precisão. Aliás, a denominada psicologia do reconhecimento facial não apenas ofereceu posteriormente as balizas para o desenvolvimento de avanços nas Tecnologias de Reconhecimento Facial (TRFs),[46] como também possibilitou o surgimento da chamada *Computação Afetiva*, campo da Ciência da Computação que se ocupa da análise das expressões da face humana.[47]

Em 1959, os matemáticos Woody Bledsoe e Iben Browning, em artigo científico intitulado *Pattern Recognition and Reading by Machine*, descreveram um modelo matemático para o reconhecimento de padrões alfanuméricos com o objetivo de reduzi-los a uma linguagem de máquina.[48] Em outras palavras, desenvolveram um modelo capaz de discriminar, categorizar e quantificar padrões em letras e números, tanto em textos impressos quanto em manuscritos. Desse modo, poderia se conceber uma máquina capaz de realizar a leitura de textos automaticamente.

Em trabalho posterior, realizado entre 1964 e 1965, em colaboração com Helen Chan e Charles Bisson, Bledsoe passou a trabalhar em um computador que pudesse reconhecer rostos humanos.[49] O sistema desenvolvido consistia basicamente em duas etapas: na primeira, se definia um banco de dados de imagem alimentados por um operador do sistema (humano). Esse banco de dados continha medidas

---

[45] Em 1960, o professor Paul Ekman, da Universidade da Califórnia realizou uma série de estudos sobre microexpressões faciais humanas. Seus estudos no campo da Psicologia até hoje influenciam na construção de Tecnologias de Reconhecimento Facial. *Dr. Ekman's Work:* A timeline of achievements. Disponível em: https://www.paulekman.com/about/paul-ekman. Acesso em: 08 jun. 2021.

[46] Ao publicarem o artigo *Eigenfaces for Recognition* PENTLAND e TURK esclareceram que sua abordagem além de biologicamente implementável estava de acordo com descobertas preliminares na fisiologia e psicologia do reconhecimento facial. PENTLAND, Alex. TURK, Matthew. *Eigenfaces for Recognition*. J Cogn Neurosci 1991; 3 (1): 71–86. Disponível em: https://doi.org/10.1162/jocn.1991.3.1.71. Acesso em: 5 jun. 2021.

[47] Conforme descreve, Shoshana Zuboff em *A era do capitalismo de vigilância*, a Computação afetiva surgiu a partir dos trabalhos de Rosalid Picard do MIT, que em 1997 publicou *Affective Computing*. As aplicações práticas desse campo da Ciência da Computação incluem a venda de análise sobre emoções de indivíduos para fins publicitários. ZUBBOF, Shoshana. Op. cit., 2021. p. 223.

[48] BLEDSOE, W. BROWNING, I. *Pattern recognition and reading by machine*. IRE-AIEE-ACM computer conference (IRE-AIEE-ACM '59 (Eastern)). Association for Computing Machinery, Nova York, 225–232. DOI: https://doi.org/10.1145/1460299.1460326. 1959.

[49] BOYER, Robert S. *Automated Reasoning:* Essays in Honor of Woody Bledsoe. Kluwer Academic Publishers, 1991. p. 11.

de pontos da face extraídas manualmente pelo operador formando padrões de rostos representados em uma fotografia.

Na segunda etapa, ocorria o reconhecimento da imagem, em que se apresentava ao sistema uma das fotografias usadas para alimentar o banco de dados. O sistema então realizava a busca e o reconhecimento do rosto a partir do banco de dados previamente definido. Os sistemas de reconhecimento facial modernos não apresentam uma lógica muito diferente, de modo que até hoje se reconhece a importante contribuição do trabalho de Bledsoe para essas tecnologias.

Muito embora, após esse período, tenha havido alguns trabalhos importantes sobre reconhecimento facial,[50] foi somente em 1991 que houve uma grande evolução, quando os pesquisadores Matthew Turk e Alex Pentland conseguiram implementar o reconhecimento facial automatizado, ou seja, sem a necessidade de participação humana.[51] Já nos anos 90, se inicia o uso comercial das TRFs, com enfoque da indústria em instituições de sistemas penais e órgãos governamentais com o papel de emissão de documentos, como passaportes, documento de identificação etc.[52]

Nos anos 2000, a guerra ao terrorismo empreendida pelos Estados Unidos intensificou o uso de tecnologias de vigilância gerando um aumento de demanda por TRFs. Conforme aponta Kevin Bowyer, os atentados de 11 de setembro de 2001 colocaram em foco estudos no campo da biometria, incluindo o reconhecimento facial.[53] Até o final da década, esta tecnologia se tornaria mais frequente, sendo disponibilizada comercialmente também a pessoas comuns, embutida em *notebooks*, telefones móveis e outros dispositivos com câmera.[54]

O *big data* representou um novo momento para as TRFs. Isso porque, conforme menciona Samuel Oliveira, enquanto tradicionalmente os sistemas inteligentes de vigilância se valiam da

---

[50] Em 1970 o professor Takeo Kanade publicou uma tese de Ph.D. intitulada *Picture processing system by computer complex and recognition of human faces*. Outro importante trabalho foi o de Kirby, M. e Sirovich, L intitulado *Application of the Karhunen-Loeve procedure for the characterization of human faces.* O primeiro desenvolveu um modelo teórico para o reconhecimento facial automatizado e o segundo resultou no surgimento de uma nova abordagem utilizada no reconhecimento facial, o *Eigenface.*

[51] LEE-MORRISON, Lila. *Portraits of Automated Facial Recognition:* on machinic ways of seeing the face. Bielefeld: Transcript Verlag, 2019. p. 56.

[52] GATES, Kelly. *Our biometric future:* facial recognition technology and the culture of surveillance. New York University Press, 2011. p. 27.

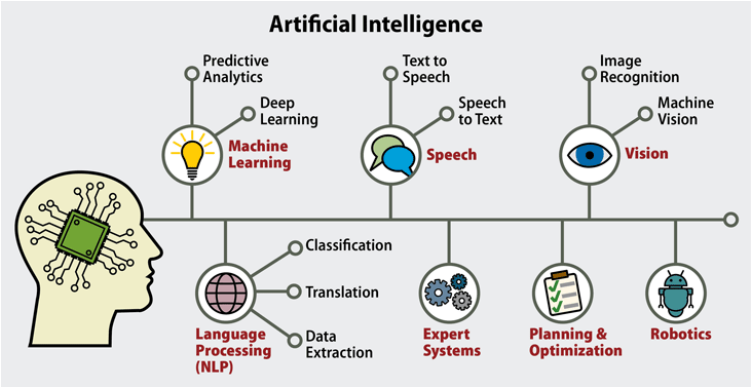
[53] BOWYER, K. W. *Face recognition technology*: security versus privacy. IEEE Technology and Society Magazine, vol. 23, no. 1, pp. 9-
19, Spring 2004, doi: 10.1109/MTAS.2004.1273467. Disponível em: https://ieeexplore.ieee.org/document/1273467. Acesso em: 11 jun. 2021.

[54] Em 2005, a empresa OMRON, atuante no campo de automação, anunciou a primeira tecnologia de reconhecimento para dispositivos móveis. *OMRON Announces "OKAO Vision Face Recognition Sensor", World's First Face Recognition Technology for Mobile Phones*. 28 fev. 2005. Disponível em: https://www.omron.com/global/en/media/press/2005/02/n_280205.html. Acesso em: 11 jun. de 2021.

tecnologia de reconhecimento facial apenas para fornecer uma confirmação visual de eventos, os sistemas digitais atuais possibilitam o reconhecimento de pessoas a partir de um cruzamento de informações com enormes bancos de dados, a própria imagem de vídeo torna-se a fonte de informação.[55]

A Inteligência Artificial foi também fundamental para o desenvolvimento das TRFs. Na verdade, o reconhecimento facial era visto como um braço do campo da Inteligência Artificial.[56] Segundo Manuel de Landa, o desenvolvimento de visão para máquinas envolvia resolver uma parte dos problemas centrais da Inteligência Artificial. Desse modo, para que a máquina fosse inteligente, seria preciso ter habilidade de ver como os seres humanos.[57] O progresso da Inteligência Artificial e seus subcampos propiciou ainda o surgimento de Redes Neurais Artificiais (*Artificial Neural Network*) e do Aprendizado de Máquina (*Machine Learning*), hoje amplamente utilizados nas TRFs.

Figura 1 - Subcampos da inteligência artificial



Fonte: GREEGARD, Samuel (2019)

Atualmente, o reconhecimento facial está consolidado como uma forma de identificar ou confirmar a identidade de um indivíduo através do rosto. Neste sentido, Samuel Oliveira explica que as TRFs correspondem a *softwares*, programas de computador, que empregam diferentes técnicas de Inteligência Artificial para reconhecer ou identificar rostos humanos a partir de uma imagem, geralmente obtida de fotos ou vídeos.[58]

---

[55] OLIVEIRA, Op. cit., 2021. p. 44.
[56] O pai do reconhecimento facial, Woody Bledsoe, também foi um dos grandes responsáveis pelo surgimento da Inteligência Artificial.
[57] LANDA, Manuel de. *War in the Age of Intelligent Machines*. New York: Zone Books, 1991. p. 193.
[58] OLIVEIRA, Op. cit., 2021. p. 43.

Quando equipadas com Inteligência Artificial e aprendizagem de máquina, as TRFs são capazes de se conectarem a grandes bases de dados, realizando processamento de imagens e fornecendo resultados em tempo real de ambientes com grande fluxo de pessoas, como aeroportos e rodovias. Parte dos desafios atuais para essas tecnologias envolvem o aprimoramento da acurácia dos seus algoritmos[59] e da qualidade dos dados que alimentam suas decisões.

Importante esclarecer que as TRFs não se resumem a algoritmos, tampouco a dispositivos de captura de imagem. São, na verdade, um conjunto de vários elementos para que o reconhecimento facial se torne possível: algoritmos, bancos de imagem (*datasets*) e dispositivos de captura de imagem. Para o seu funcionamento, não necessariamente são acopladas soluções de *big data* ou inteligência artificial à sua estrutura. Dessa forma, diferente de sistemas de reconhecimento facial em tempo real, instalados em locais públicos com grande fluxo de pessoas, que requerem o processamento rápido de grande volume de informações, sistemas embutidos em celulares, por exemplo, são mais simples e, portanto, não carecem de acesso a grandes volumes de dados.

Com relação às TRFs no Brasil, no final dos anos 90, a impressa brasileira repercutia o uso do reconhecimento facial no exterior,[60] mas internamente ainda estava restrito a laboratórios de pesquisa nas universidades. Em meados dos anos 2000, já havia utilização prática na segurança pública com implementação voltada para a emissão de documentos oficiais de identificação e monitoramento de locais públicos.[61] Já nos últimos anos, pôde se verificar, cada vez mais, a presença dessas tecnologias no mercado brasileiro atendendo ao setor privado e público.

No setor privado, por exemplo, empresas tem utilizado o reconhecimento facial até mesmo para identificar as emoções do usuário ao comprar os seus produtos.[62] No setor público, vem ganhando destaque notícias referentes à utilização de reconhecimento facial pela segurança pública na realização

---

[59] Empresas tem competido entre si para aperfeiçoar tecnologias de reconhecimento facial submetendo seus algoritmos a agências de qualidade ou mesmo a torneios internacionais para algoritmos de reconhecimento facial como o *Wider Face and Person Challenge*.

[60] Em 1998, o Jornal do Brasil, publicou a matéria *Sob o olhar do Grande Irmão: Recursos eletrônicos ajudam o Estado a fiscalizar seus cidadãos e emprestam à democracia britânica um sombrio manto solitário*. Com referência à clássica obra de George Orwell, 1984, a matéria destacava o uso de tecnologia na vigilância estatal, incluindo o reconhecimento facial.

[61] Em 2006, o Jornal do Rio Grande do Sul, Ponto Inicial destacava na matéria *Documento de Identificação sofrerá mudança* um contrato assinado pelo Governador do RS para emissão e carteira de identidade digitalizada. Segundo a mesma matéria, as imagens registradas no órgão responsável pela emissão de documentos integrariam um banco de dados de última geração que seria também utilizado para o reconhecimento facial de indivíduos em jogos de futebol e eventos semelhantes.

[62] Em 2019, a Loja *Hering* desenvolveu uma loja conceito, chamada *Hering Experience*, em que o cliente tinha suas emoções captadas por meio de tecnologia de reconhecimento facial.

de prisões.[63] Também, por influência da pandemia da Covid-19, autoridades do setor aeroportuário tem adotado o reconhecimento facial nos aeroportos de algumas cidades para realização de embarques.[64] Contudo, grande parte do uso dessa tecnologia pelo poder público está no setor de transporte, visando reduzir fraudes em gratuidades.[65]

II.2 – COMPREENDENDO O PROCESSO DE RECONHECIMENTO FACIAL

Muito embora ainda sejam vistas como elementos de ficção científica, as TRFs ganham cada vez mais espaço no cotidiano. Utilizamos rotineiramente nossa face não só para desbloquear dispositivos eletrônicos como também para autenticação de acesso em diversos aplicativos móveis de bancos, investimentos, mensagens eletrônicas etc. Aos poucos, as senhas pessoais estão sendo deixadas de lado, pois passaram a ser vistas como menos seguras que alternativas biométricas como o reconhecimento facial, a digital e a íris.

O motivo pelo qual, dentre tantas formas de biometria existentes, o reconhecimento facial tem se tornado tão utilizado é por ser uma tecnologia não invasiva, podendo ser utilizada à distância, sem a interação do usuário, em tempo real ou até mesmo por imagens e vídeos já gravados. Há ainda o importante fato de que seres humanos são limitados na capacidade de memorizar e reconhecer rostos, se comparados com máquinas que podem realizar essas tarefas em velocidades muito maiores. Além dessas características, destaca-se o grande avanço na qualidade de câmeras de segurança e de aparelhos móveis.[66] Também foram importantes o surgimento de novos modelos matemáticos e a evolução da Inteligência Artificial[67] que propiciaram o aperfeiçoamento dos algoritmos[68] empregados no reconhecimento facial.

---

[63] FORAGIDO da Justiça é preso com ajuda do reconhecimento facial. UOL, 20 mar. 2021. Disponível em: https://atarde.uol.com.br/bahia/salvador/noticias/2161780-foragido-da-justica-e-preso-com-ajuda-do-reconhecimento-facial. Acesso em: 15 jun. 2021.

[64] AEROPORTOS testam sistema de reconhecimento facial para facilitar embarque. GLOBO, 21 dez. 2020. Disponível em: https://g1.globo.com/economia/tecnologia/noticia/2020/12/21/aeroportos-testam-sistema-de-reconhecimento-facial-para-facilitar-embarque.ghtml. Acesso em: 15 de jun. 2021.

[65] Segundo levantamento do Instituto Igarapé, foram registrados 48 casos de implementação de reconhecimento facial pelo setor público. Sendo 13 na área de segurança pública e 21 na área de transporte. Ver mais em: INSTITUTO IGARAPÉ. *Reconhecimento facial no Brasil*. Instituto Igarapé. Disponível em: https://igarape.org.br/infografico-reconhecimento-facial-no-brasil. Acesso em: 15 jun. 2021.

[66] STAN, L. JAIN, Anil K. Introduction. *In: Handbook of Face Recognition*. Editado por STAN, L. JAIN, Anil K. 2ª Edição. London: Springer, 2011. p. 1

[67] O método *Eigenface* revolucionou o Reconhecimento facial melhorando sua performance e eficiência, chegando a superar seres humanos em ambientes controlados. Ibid. p. 2.

[68] BANERJEE, Pradipta, DATTA, Asit. DATTA, Madhura. *Face Detection and Recognition*: Theory and Practice. Boca Raton, FL: Taylar & Francis Group, 2016. p. 28.

O uso cada vez mais recorrente das TRFs é acompanhado de considerável risco à sociedade. Isso porque os modelos e algoritmos utilizados podem apresentar problemas de ordem técnica em seus processos, que podem afetar diretamente os indivíduos objetos de reconhecimento. Nesse sentido, faz-se necessário um conhecimento mínimo sobre as etapas existentes em um processo de reconhecimento facial.

O processo de reconhecimento facial é dividido em quatro etapas: detecção, normalização, extração e reconhecimento. Conforme descrevem Li Stan e Anil Jain, a detecção é o processo de localizar pontos que formam o rosto (olhos, boca, nariz, linha facial). Na normalização, são realizados ajustes fotométricos, padronização da imagem (escala de cinza, iluminação, tamanho). Após normalizada, o processo de extração identifica saliências da face que a tornam distinguíveis de outras faces.[69]

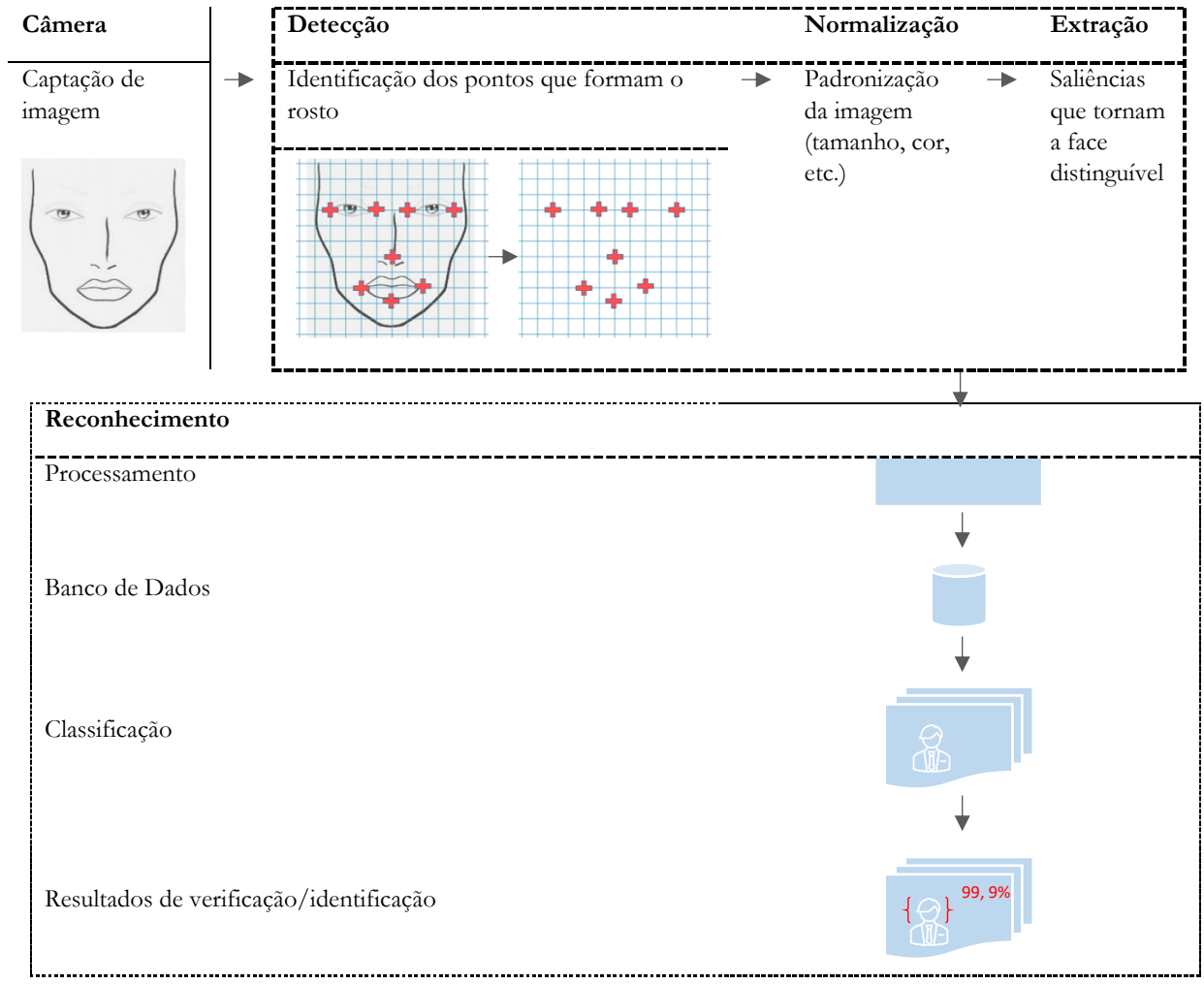
Por fim, o reconhecimento é um processo que compara o rosto detectado com os registros de um banco de dados de imagens buscando uma correspondência. Na etapa de reconhecimento as falhas podem estar relacionadas ao banco de imagens, que pode conter vieses. Um algoritmo treinado em um banco de imagens com pessoas negras pode ter uma taxa de eficácia de reconhecimento diferente quando utilizado com pessoas brancas, por exemplo, o que traz o risco de graves consequências para um dos grupos.[70]

---

[69] STAN, L. JAIN, Anil K. Op. cit., 2011. p. 4.

[70] Em 2016, o jornal independente americano, *Pro Publica*, publicou um editorial sobre discriminação contra negros na análise de risco de um sistema que avaliava a probabilidade de uma pessoa detida cometer crimes no futuro. Ver mais em: ANGWIN, JULIA. ET. AL. *Machine Bias:* There's software used across the country to predict future criminals. And it's biased against blacks. Pro Publica, 23 maio 2016. Disponível em: https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing. Acesso em: 12 fev. 2021.

Figura 2 – Etapas básicas do Processo de reconhecimento facial



Fonte: elaborado pelo autor

Existe uma grande variedade de bancos de dados de imagens que são utilizados nesse processo. Esses bancos são importantes para testar a eficácia e a acurácia dos algoritmos no processo de reconhecimento facial. Apesar das variações, em linhas gerais, esses bancos de dados se constituem de uma série de imagens com diferentes posições, angulações e iluminação que são comparadas com o rosto detectado na primeira fase do processo de reconhecimento facial. Quanto maior o banco de dados utilizado para testagem melhor a performance do algoritmo.[71]

[71] No artigo *Naive-deep face recognition: Touching the limit of LFW benchmark or not?* os pesquisadores E. Zhou, Z. Cao, e Q. Yin, da Universidade de Cornell, demonstraram que bancos de dados maiores proporcionam mais eficácia em testes de algoritmos de reconhecimento facial. CAO, Z. Yin, Q. ZHOU, E. *Naive-Deep Face Recognition:* Touching the Limit of LFW Benchmark or Not?. 2015. p. 1. Disponível em: https://arxiv.org/abs/1501.04690. Acesso em: 12 fev. 2021.

Figura 3 - Variações de poses de um rosto do banco de imagens *Multi-PIE*.

Fonte: GROSS, Ralph et al (2008, np)

A performance de um algoritmo de reconhecimento facial é medida pela margem de acertos realizados a partir de testes com bancos de imagens e em ambientes controlados. Segundo William Crumpler e James Lewis, na prática, ferramentas de reconhecimento facial podem ser pensadas como uma forma de avaliar uma alegação. Esta alegação pode ser qualquer coisa entre "*essa pessoa é quem alegam que ela é?*" e "*esta pessoa está registrada nesta base de dados?*". Nesse sentido, um algoritmo não vai afirmar categoricamente que o indivíduo detectado na imagem analisada é o mesmo registrado no banco de imagens.[72] Na verdade, os algoritmos realizam uma avaliação estatística, ou seja, apontam a probabilidade de o indivíduo detectado ser o indivíduo registrado no banco de dados. Isso quer dizer que as TRFs, de um modo geral, são baseadas em previsões estatísticas.

Em síntese, o algoritmo identifica a presença de um rosto e realiza o seu reconhecimento por meio de comparação probabilística com rostos já guardados em um banco de dados. Falhas no processo de detecção poderão afetar os indivíduos na medida em que seus rostos não puderem ser reconhecidos ou forem falsamente reconhecidos.[73]

---

[72] CRUMPLER, William. LEWIS, James A., *Questions about Facial Recognition*. Center for Strategic and International Studies (CSIS), 2021. p. 6. Disponível em: http://www.jstor.org/stable/resrep28766. Acesso em: 19 jun. 2021.

[73] No documentário Coded Bias, a pesquisadora do MIT Media Lab, Joy Buolamwini, conta como descobriu, desenvolvendo um software que simula um espelho, que mulheres negras não eram adequadamente reconhecidas pelo sistema. O software utilizava modelos de reconhecimento facial existentes e amplamente utilizados. CODED BIAS. Direção: Shalini Kantayya. Produção: Shalini Kantayya. Co-Produção: Sabine Hoffman. China, Estados Unidos, Gra Bretênia: 7ª Emire Media, 2020. *Streaming*.

II.3 – O PROBLEMA DA ACURÁCIA

Conforme explicam Débora Bonat e Fabiano Hartmann, a acurácia refere-se à exatidão de um resultado em relação a um parâmetro tomado como referência.[74] Desse modo, pode se concluir que a acurácia de um sistema de reconhecimento facial está relacionada com a exatidão em relação à identificação e ao reconhecimento do rosto humano.

Como sistemas que tentam imitar os sentidos humanos, as TRFs encontram problemas muito similares enfrentados pelas pessoas. O ser humano pode apresentar falhas na tarefa de reconhecimento de um rosto em decorrência de fatores como a iluminação do ambiente, a distância e a posição do indivíduo a ser reconhecido. A acurácia dos algoritmos de reconhecimento facial pode ser afetada por esses mesmos fatores.

A taxa de acurácia de um algoritmo de reconhecimento facial inferior a 100% indica que uma parcela dos resultados se constitui de rostos não reconhecidos ou de falsos positivos. No mundo real, esses erros ou falsos positivos representam pessoas que não tiveram seus rostos detectados ou que foram falsamente reconhecidos. Nestas situações é que se verificam casos de injustiça, como a associação de um indivíduo a um determinado crime, identificação incorreta de gênero ou a negativa de um serviço ou direito a um consumidor, por exemplo.

Conforme Cathy O'Neil, para as instituições que empregam algoritmos na tomada de decisões automatizadas, as pessoas afetadas injustamente por decisões automatizadas representam dano colateral.[75] São as vítimas não intencionais de uma guerra empreendida para o controle absoluto de nossos dados. Muito embora os índices de dano colateral possam sugerir um número baixo de indivíduos afetados, o largo uso dessas tecnologias na sociedade atual demonstra que grupos inteiros podem ser prejudicados. Não é por outra razão que, algoritmos como esses, são denominados por Cathy O'Neil de Armas de Destruição em Massa – ADMs.[76]

---

[74] BONAT, Débora. HARTMANN PEIXOTO, Fabiano. *Racionalidade no Direito:* inteligência artificial e precedentes. 1ª ed. Curitiba: Alteridades. 2020. n.p.

[75] O'NEIL, Cathy. *Algoritmos de destruição em massa:* como o *big data* aumenta a desigualdade e ameaça à democracia. 1ª edição. Tradução: Rafael Abraham, Santo André, SP: Ed. Rua do Sabão, 2020. p. 23.

[76] Ibid. p. 8. Armas de destruição em massa foi a tradução dada pela editora ao traduzir o livro da autora chamado *Weapons of Math Destruction*, que fez um trocadilho com a palavra *Math* (matemática), tendo em vista que esses algoritmos que afetam as pessoas são desenvolvidos por matemáticos.

Em laboratórios e com ambientes controlados os testes de TRFs apresentam altas taxas de eficácia, superando inclusive o ser humano. Contudo, em ambientes não controlados, essas taxas sofrem significativas reduções. Nesse sentido, Crumpler elucida[77] que:

> Em condições ideais, os sistemas de reconhecimento facial podem ter uma precisão quase perfeita. Algoritmos de verificação usados para combinar assuntos com imagens de referência claras (como uma foto de passaporte ou foto) podem alcançar pontuações de precisão de até 99,97% em avaliações como o Teste de Fornecedor de Reconhecimento Facial (FRVT)[78] do NIST[79] [...]. No entanto, esse grau de precisão só é possível em condições ideais, onde há consistência na iluminação e no posicionamento e onde as características faciais dos sujeitos são claras e não obscurecidas. Em implantações no mundo real, as taxas de precisão tendem a ser muito mais baixas (tradução nossa).

Como abordado no tópico anterior, no reconhecimento facial a etapa de detecção envolve a localização das características da face como olhos, boca, nariz, contorno do rosto. De acordo com Banerjee et al, a acurácia de um sistema de reconhecimento facial é altamente dependente das características que são extraídas para representar um rosto, que, por sua vez, dependem da localização e normalização correta do rosto.[80] Os mesmos autores apontam que a melhoria de acurácia dos sistemas de reconhecimento facial envolve a combinação de outros métodos biométricos como o reconhecimento da voz, da impressão digital e leitura da íris.[81]

O aperfeiçoamento das TRFs por meio de combinação com outros métodos biométricos encontra problemas na sua concretização, pois nem sempre é possível essa combinação. Aparelhos de telefones podem vir equipados com sensores capazes de ler simultaneamente as digitais e o rosto, o que em tese aumentaria a sua acurácia, conforme a sugestão dada por Banerjee et al. Contudo, sistemas de vigilância realizam o reconhecimento facial até mesmo sem o conhecimento do indivíduo e à distância, de modo que a combinação com outras tecnologias pode ser, não apenas econômica, mas também tecnicamente inviável. Nesse sentido, a acurácia das TRFs no nível algorítmico ainda constitui um problema importante a ser resolvido.

---

[77] CRUMPLER, William. *How Accurate are Facial Recognition Systems* – and Why Does It Matter?. CSIS. 2020. Disponível em: https://www.csis.org/blogs/technology-policy-blog/how-accurate-are-facial-recognition-systems-%E2%80%93-and-why-does-it-matter. Acesso em: 20 de jun. 2021.

[78] O Teste de Fornecedor de Reconhecimento Facial ou FRVT é um teste de algoritmos de reconhecimento facial realizado pelo *National Institute of Standards and* Technology (NIST) órgão congênere do Inmetro no Brasil.

[79] O *National Institute of Standards and Technology* (NIST) é um órgão congênere do Inmetro no Brasil.

[80] BANERJEE, DATTA e DATTA. Op. cit., 2016. p. 10.

[81] Ibid. p. 303.

Um caso notório relacionado à falta de acurácia das TRFs foi o já mencionado *Rekogntion*, *software* de reconhecimento facial da *Amazon* anunciado com acurácia de 99,9997%. A ACLU conduziu um teste do *Rekognition* com os membros do Congresso Nacional americano. Os resultados apontaram o reconhecimento errôneo de 28 dos 535 congressistas analisados a partir de um banco de dados com 25 mil imagens de pessoas condenadas à prisão.[82] Em um artigo, John Honovich apontou que a *Amazon* estava correta, considerando 28 falsos positivos de um universo de 132.375.000 comparações (535 congressistas x 25.000 imagens de presos condenados).[83]

Números são mais facilmente descartáveis, contudo, os resultados do teste realizado pela ACLU reforçam a afirmação de Cathy O'Neil de que pessoas do mundo real podem, eventualmente, virem a ser consideradas como dano colateral. Daí surge uma problemática que é o risco de naturalização da violência por meio de decisões automatizadas. A partir de uma reflexão sobre o papel da tecnologia como importante ferramenta para o combate às violações de direitos humanos, apesar do possível pequeno número de vítimas que o percentual desses danos possa indicar, não se pode encarar com desprezo a grave violação de direitos fundamentais decorrentes do uso dessas tecnologias.

II.4 – ENVIESAMENTO

Alguns autores criticam a chamada fé na imparcialidade e objetividade da tecnologia, que assume aos poucos algumas tarefas humanas. Frank Pasquale expõe que os preconceitos e valores humanos estão embutidos em cada etapa do desenvolvimento de sistemas automatizados.[84] Em sentido semelhante, Safiya Noble destaca que os modelos matemáticos codificam preconceitos humanos, equívocos e vieses, e que tendem a punir os pobres e oprimidos em nossa sociedade.[85]

Tarcizio Silva faz uma interessante conexão entre a ideia de democracia racial e neutralidade na tecnologia. Para o autor, há uma dupla opacidade na convergência entre a negação do racismo e na negação da política na tecnologia. Nesse sentido, explica que, apesar de serem dois conceitos

---

[82] SNOW, Jacob. *Amazon's Face Recognition Falsely Matched 28 Members of Congress With Mugshots*. ACLU, 2018. Disponível em: https://www.aclu.org/blog/privacy-technology/surveillance-technologies/amazons-face-recognition-falsely-matched-28. Acesso em: 20 jun. 2021.
[83] HONOVICH, John. *99.9997% Accurate Amazon Facial Rekogntion Falsely Matches 28*. IPVM. 2018. Disponível em: https://ipvm.com/reports/amazon-aclu-28. Acesso em: 20 jun. 2021.
[84] PASQUALE, Frank. Op. Cit., 2015. p. 35.
[85] NOBLE, Op. cit., 2018. p. 39.

aparentemente distantes, se irmanam no propósito de ocultar relações de poder que constroem interpretações de mundo, naturalizam e aprofundam exploração de desigualdades.[86]

Os algoritmos são passíveis de enviesamento devido ao fato de atenderem exclusivamente ao modo e aos critérios aplicados pelo seu criador – o programador.[87] O questionamento da objetividade da tecnologia esbarra na opacidade que envolve esses modos e critérios, o que potencializa seus efeitos danosos para sociedade.

Para Safiya Noble, os veredictos proferidos por matemáticos e cientistas da computação estão fora de discussão e de apelação.[88] Nessa linha, Ana Frazão dispõe que, à medida em que são elaborados por homens, é inequívoco que a racionalidade limitada dos programadores pode transpor para as fórmulas dos algoritmos uma série de vieses e problemas cognitivos, os quais, diante da falta de transparência, não terão como ser objeto do devido escrutínio social, da crítica e do aprimoramento.[89]

A compreensão do problema do enviesamento na tecnologia demanda um olhar sobre a participação de minorias na produção tecnológica. Conforme Samuel Oliveira, geralmente, os pesquisadores e desenvolvedores de IA são pessoas do sexo masculino, provenientes de determinadas demografias raciais, que cresceram em áreas socioeconômicas elevadas, e são, principalmente, pessoas sem deficiência. [90]

A falta de inclusão de mulheres na indústria tecnológica, por exemplo, resulta em machismo. Assim explica Maria Lindoso, segundo a qual o conhecimento produzido, majoritariamente, por homens foi (e vem sendo) determinante para justificar o motivo pelo qual, também na área da tecnologia, é responsável pela perpetuação da discriminação de mulheres.[91]

Outro fator para a compreensão do enviesamento na tecnologia diz respeito aos dados que alimentam os modelos matemáticos desenvolvidos. Como explica Fabiano Hartman, o enviesamento dos dados tem forte ligação com *datasets* inadequados.[92] Conforme Fujimoto et al, embora algoritmos não possam fornecer respostas precisas a todas as questões, eles podem analisar os dados fornecidos

---

[86] SILVA, Tarcizio. *Racismo Algorítmico*: Inteligência artificial e discriminação nas redes digitais. São Paulo: Edições Sesc SP, 1ª ed. 2022. n.p. [*E-book*].
[87] OLIVEIRA, Op. cit., 2021. p. 43.
[88] NOBLE, Op. cit., 2018. p. 39.
[89] FRAZÃO, Ana. *Dados, estatísticas e algoritmos*. Perspectivas e riscos da sua crescente utilização. Jota, 28 de jun. 2017. Disponível em: https://www.jota.info/opiniao-e-analise/colunas/constituicao-empresa-e-mercado/dados-estatisticas-e-algoritmos-28062017. Acesso em: 17 ago. 2021.
[90] OLIVEIRA, Op. cit., 2021. p. 43
[91] LINDOSO, Maria Cristine Branco. *Discriminação de gênero no tratamento automatizado de dados pessoais* – Como a automatização incorpora vieses de gênero e perpetua a discriminação de mulheres. Rio de Janeiro: Processo, 2021. p. 84.
[92] HARTMANN PEIXOTO, Fabiano. *Direito e Inteligência Artificial*. Coleção Inteligência Artificial e Jurisdição. Volume 2. DR.IA. Brasília, 2020. Disponível em: https://orcid.org/0000-0002-6502-9897. p. 26.

(*inputs*) e oferecer "palpites" coerentes. Quanto maior a quantidade e qualidade dos dados disponibilizados ao algoritmo, maior a chance de o resultado estar próximo do real.[93]

Tanto a falta de representatividade na produção tecnológica quanto a má representação de determinados grupos nas bases de dados que alimentam a estrutura tecnológica são reflexos de uma racionalidade que se propõe dominante e superior. Nessa direção, Tarcizio Silva afirma que os processos de construção tanto das tecnologias digitais de comunicação quanto da ideologia do Vale do Silício são racializados, tendo como ponto de partida uma lógica de supremacia branca.[94] Diante disso, é possível observar impactos nocivos sobre diversos grupos vulnerabilizados: negros, latinos, asiáticos[95] e LGBTQIA+.[96]

Quando observamos especificamente as TRFs, modelos matemáticos testados com banco de imagens populado com imagens de pessoas brancas podem apresentar taxas de eficácia diferentes para pessoas não brancas, por exemplo.[97] A representatividade nos dados e a qualidade dos bancos de imagens utilizado na testagem são, por conseguinte, determinantes no resultado do processo de reconhecimento facial.

Conclui-se, portanto, que o enviesamento na tecnologia se dá tanto em razão de falta de representatividade na produção tecnológica, quando em razão da qualidade dos dados que alimentam essas tecnologias. Nesse contexto, muito embora, no reconhecimento facial, homens e máquinas cometam falhas similares, no caso das máquinas, há o agravante de que seus mecanismos são protegidos pelo segredo comercial. A real justificativa para a utilização de TRFs seria, na verdade, a massificação da vigilância. Não é à toa que Cathy O'Neil, ao questionar o uso das ADMs, posiciona a

---

[93] FUJIMOTO, Mônica Tiemy, MATTIUZZO, Marcela, MENDES, Laura Schertel. *Discriminação Algorítmica à Luz da Lei Geral de Proteção de Dados*. In: DONEDA, Danilo (coord.); SARLET, Ingo Wolfgang (coord.); MENDES, Laura Schertel (coord.); RODRIGUES JUNIOR, Otavio Luiz (coord.) BIONI, Bruno Ricardo (coord.). *Tratado de Proteção de Dados Pessoais*. Rio de Janeiro: Forense, 2021. p. 423.

[94] SILVA, Op. cit. 2022. n.p.

[95] Em 2018, o Governo americano apontou no relatório *Diversity in High Tech* que no setor da alta tecnologia brancos representavam 68,53% dos funcionários contratados. Negros somente 7,4%. Ver mais em: *Diversity in high tech*: Executive Summary. U.S. EQUAL EMPLOYMENT OPPORTUNITY COMISSION. Disponível em: https://www.eeoc.gov/special-report/diversity-high-tech. Acesso em: 24 jul. 2021.

[96] Em *Reconhecimento Facial no Setor Público e Identidade Trans*, as pesquisadoras Rafaela Silva e Joana Varon denunciam a falta de representatividade na produção tecnológica e como o reconhecimento facial pode afetar pessoas transgêneros. SILVA, Mariah Rafaela. VARON, Joana. *Reconhecimento Facial no Setor Público e Identidade Trans*:

[97] "[...] boa parte dos bancos de imagens utilizados para treinar esses algoritmos são compostos por pessoas brancas". Ver mais em: NUNES, Pablo. *O algoritmo e racismo nosso de cada dia*: Reconhecimento facial aposta no encarceramento e pune preferencialmente população negra. Piauí, 2 jan. 2021. Disponível em: https://piaui.folha.uol.com.br/o-algoritmo-e-racismo-nosso-de-cada-dia. Acesso em: 24 jul. 2021

imparcialidade e a objetividade em um segundo plano, enfatizando, no primeiro, o interesse empresarial por ganhos espetaculares prometidos pela economia do *big data*.[98]

II.5 – CORRELACIONAMENTO E PERFILAMENTO

Na Estatística, a correlação é a relação existente entre duas variáveis.[99] É uma técnica utilizada para resolução de problemas. Segundo Keneth Cukier e Viktor Mayer-Schönberger, as correlações nos ajudam a captar o presente e a prever o futuro.[100] Nesse sentido, a título de exemplo, a variável velocidade de automóveis em um determinado trecho de uma rodovia e a variável incidência de chuva podem ser correlacionadas para ajudar a resolver um problema de acidentes recorrentes.

Contudo, a correlação entre variáveis nem sempre implica em uma relação de causalidade, ou seja, de causa e efeito. Deste modo, no exemplo acima, o aumento das chuvas não necessariamente será a causa do aumento de acidentes em uma rodovia. As correlações que tentam estabelecer essa relação de causalidade sem qualquer fundamento estatístico são chamadas de *correlações espúrias*. Nesse sentido, não passa de mera coincidência o aumento de acidentes em uma rodovia e o aumento do índice de chuvas em uma região em que a rodovia não se encontra.

O *big data* intensificou a utilização da correlação. Cukier e Mayer-Schönberger afirmam que o motivo dessa intensificação, que deixou de lado a investigação pela causalidade, é que, em um contexto de grande volume de dados disponíveis, a correlação acaba sendo uma abordagem mais pragmática, pois não se preocupa com o porquê (causa), mas sim com o quê.[101] Os mesmos autores destacam a necessidade de cautela na utilização da correlação, pois à medida que a quantidade de dados aumenta em magnitude, também são encontradas mais correlações ilegítimas — fenômenos que parecem correlacionados, mas não estão.[102]

Como *softwares* capazes de determinar a probabilidade de ocorrência de um crime em determinado local já são realidade,[103] correlações ilegítimas constituem um sério problema a ser enfrentado no uso das TRFs, em especial quando utilizadas pela vigilância estatal. São vários os casos

---

98 O'NEIL. Op. cit., 2020. p. 7.
99 FARBER, Betsy. RON, Larson. *Estatística Aplicada*. Tradução: Luciane Ferreira Pauleti Vianna. 4ª Ed. São Paulo: Pearson Prentice Hall, 2010. p. 395.
100 MAYER-SCHÖNBERGER, Viktor. CUKIER, Keneth. *Big Data:* como extrair volume, variedade, velocidade e valor da avalanche de informação cotidiana. Tradução: Paulo Polzonoff Junior. 1. ed. Rio de Janeiro: Elsevier, 2013. p. 37.
101 Ibid. p. 36.
102 Ibid. p. 38.
103 Nos Estados Unidos o Clearview AI é um software de reconhecimento facial largamente utilizado por agências de polícias americanas. Na Inglaterra, a polícia britânica realizou testes com o *Most Serious Violence (MSV)*.

reportados de pessoas presas injustamente em decorrência de falhas em TRFs.[104] Como vimos, grupos sociais mais vulneráveis são os mais afetados por essas falhas, especialmente em países como os Estados Unidos e o Brasil, que adotam uma política de encarceramento em massa desses grupos, sobretudo da população negra.

Importante mencionar que nem sempre os sistemas preditivos recebem *inputs* de dados com potencial discriminatório (sensíveis), como os referentes à raça, etnia ou orientação sexual, por exemplo. Inclusive, há países, em que é proibido alimentar o sistema preditivo com essas informações justamente para evitar discriminação. Contudo, de acordo com Cathy O'Neil, mesmo que um algoritmo não enxergue a cor da pele, o resultado o faz,[105] o que é possível graças às correlações que os modelos matemáticos são capazes de realizar.

Para Tarcizio Silva, a exclusão de categorias consideradas sensíveis nas interfaces e nas bases de dados de treinamento são soluções ineficazes oferecidas pelos tecnologistas,[106] pois a discriminação pode ocorrer por meio de desvios e estratégias possíveis, como técnicas de engenharia social e técnicas algorítmicas.[107] Silva exemplifica que anúncios de serviços ligados à criminalização, como levantamento de fichas criminais ou remoção de fotos de prisão, são sistematicamente mais oferecidos para pessoas com nomes afro-americanos.[108]

Para Samuel Oliveira, a natureza antecipatória do policiamento preditivo significa que os indivíduos podem ser tratados de maneira diferente, não por causa do que fizeram, mas por causa de inferências baseadas em dados sobre o que poderiam fazer. Como resultado, esses tipos de sistemas podem reforçar práticas discriminatórias, replicando padrões em dados históricos.[109]

Há um risco discriminatório tanto em decorrência de correlações espúrias quanto de correlação legítima. Fujimoto et al. denominam este último tipo de discriminação decorrente de uma correlação legítima de discriminação por generalização injusta (correlação abusiva). Segundo os autores, embora o modelo matemático funcione bem e seja estatisticamente correto, leva a uma situação na qual algumas pessoas são equivocadamente classificadas em certos grupos.[110]

---

[104] ANOTHER Arrest, and Jail Time, Due to a Bad Facial Recognition Match. The New York Times. Disponível em: https://www.nytimes.com/2020/12/29/technology/facial-recognition-misidentify-jail.html. Acesso em: 13 ago. 2021.
[105] O'NEIL. Op. cit., 2016. p. 137.
[106] SILVA, Op. Cit. 2022. n.p.
[107] Ibid. n.p.
[108] As empresas se aproveitam do histórico de busca do usuário. Como é comum que usuários buscam o próprio nome, essa informação é coletada e posteriormente utilizada para publicidade direcionada. Ibid. n.p.
[109] OLIVEIRA. Op. cit., 2020. p. 78.
[110] FUJIMOTO e al. Op. cit., 2020. p. 430.

Na mesma direção, Maria Lindoso explica que, apesar de se tratar de uma quantidade incalculável de dados analisados dentro de uma base, justamente em razão do *big data*, ainda assim o algoritmo não possui acesso a todas as informações sobre determinado usuário. Desse modo, a correlação pode ser estatisticamente verdadeira para a realidade daquela base de dados, mas não necessariamente o será para a realidade daquele usuário.[111]

Ana Frazão ressalta que, mesmo quando o raciocínio estatístico é certo, na medida em que o julgamento a respeito de uma pessoa é feito a partir de critérios gerais que desconsideram a sua individualidade não deixa de representar uma espécie de discriminação. Nesse sentido, a autora aponta para a necessidade de se tomar cuidado com o emprego amplo e absoluto da estatística, sem que existam mecanismos ou válvulas de escape para a correção dos resultados.[112]

Em modelos matemáticos de previsão, uma grande variedade e volume de dados são correlacionados para desenhar verdadeiros perfis alternativos dos indivíduos. Dados correlacionados a partir de outros dados, aparentemente sem insignificância, são agrupados e categorizados para permitir uma série de inferências sobre as pessoas. Essa combinação de dados que resulta num perfil alternativo de um indivíduo é chamada de perfilamento (*profiling*).

Dinant et al. definem o perfilamento como um processo que envolve categorizar os indivíduos de acordo com suas características pessoais. Essas características podem ser imutáveis (como idade ou altura) ou mutáveis (como roupas, hábitos, preferências e outros elementos de comportamento). Segundo os mesmos autores, a criação de perfil inclui mineração de dados em que os indivíduos são categorizados com base em algumas de suas características observáveis, a fim de inferir, com uma certa margem de erro, outras que não são observáveis.[113]

Esses perfis podem ser criados inclusive a partir do correlacionamento de dados disponibilizados publicamente pelo indivíduo. O *Clearview Ai,* por exemplo, software de prevenção de crimes baseado em reconhecimento facial, utilizando por milhares de agências de polícia norte-americanas, tem suas bases de dados alimentadas com milhões de fotografias extraídas de usuários do *Facebook*.[114]

---

[111] LINDOSO. Op. cit., 2021. p. 144.

[112] FRAZÃO, Ana. *Fundamentos da proteção de dados pessoais*. Noções introdutórias para a compreensão da importância da Lei Geral de Proteção de Dados. In: TEMPEDINO, Gustavo, OLIVA, Milena. *Lei Geral de Proteção de Dados e duas repercussões no Direito brasileiro*. 2ª Edição. Thomson Reuters, Revista dos Tribunais, 2020. p. 34.

[113] Dinant, Lazaro, Lefever et. Al (2008), *Application of Convention 108 to the Profiling Mechanism* - Some ideas for the future work of the consultative committee (T-PD), Doc. T-PD 01, p. 3.

[114] Kashmir, Hill. *The Secretive Company That Might End Privacy as We Know It*. The New York Times, New York. 18 jan. 2020. Disponível em: https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html. Acesso em: 18 ago. 2021.

Pelo alto potencial discriminatório, o perfilamento traz riscos para uma série de direitos fundamentais, incluindo a privacidade e a proteção de dados. Especialmente pelo fato de que frequentemente esses perfis são utilizados com dados extraídos sem o conhecimento do usuário, servindo a finalidades muitas vezes ilegítimas.

II.6 – RECONHECIMENTO FACIAL E RACISMO

O racismo na tecnologia, segundo Cathy O'Neil, é alinhado por coleta irregular de dados e por correlações espúrias, reforçado por injustiças institucionais e contaminado por viés de confirmação. Daí a conclusão da autora de que o racismo é o mais desleixado dos modelos de previsão[115] que, como vimos no tópico II.4, não afetam somente os negros. Outros grupos como os asiáticos e os latinos também sofrem seus efeitos racistas,[116] indicando que a tecnologia pode revelar o preconceito estrutural que há em cada sociedade.

No Brasil, as altas taxas de feminicídio, de crimes de ódio contra LGBTQIA+ e negros, acendem um alerta para que se observe com cautela a implementação de tecnologias com potencial discriminatório, em especial pela segurança pública. Para Tarcizio Silva, a tecnologia de reconhecimento facial na segurança pública é utilizada como ferramenta de violência estatal, dentro de um histórico de ideação em que as próprias instituições policiais são instrumentos de segregação racial.[117]

Inclusive, a experiência relativamente recente do uso do reconhecimento facial na segurança pública em alguns estados brasileiros demonstra essa necessidade de cautela. Ao monitorar o reconhecimento facial em cinco estados brasileiros, a organização Rede de Observatório de Segurança verificou que mais de 90% eram negros.[118]

---

[115] O'NEIL. Op. cit. 2016. p. 37.
[116] ROSE, Adam. Are Face-Detection Cameras Racist?. Time, 22 jan. 2010. Disponível em: http://content.time.com/time/business/article/0,8599,1954643,00.html. Acesso em: 18 ago. 2021.
[117] SILVA, Op. cit. 2022. n.p.
[118] NUNES, Pablo. *Exclusivo: levantamento revela que 90,5% dos presos por monitoramento facial no Brasil são negros*. The Intercept Brasil. 21 nov. 2019. Disponível em: https://theintercept.com/2019/11/21/presos-monitoramento-facial-brasil-negros/. Acesso em: 19 ago. 2021.

O levantamento da Rede de Observatório de Segurança confronta a ideia de democracia racial no Brasil,[119] que mesmo após amplamente rechaçada,[120] até hoje encontra vozes em sua defesa.[121] Ao criticar a ideia de democracia racial, Abdias Nascimento relembrou o seguinte trecho de matéria jornalística publicada em 14 de junho de 1959 pelo O Jornal, do Rio de Janeiro, 10 anos após a promulgação da Lei Afonso Arinos (Lei nº 1.390), a primeira norma contra o racismo do Brasil:[122]

> Candidato de côr, mesmo com habilitação para o comércio, escritório, cinemas, consultórios, portarias, bares, hospitais, firmas, estrangeiras e outros estabelecimentos que exigem pessoas de "boa aparência, não conseguem trabalho". Por ordem é o preconceito de cor que se encontra em primeiro lugar, em seguida vem a idade, e, finalmente, a nacionalidade. PRECONCEITO racial como o maior fator de desemprego. O JORNAL, Rio de Janeiro, 14 de junho de 1959. Segunda Seção. p 9.[123]

O trecho destacado supra revela o quanto o Brasil é um país historicamente marcado pelo preconceito. Todavia, desde o início de sua história, o preconceito com os negros sempre teve raízes mais profundas na sociedade brasileira. Não por outra razão, vestígios da escravidão ainda são frequentemente encontrados em nossa estrutura social. Além de menos acesso material a direitos fundamentais e baixa representatividade nas instituições, destaca-se ainda um sistema penal que não disfarça que tem seu principal enfoque no aprisionamento dos negros.

Essas características são essenciais para o estudo dos possíveis riscos e impactos das TRFs no Brasil, pois como abordando anteriormente, a falta de representatividade na produção tecnológica e nos dados é um fator determinante para a ocorrência de discriminação. Como a construção dessas tecnologias não é democrática, muitas pessoas são afetadas e, da mesma forma que machismo,

---

[119] Segundo MUNANGA (2010), a democracia racial, ideia de que não existe racismo no Brasil, é na verdade um mito e decorre da dificuldade de o brasileiro não admitir que é racista, sendo racista apenas os outros, americanos e sul-africanos brancos. MUNANGA, Kabengele. *Teoria social e relações raciais no Brasil contemporâneo*. Cadernos Penesb, Niterói, n. 12, 2010. p. 169-203. Disponível em: https://www.mprj.mp.br/documents/20184/172682/teoria_social_relacoes_sociais_brasil_contemporaneo.pdf. Acesso em: 23 ago. 2021.

[120] MILENA, Lilian. *Kabengele Munanga, o antropólogo que desmistificou a democracia racial no Brasil*. Carta Maior, 15 maio 2019. Disponível em: https://www.cartamaior.com.br/?/Editoria/DireitosHumanos/Kabengele-Munanga-o-antropologo-quedesmistificou-a-democracia-racial-no-Brasil/5/44091. Acesso em: 23 ago. 2021.

[121] MAZUI, Guilherme. *"No Brasil, não existe racismo", diz Mourão sobre assassinato de homem negro em supermercado*. Portal G1, 20 nov. 2020. Disponível em: https://g1.globo.com/politica/noticia/2020/11/20/mourao-lamenta-assassinato-de-homem-negro-em-mercado-mas-diz-que-no-brasil-nao-existe-racismo.ghtml. Acesso em: 23 ago. 2021.

[122] NASCIMENTO, Abdias. *O genocídio do negro brasileiro:* processo de um racismo mascarado. 1.ª ed. São Paulo: Perspectivas, 2016. p. 75.

[123] *PRECONCEITO racial como o maior fator de desemprego*. O Jornal, Rio de Janeiro, 14 jun. 1959. Segunda Seção. p. 9. Disponível em: http://memoria.bn.br/DocReader/110523_05/76038. Acesso em: 22 de ago. 2021

homofobia e racismo, não apenas os membros de suas respectivas comunidades são impactados, mas também a sociedade como um todo.

Frente ao mau uso das TRFs, podemos verificar dois tipos de riscos ao exercício de liberdades individuais e garantias fundamentais. O primeiro é um risco geral, que afeta a todos e decorre do simples uso das TRFs. É um risco geral, pois direitos fundamentais como a dignidade da pessoa humana, liberdade, privacidade e proteção de dados estão ameaçados em algum grau para todos. O segundo é um risco específico, pois incide primordialmente sobre grupos mais vulneráveis, em razão do preconceito e discriminação institucionalizados, e decorre, em parte, da falta de representatividade.

A concretização desses riscos gera várias formas de violência, singularmente contra os negros. Ao analisar o racismo algorítmico *online*, Tarcizio Silva traz uma série de exemplos de situações em que o reconhecimento facial, como componente de uma estrutura técnico-algorítmica, é responsável por facilitar manifestações de racismo.[124]

A análise de Silva vem a partir do conceito de microagressões raciais,[125] classificadas em 1) **microinsultos** (grifei): a) hipersexualiação de mulheres e crianças negras por motores de busca como resultado de buscas não pornográficas; b) embranquecimento por aplicativos de "*embelezamento*" ou "envelhecimento"; e c) associação de categorias negativas a pessoas negras, a partir da análise facial; e em 2) **microinvalidações** (grifei): a) não detecção de pessoas negras por sistemas de reconhecimento facial; b) incorreta etiquetagem de mulheres negras; e c) não exibição de pessoas negras por mecanismos de buscas quando há inclusão de qualificador racial.[126]

Silva explica que, enquanto os microinsultos [...] transmitem grosseria, insensibilidade e rebaixaram a herança racial ou identidade de uma pessoa, as microinvalidações são afirmações verbais que negam, anulam ou minam as realidades dos membros de grupos-alvo.[127] O autor esclarece ainda que "*micro*" não se refere ao grau de violência, mas sim à pervasividade e ao fato de que a "agressão" incide em um nível individual e/ou local ou mesmo em situações privadas ou limitadas[...].[128]

---

[124] SILVA, Op. cit. 2022, n.p.
[125] Segundo SILVA (2019, p5), microagressões raciais são mensagens rotineiras que comunicam insultos e desprezo racial e podem ser apresentadas de forma verbal, comportamental ou ambientalmente contra grupos racializados. SILVA, Tarcizio. *Racismo Algorítmico em Plataformas Digitais*: microagressões e discriminação em código. Disponível em: https://lavits.org/wp-content/uploads/2019/12/Silva-2019-LAVITSS.pdf. Acesso em: 10 mar. 2022. p. 5.
[126] SILVA, 2022, n.p. apud TYNES, 2019, p. 195. Ver Figura 1 e Tabela 1.
[127] SILVA, Op. cit. 2022, n.p.
[128] Ibid. n.p.

II.7 – OPACIDADE E PRIVACIDADE

Samuel Oliveira registra que a vigilância, notadamente a vigilância operada mediante o reconhecimento facial, é também uma forma abrangente de poder investigatório. Ela se estende para além das meras buscas, pois registra comportamentos, interações sociais e potencialmente tudo o que uma pessoa faz.[129] Daí se compreende por que a privacidade ganha cada vez mais evidência no debate social, especialmente em uma sociedade movida a dados. As TRFs se incluem com destaque nesse debate pelo fato de que possuem a capacidade de coletar e tratar dados pessoais sensíveis[130] à distância e sem o consentimento dos indivíduos.

Oliveira também observa que o problema ocorre quando a vigilância é empregada de maneira excessiva ou desproporcional, gerando um estado de monitoramento contínuo. O excesso de controle, no entanto, é claramente nocivo e incabível em uma democracia.[131] Contudo, demandas progressivas por mais segurança forçam a adoção dessas tecnologias de vigilância e, consequentemente, trazem desafios de se equilibrar os interesses envolvidos nesse processo, qual sejam, mais privacidade e mais segurança. Sobre o tema, Ana Frazão afirma que a economia movida a dados e o capitalismo de vigilância são as duas faces da mesma moeda pois, quanto maior a importância dos dados, mais incentivos haverá para o aumento da vigilância e, por conseguinte, maior será a coleta de dados.[132]

A opacidade característica desses modelos matemáticos é um ponto central no debate sobre o equilíbrio entre segurança e privacidade, haja vista que o questionamento das decisões automatizadas sentenciadas pelas tecnologias de vigilância esbarra na falta de transparência sobre suas estruturas, seus parâmetros internos e critérios utilizados para tomada de decisão. Não obstante, essas tecnologias são desenvolvidas com base em linguagens altamente sofisticadas e acessíveis a um grupo muito seleto: programadores.

Portanto, o problema não necessariamente está no uso das TRFs, mas sim no fato de que os indivíduos afetados encontram problemas para compreender os mecanismos escondidos por traz dos códigos que as compõem. Daí a afirmação de Cathy O'Neil de que os programadores são altos sacerdotes e os seus algoritmos, deuses.[133] Para Danielle Citron, a opacidade dos sistemas

---

[129] OLIVEIRA, Samuel. Op. cit.,2021. p. 108-109

[130] Segundo a LGPD, art. 5º, II, são dados sensíveis os dados pessoais sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural.

[131] OLIVEIRA. Op. cit.,2021 apud RODOTÀ, 2011., p. 109.

[132] FRAZÃO, Ana. Op. cit., 2020. p. 28.

[133] O'NEIL. Op. cit., 2016. p. 8.

automatizados os protege do escrutínio. Desse modo, os cidadãos não podem ver ou debater sobre suas regras. Por sua vez, a transparência, a precisão e a responsabilidade política da regulamentação administrativa são perdidas.[134]

É importante refletir sobre para quem interessa a opacidade por traz dos algoritmos. Afinal, em linhas gerais, os programadores agem em nome de agentes públicos ou privados. No decorrer deste trabalho, temos visto o quanto o Estado e grandes companhias vem se empenhando para manipular dados e concentrar informações sobre os indivíduos a fim de atender a seus interesses.

As normativas sobre proteção de dados podem oferecer um caminho para proteção dos indivíduos ao estabelecer direito de oposição e mecanismos de auditoria e revisão das decisões automatizadas. A Lei Geral de Proteção de Dados – LGPD (Lei nº 13.709/2018), por exemplo, elenca no seu art. 20 o direito de o titular de dados pessoais solicitar a revisão de decisões automatizadas, devendo o controlador fornecer, sempre que solicitadas, informações claras e adequadas a respeito dos critérios e dos procedimentos utilizados para a decisão automatizada, observados os segredos comercial e industrial. Mister destacar que, especificamente no caso brasileiro, a LGPD não se aplica no âmbito da segurança pública, setor que mais emprega as TRFs.[135] Este vácuo regulatório aumenta a desconfiança sobre a implementação e uso dessas tecnologias.

Fabiano Hartmann entende que resultados produzidos pela Inteligência Artificial marcados pela opacidade são parte do risco genérico relacionados a essas tecnologias. Para o autor, todos esses riscos são controláveis em um sistema de IA robusto (eticamente estruturado). Além disso, conclui o autor, a Inteligência Artificial é conceitualmente a reprodução de padrões humanos e, portanto, o próprio comportamento humano também possui esses riscos, contudo o resultado da atividade cognitiva artificial pode ser mais facilmente corrigido que os desvios e preconceitos do próprio ser humano.[136]

---

[134] CITRON, Danielle Keats. *Technological Due Process*. Washington University Law Review. nº. 1249. Volume 85, 2008. Disponível em: https://openscholarship.wustl.edu/law_lawreview/vol85/iss6/2. Acesso em: 29 out. 2021.
[135] O art. 4º da LGPD define hipóteses em que a Lei não se aplica.
[136] HARTMAN PEIXOTO, Fabiano. Op. cit., 2020. p.28.

CAPÍTULO III – REGULAÇÃO DAS TECNOLOGIAS DE RECONHECIMENTO FACIAL

III.1 – RESPOSTAS AO RECONHECIMENTO FACIAL: BANIMENTO, MORATÓRIA E REGULAÇÃO

Jacob R. Lilly lembra que em grandes momentos críticos da história americana houve tensão entre privacidade e segurança.[137] Daniel Solove aponta marcos importantes já no começo do século XX como a criação do FBI, por exemplo. Nos anos 40 e 50, houve a intensificação por meio da criação de novas agências de inteligência impulsionada por políticas de combate ao Comunismo, com a justificativa de proteção da segurança nacional. Por fim, o emblemático caso do *USA Patriot Act*, em decorrência dos atentados de 11 de setembro de 2001, ampliando consideravelmente o poder de vigilância do Estado americano, que se engajava em programas clandestinos de coleta de informações.[138]

Aliás, Shoshana Zuboff observa que grandes companhias privadas também se beneficiaram do histórico atentado de 11 de setembro enquanto o aparato de segurança nacional americana estava disposto a alimentar, imitar, proteger e se apropriar das emergentes capacidades do capitalismo de vigilância.[139] Jacob R. Lilly afirma que, em cada um desses momentos críticos, recorreu-se ao sistema legal para responder até que ponto uma sociedade democrática pode violar os próprios direitos em que foi fundada para garantir sua sobrevivência.[140]

Por muito tempo a privacidade vinha sendo deixada de lado,[141] mas com o aumento da preocupação com a privacidade conduzido pelas normativas de proteção de dados pessoais mundo afora, despontaram movimentos organizados pela sociedade civil visando responder o progressivo emprego do reconhecimento facial por meio da reivindicação de regulação adequada, moratória do seu uso ou até mesmo seu banimento completo.

A moratória compreende a suspensão do uso do reconhecimento facial por um determinado período e em determinado contexto a fim de propiciar aos reguladores tempo para que encontrem maneiras de evitar abusos com o uso dessas tecnologias. Nesta linha seguiu o Conselho de Direitos

---

[137] LILLY, Jacob R. *Nation Security at What Price? A Look into Civil Liberty Concerns in the Information Age under the USA Patriot Act* In: *Information ethics: privacy, property, and power*. Edited by Adam D. Moore. 1. ed. Seattle and London: University of Washington Press, 2005. p. 416.
[138] SOLOVE, Daniel J. *Nothing to Hide: the false tradeoff between privacy and security*. Yale University Press Book, 2011. pp. 5-12.
[139] ZUBOFF, Shoshana. Op. Cit., 2021. p.20.
[140] LILLY, Jacob R. Op. cit., 2005. p. 417.
[141] OLIVEIRA, Samuel. Op. cit., 2021. p. 130.

Humanos da ONU que, em 2020, recomendou que os países estabelecessem uma moratória sobre o uso de tecnologia de reconhecimento facial no contexto de assembleias pacíficas, pelo menos, até que as autoridades responsáveis pudessem demonstrar conformidade com os padrões de privacidade e proteção de dados, bem como a ausência de problemas de precisão significativos e impactos discriminatórios.[142]

Após as recomendações da ONU, de protestos desencadeados pelo *Black Lives Matter* em 2020, e ainda, com a pressão de entidades de defesa da privacidade, *big techs* desenvolvedoras de produtos com reconhecimento facial sinalizaram apoio ao movimento da moratória, anunciando a suspensão da venda desse tipo de tecnologia para forças de segurança com intuito de forçar uma demanda por regulamentação. Enquanto a *Microsoft*, *Google* e *Amazon* anunciaram a suspensão da comercialização com governos,[143] a *IBM* foi além, anunciando que não mais desenvolveria esse tipo de tecnologia.[144]

Para Malkia Devich-Cyril, os reais interesses dessas companhias podem estar mais associados ao risco financeiro e à imagem pública do que propriamente com as vidas negras.[145] Contudo, muito embora se questione os reais interesses dessas companhias, uma sinalização ao movimento pela moratória pode ser positiva para pressionar os legisladores na elaboração de normas regulamentadoras.

Especialmente nos Estados Unidos, onde o emprego de TRFs é mais intensificado, movimentos pela moratória obtiveram alguns resultados: a *The Facial Recognition and Biometric Technology Moratorium Act*, iniciativa mais abrangente, com vistas a proibir o uso de reconhecimento facial pelo governo federal americano, até que haja uma regulamentação específica;[146] e a proposta A6787D, que alterou a Lei educacional do Estado de Nova Iorque para proibir o uso nas escolas do estado até julho

---

142 UNITED NATIONS. *Impact of new technologies on the promotion and protection of human rights in the context of assemblies, including peaceful protests*: Report of the United Nations High Commissioner for Human Rights. United Nations, 24 jun. 2020. p. 15. Disponível em: https://undocs.org/A/HRC/44/24. Acesso em: 30 set. 2021.

143 GREENE, Jay. *Microsoft won't sell police its facial-recognition technology, following similar moves by Amazon and IBM*. Washington Post, 11 jun. 2020. Disponível em: https://www.washingtonpost.com/technology/2020/06/11/microsoft-facial-recognition. Acesso em: 30 set. 2021.

144 HEILWEIL, Rebecca. *Why it matters that IBM is getting out of the facial recognition business*. Vox, 10 jun. 2020. Disponível em: https://www.vox.com/recode/2020/6/10/21285658/ibm-facial-recognition-technology-bias-business. Acesso em: 30 set. 2021.

145 Segundo a ativista de direitos digitais Malkia Devich-Cyril as empresas que estão decidindo não vender tecnologias baseadas em reconhecimento facial, à medida que um poderoso movimento de protesto ganha força, podem ser motivadas mais por um cálculo cuidadoso dos riscos financeiros e de relações públicas do que pela preocupação com a vida dos negros (tradução nossa). Ver mais em: DEVICH-CYRIL, Malkia. *Defund Facial Recognition*. The Atlantic, 5 jun. 2020. Disponível em: https://www.theatlantic.com/technology/archive/2020/07/defund-facial-recognition/613771/. Acesso em: 30 set. 2021.

146 MARKLEY *lead colleagues on legislation to ban government use of facial recognition, other biometric technology*. Markey, 15 jun. 2021. Disponível em: https://www.markey.senate.gov/news/press-releases/senators-markey-merkley-lead-colleagues-on-legislation-to-ban-government-use-of-facial-recognition-other-biometric-technology. Acesso em: 4 out. 2021.

de 2022.[147] Outras iniciativas mais locais também ocorreram em outros estados americanos, como a moratória do uso das TRFs pela segurança pública da Califórnia até 2023; [148] e a moratória aprovada pela cidade de *Springfield*, no estado de *Oregon*, para suspensão do uso de TRFs pelo governo local.[149]

Na China, o uso de TRFs é ainda mais intenso que nos EUA, sendo difícil evitar ser filmado por câmeras com reconhecimento facial, pois o país asiático utiliza largamente a tecnologia para controlar a população.[150] Além disso, o país é grande concorrente do EUA no desenvolvimento de tecnologias de reconhecimento facial, muito em decorrência da prioridade do governo de chinês em se tornar líder mundial em Inteligência Artificial.[151] Todavia, apesar da preocupação geral dos cidadãos chineses, o governo sinalizou abertura para discutir o uso apenas pelo setor privado.[152] Grandes companhias chinesas, como a *SenseTime Group* e a *Ant Financial*, braço financeiro da *Ali Baba Group*, também se organizaram para apresentar uma resposta às preocupações com o uso das TRFs.[153]

Na contramão dos movimentos pela moratória, os movimentos pelo banimento advogam pela completa proibição das TRFs. Esses movimentos argumentam que suas ameaças superam os potenciais benefícios, pois seria invasiva, vulnerável e perigosa. Há quem defenda que esses sistemas sequer possam ser desenvolvidos, implementados (mesmo a título experimental) ou utilizados por entidades públicas ou privadas, com a justificativa de que são suscetíveis de conduzir a uma violação desnecessária ou desproporcional dos direitos fundamentais dos indivíduos.[154]

Para a organização americana *Ban Facial Recognition*, a regulação não seria suficiente, pois o reconhecimento facial além de injusto, não seria confiável, representando uma ameaça aos direitos

---

147 Projeto de lei acessível em: https://www.nysenate.gov/legislation/bills/2019/a6787. Acesso em: 4 out. 2021.

148 GUARIGLIA, Mathew. *Victory! California Governor Signs A.B. 1215*. Eletronic Frontier Foundation, 9 out. 2019. Disponível em: https://www.eff.org/deeplinks/2019/10/victory-california-governor-signs-ab-1215. Acesso em: 4 out. 2021.

149 COTE, Jackson. *Springfield City Council passes facial recognition moratorium*. Masslive, 25 fev. 2020. Disponível em: https://www.masslive.com/springfield/2020/02/springfield-city-council-passes-facial-recognition-moratorium.html. Acesso em: 4 out. 2021.

150 NG, Alfred. *How China uses facial recognition to control human behavior*. Cnet, 11 ago. 2020. Disponível em: https://www.cnet.com/news/in-china-facial-recognition-public-shaming-and-control-go-hand-in-hand/. Acesso em: 4 out. 2021.

151 SIMONITE, Tom. *Behind the Rise of China's Facial-Recognition Giants*. Wired, 8 mar. 2019. Disponível em: https://www.wired.com/story/behind-rise-chinas-facial-recognition-giants. Acesso em: 4 out. 2021.

152 SHEAD, Sam. *Chinese residents worry about rise of facial recognition*. BBC, 5 dez. 2019. Disponível em: https://www.bbc.com/news/technology-50674909. Acesso em: 4 out. 2021.

153 A iniciativa das companhias chinesas são voltadas para a autorregulação visando o estabelecimento de algumas diretrizes mínimas para o setor. Ver mais em: SHENZHEN, Chai Hua in. *Nation to set up standard for facial recognition technology*. China Daily, 11 dez. 2019. Disponível em: https://global.chinadaily.com.cn/a/201912/11/WS5df043b6a310cf3e3557d50c.html. Acesso em: 04 out. 2021.

154 ECI nº (2021) 000001. *Initiative de la société civile en vue d'une interdiction des pratiques de surveillance biométrique de masse*. SITE OFICIAL DA UNIÃO EUROPEIA, 1 de jul. 2021. Disponível em: https://europa.eu/citizens-initiative/initiatives/details/2021/000001_fr. Acesso em: 4 out. 2021.

básicos e à segurança dos indivíduos. Nesta direção, algumas cidades americanas, como São Francisco, *Oakland*, *Berkeley* e *Somerville*, optaram pelo banimento total do reconhecimento facial.[155] Movimentos no mesmo sentido também são encontrados na Europa e na América Latina, como o *Claim Your Face* e o *Derechos Digitales*, respectivamente.

Na Europa, os movimentos pelo banimento ganharam ainda mais força com o parecer conjunto nº 5/2021 emitido pelo Comitê Europeu para a Proteção de Dados (EDPB) e pela Autoridade Europeia de Proteção de Dados (EDPS). No referido parecer, as entidades propuseram o banimento de qualquer utilização de IA para o reconhecimento automatizado de características humanas em espaços acessíveis ao público, em qualquer contexto, tendo em consideração os riscos extremamente elevados representados pelo reconhecimento facial nesses espaços.[156]

De modo geral, tanto moratória quanto banimento se alinham com o princípio da precaução. Na proteção de dados, o princípio da precaução entra em ação nas situações em que as necessidades e os uso de dados pessoais não estão claros.[157] Em linhas gerais, esse princípio gira em torno da ideia de que, diante do grau de incertezas e de poucas evidências, um determinado proponente tome medidas de precaução para evitar riscos ou, até mesmo, que seja proibida a atividade potencialmente arriscada até que seja possível demonstrar que ela não ofereça risco ou que o risco oferecido seja aceitável.

Aliás, Bruno Bioni e Maria Luciano refletem sobre a aplicação do princípio da precaução na regulação da inteligência artificial a partir da LGPD. Para os autores, as leis gerais de proteção de dados pessoais, leis setoriais de dados biométricos e de reconhecimento facial apresentam um ferramental precaucionário a ser analisado.[158]

Pela regulação destacam-se iniciativas encabeçadas pelas próprias *big techs*. Enquanto anunciam moratórias na comercialização de produtos baseados em reconhecimento facial, as *big techs* tentam forçar os governos a aprovarem normas regulatórias. Para Sebastian Herrera, esse impulso por novas regulações vindo de *big techs* decorre, em parte, por uma sensação de que a regulação para o setor é

---

155 Ver mais em: BAN FACIAL RECOGNTION. *Ban Facial Recognition*. Ban Facial Recognition. Disponível em: https://www.banfacialrecognition.com. Acesso em: 4 out. 2021.

156 *Parecer conjunto nº 05/2021 do EDPB e EDPS*, p.2. Disponível em: https://edpb.europa.eu/system/files/2021-06/edpb-edps_joint_opinion_ai_regulation_en.pdf. Acesso em: 4 out. 2021.

157 BRASIL. *Guia de boas práticas*. Lei Geral de Proteção de Dados (LGPD). Comitê Central de Governança de Dados, 16 jun. 2021. Disponível em: https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/guias/guia_lgpd.pdf. Acesso em: 18 jan. 2021. p.54.

158 BIONI, Bruno Ricardo; LUCIANO, Maria. *O princípio da precaução na Regulação de Inteligência artificial:* seriam as lei de proteção de dados o seu pontal de entrada? In: FRAZÃO, Ana; MULHOLLAND, Catlin (Org). *Inteligência Artificial e direito*: ética, regulação e responsabilidade. São Paulo: Thomson Reuters Brasil, 2019, p.22.

inevitável. Logo, conduzir iniciativas regulatórias significa tentar garantir que seus interesses sejam levados em consideração.

Essas companhias gastam enormes quantias para influenciar os legisladores a moldar as leis a seu favor. Nesse sentido, Herrera também destaca como os esforços dessas grandes companhias por regulação do setor, seja para se opor ou atenuar as propostas existentes, pode ser diferente do discurso público,[159] que é mais harmonizado com o das entidades de proteção de direitos digitais.

Aliás, Ana Frazão observa que a assimetria informacional e os benefícios das inovações geram um cenário que possibilitou com que vários desses negócios evoluíssem em um ambiente no qual o suposto vácuo regulatório fosse convenientemente preenchido pela autorregulação criada pelos agentes em seu próprio benefício, muitas vezes em razão do regulador não saber como fazer para proteger minimamente o cidadão.[160]

Em outra perspectiva, a compreensão do movimento das *big techs* no debate político em torno da regulação do reconhecimento facial pode estar na afirmação de Fabiano Hartmann de que a Inteligência Artificial[161] tem desafios no plano ético e social, mas também tem repercussões econômicas concretas. Além disso, Hartmann aponta que as pesquisas em IA são estratégicas e movimentam três espaços: governo, academia e indústria.[162] Por isso, entidades com uma forte ligação com a economia tem se preocupado com questões comportamentais e éticas.

No Brasil, a discussão sobre banimento e moratória é muito incipiente. Rafael Zanatta et. al, observa que, ainda não há no país um movimento pelo banimento do reconhecimento facial, nem por uma moratória.[163] Recentemente, ativistas e associações civis brasileiras se juntaram a centenas de outras associações internacionais para assinar a *Carta aberta para banimento global de usos de reconhecimento facial e outros reconhecimentos biométricos remotos que permitam vigilância em massa, discriminatória e enviesada*, iniciativa liderada pela *Access Now*, organização internacional de defesa de direitos digitais.[164]

---

[159] HERRERA, Sebastian. *Tech Giants' New Appeal to Governments:* Please Regulate Us. Wall Street Journal, 27 jan. 2020. Disponível em: https://www.wsj.com/articles/tech-giants-new-appeal-to-governments-please-regulate-us-11580126502. Acesso em: 7 out. 2021.

[160] FRAZÃO, Ana. Op. cit., 2021. p. 31.

[161] É preciso relembrar que o reconhecimento facial surgiu como uma área da inteligência artificial.

[162] HARTMANN, FABIANO. *Inteligência artificial e direito:* convergência ética e estratégica. 1ª ed. Curitiba: Alteridade Editora, 2020. p. 192.

[163] FAVARO, Iasmine. VERGILI, Gabriela. RIELLI, Mariana. ZANATTA., Rafael et. al. *Banimento, moratória, regulação: os movimentos em torno do reconhecimento facial*. Observatorioprivacidade – Dataprivacy Brasil, 6 fev. 2020. Disponível em: https://www.observatorioprivacidade.com.br/2020/02/06/banimento-moratoria-regulacao-os-movimentos-em-torno-do-reconhecimento-facial. Acesso em: 4 out. 2021.

[164] ACCESS NOW. *Ban Biometric Surveillance*. Access Now, 7 jun. 2021. Disponível em: https://www.accessnow.org/ban-biometric-surveillance. Acesso em: 4 out. 2021.

A participação brasileira em movimentos internacionais aponta para a falta de um protagonismo próprio em torno das problemáticas envolvendo o reconhecimento facial[165] e reforça a observação de Rafael Zanatta et. al. Apesar da pouca aderência brasileira a movimentos pela moratória ou banimento das TRFs, já existem diversos projetos de lei tratando sobre o tema, os quais veremos adiante com mais detalhes.

III.2 – CENÁRIO REGULATÓRIO NO BRASIL

Como já abordado no tópico II.1, o reconhecimento facial surgiu como um subcampo da inteligência artificial. Aliás, no mesmo tópico, destacou-se que os avanços nas pesquisas em Inteligência Artificial foram fundamentais ao aprimoramento das TRFs. Essas observações se fazem importantes para uma melhor compreensão das possibilidades inseridas do contexto regulatório que tem se formando em torno dessas tecnologias. Nessa perspectiva, é possível tanto uma regulação específica para as TRFs, em decorrência de suas particularidades e de riscos relacionados ao seu uso, quanto um marco regulatório para toda a Inteligência Artificial, o que poderia incluir disposições sobre parâmetros mínimos normativos para o reconhecimento facial.

Nesse último sentido, caminhou o Projeto de Lei nº 1.969/2021, que dispunha sobre os princípios, direitos e obrigações na utilização de sistemas de inteligência artificial.[166] O seu art. 2º, II, define um sistema de IA como um software desenvolvido com capacidade de, em vista de objetivos determinados por pessoa natural, gerar conteúdos, previsões, recomendações ou decisões que influenciam o ambiente em que interage.

A definição de IA proposta pelo PL nº 1.969/21 traz características muito comuns em sistemas de reconhecimento facial, especialmente aquelas voltados para policiamento preditivo. O referido projeto também tratou do reconhecimento facial ao definir um sistema de reconhecimento de emoções, segundo o qual consistiria em um sistema de IA que identifica ou infere emoções e intenções da pessoa natural com base em dados biométricos.

---

[165] Com o aumento da discussão em âmbito nacional algumas iniciativas importantes têm surgido mais recentemente, como foi o caso da ofensiva liderada pelo IDEC com o apoio de mais 26 entidades contra o PL 865/2019 que visava determinar a instalação de reconhecimento facial no metrô de São Paulo. Apesar da ofensiva o projeto foi aprovado em regime de urgência pela Câmara Legislativa de São Paulo, mas foi vetado totalmente pelo Governador sob a fundamentação de o projeto interferia indevidamente nas competências das empresas que administram o sistema de transporte de passageiros por trilhos em São Paulo. Nada sobre possível ameaça à privacidade foi levado em consideração no veto.

[166] PL nº 1.969/2021 proposto pelo dep. Gustavo Fruet – PDT/PR. Disponível em: https://www.camacra.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2284814. Acesso em: 7 out. 2021.

Por fim, na exposição de motivos, o legislador tratou de esclarecer que um dos objetivos do Projeto de Lei seria impedir que, sob o pretexto de garantir a segurança pública à população, o Estado simplesmente promova a disseminação de câmeras de reconhecimento facial ou de sistemas que tratem dados biométricos em espaços públicos de forma abusiva. O projeto foi arquivado.

Outro projeto que merece destaque é o Projeto de Lei nº 21/2020, cuja pretensão é de se instituir um marco legal do desenvolvimento e uso da Inteligência Artificial pelo poder público, empresas, entidades diversas e pessoas físicas. O projeto estabelece diversos direitos, obrigações, princípios bem como instrumentos de governança. O PL teve forte envolvimento do Governo, por meio do Ministério da Economia, visando garantir, de alguma maneira, uma legislação livre de barreiras regulatórias que prejudicam a competitividade.[167] Segundo o próprio Ministério da Economia, a proposta da Secretaria Especial de Produtividade e Competitividade (SEPEC) para o projeto é o limite da regulação, para que o setor de IA seja regulado sem excessos.[168] O projeto foi aprovado na Câmara e está pendente de votação no Senado.

O PL nº 21/2020 recebeu algumas críticas da sociedade civil. O Laboratório de Políticas e Internet (LAPIN) demonstrou preocupações com o projeto. Em nota técnica, o LAPIN destacou a necessidade de ampliar o debate sobre o PL substitutivo com os diversos atores da sociedade brasileira, considerando o grau de complexidade e o impacto da IA.[169] Para alguns pesquisadores e especialistas da área, a comunidade não foi consultada sobre o projeto.[170]

Com relação ao texto, o Instituto de Referência em Internet e Sociedade (IRIS) enfatizou que há diversas lacunas, pontos genéricos e falta de embasamento técnico.[171] Nesse sentido, o LAPIN também observou que a inteligência artificial é classificada tanto como uma disciplina científica quanto

---

[167] A intervenção do governo no processo legislativo da regulação a IA segue a linha da denominada Estratégia Brasileira de Inteligência Artificial – EBIA que elencou como um de seus objetivos a remoção de barreiras para a inovação em IA. O documento, publicado em junho de 2021 pode ser acessado no portal do Ministério da Ciência e Tecnologia disponível em: https://www.gov.br/mcti/pt-br/acompanhe-o-mcti/transformacaodigital/arquivosinteligenciaartificial/ia_estrategia_documento_referencia_4-979_2021.pdf. Acesso em: 7 out. 2021.

[168] BRASIL. *Projeto de Lei sobre uso de Inteligência Artificial avança no Congresso*. Ministério da Economia, 29 set. 2021. Disponível em: https://www.gov.br/economia/pt-br/assuntos/noticias/2021/setembro/projeto-de-lei-sobre-uso-de-inteligencia-artificial-avanca-no-congresso. Acesso em: 7 out. 2021.

[169] LABORATÓRIO DE POLÍTICAS PÚBLICAS E INTERNET. *Nota Técnica Substitutivo ao PL 21/2020*. LAPIN, 28 de set. de 2021. Disponível em: http://lapin.org.br/2021/09/28/nota-tecnica-pl-21-2020/. Acesso em: 12 out. 2021.

[170] PROJETO *de marco legal da IA no Brasil é pouco consistente e pode ser inútil, dizem especialistas*. Jornal Unesp, 29 de jul. de 2021. Disponível em: https://jornal.unesp.br/2021/07/29/projeto-de-marco-legal-da-ia-no-brasil-e-pouco-consistente-e-pode-ser-inutil-dizem-especialistas/. Acesso em: 12 out. 2021.

[171] INSTITUTO DE REFERÊNCIA EM INTERNET E SOCIEDADE. *Inteligência Artificial no Brasil: a Estratégia Brasileira de Inteligência Artificial (EBIA) e o Projeto de Lei nº 21/2020*. IRISBH, 5 de out. de 2021. Disponível em: https://irisbh.com.br/inteligencia-artificial-no-brasil-a-estrategia-brasileira-de-inteligencia-artificial-ebia-e-o-projeto-de-lei-no-21-2020/. Acesso em: 12 out. 2021.

uma família de tecnologias, abarcando técnicas muito distintas, estando presente em aplicações diversas, incluindo sistemas de reconhecimento facial. Por essa multiplicidade que abarca a IA, o estabelecimento de direitos e deveres de ordem generalista, que se aplique indistintamente a qualquer um desses sistemas, pode se revelar precipitado sem o devido amadurecimento do debate.

Projetos de leis federais especificamente sobre reconhecimento facial foram propostos já a partir de 2014,[172] sendo grande parte deles no sentido de tornar obrigatório o uso dessas tecnologias em determinado contexto como: uso de biometria, incluindo facial, para emissão de documento de registro civil (PL nº 7.759/2014) e carteira nacional de habilitação (PL 7.692/2014); uso de reconhecimento facial em aeroportos (PL nª 5.699/2016); transportes coletivos (PL nº 9.414/2017 e PL nº 811/2020); transporte por motoristas de aplicativos (PL nº 329/2020 e PL nº 4.768/2020); e no sistema prisional (PL nº 3.627/2015, PL nº 9.054/2017, PL nº 9.736/2018 e PL nº 4.827/2019).

Muito focados em segurança, esses projetos deixam de lado a privacidade nas suas justificativas e não apresentam detalhamento do risco para a sociedade no uso das TRFs. Neste sentido, destaque para o PL nº 4.413/2016, que visou tornar obrigatória a implantação de sistema de controle de frequência de alunos em escolas públicas. O registro de presença seria realizado por meio de um leitor de reconhecimento facial. O projeto não tinha qualquer indicação a respeito dos possíveis riscos envolvidos no tratamento das informações relacionadas a crianças e adolescentes, justificando a sua iniciativa por mais controle da evasão escolar e por mais segurança.

Fora do âmbito federal, são muitas as iniciativas regulatórias de TRFs, das quais importa destacar: o PL nº 865/2019, do Estado de São Paulo, sobre a instalação de TRF nas estações de Metrô e Trens de São Paulo; o PL nº 391/2019, de Minas Gerais, sobre o uso de TRFs em estádio de futebol; o PL nº 318/2019, do Rio de Janeiro, e o PL nº 148/2019, do Paraná, ambos sobre a obrigatoriedade de reconhecimento facial em locais e eventos públicos.

Em termos de legislação aprovada temos: a Lei nº 16.873/2019, do Ceará; a Lei nº 7.123/2015, do Rio de Janeiro; a Lei nº 21.737/2015, de Minas Gerais e a Lei nº 8.113/2019, de Alagoas, todas voltadas para o uso de TRFs em estádios de futebol. E, por fim, a Lei nº 6.712/2020 do Distrito Federal, que dispõe sobre o uso de tecnologia de reconhecimento facial na segurança pública do DF.

De modo geral, esses projetos têm em comum o fato de se voltarem para um contexto específico, como uso em escolas e estádios de futebol, por exemplo. Além disso, não se verifica a busca

[172] Os projetos de lei nº 3372/2004 e 1230/2007 versavam sobre acesso a informações constantes em bancos de dados da Administração Pública Federal e sugeriam a adoção de medidas de segurança baseadas em biometria (voz, digitais ou reconhecimento facial) para acesso aos bancos de dados a fim de prover mais segurança.

por um equilíbrio entre interesses entre privacidade e segurança, falhando em propor mecanismos de defesa aos indivíduos afetados por essas tecnologias. Ademais, falham com relação ao diálogo com outras normas importantes, como a Lei nº 8.078/1990 (Código de Defesa do Consumidor - CDC) e a recente Lei nº13.709/2018 (Lei Geral de Proteção de Dados - LGPD).

A falta de uma regulação nacional gera um vácuo regulatório enquanto algumas legislações de caráter estadual intentam tornar obrigatório o uso de TRFs em diversos contextos e sem o correto debate sobre os riscos para direitos fundamentais. Rafael Zanatta et. al. nos lembra que enquanto não surge uma regulação específica para a matéria, o Brasil possui um marco robusto de proteção aos direitos fundamentais, inclusive a privacidade, e que a LGPD, também traz elementos principiológicos importantes na disputa regulatória do tema.[173]

III.3 – PL 4.612/2019

O PL nº 4.612/2019 merece análise destacada pois é o único projeto de lei federal com a pretensão de regular de forma abrangente o reconhecimento facial.[174] Chama atenção o fato de que o referido projeto dispõe não só sobre o uso, mas também sobre o desenvolvimento, a aplicação de tecnologias de reconhecimento facial e emocional, bem como de outras tecnologias digitais voltadas à identificação de indivíduos e à predição ou análise de comportamentos.[175] O fato de dispor sobre o desenvolvimento é surpreendente, pois indica que os desenvolvedores devem se preocupar com as questões legais desde a concepção das tecnologias.

O projeto inova ao adotar a proibição do tratamento discriminatório como um de seus pressupostos. Partindo disso, com vistas ao avanço das tecnologias digitais como fator estratégico para o desenvolvimento econômico e social, o uso da tecnologia deve se destinar a fins benéficos e dentro de padrões razoáveis e aceitáveis (art. 2, I). Verifica-se, portanto, a tentativa de um diálogo com a LGPD, que veda o tratamento de dados pessoais para fins discriminatórios ilícitos ou abusivos por meio do princípio da não discriminação.[176]

---

[173] ZANATA et al, Op. cit., 2020.

[174] BRASIL. *Ficha de tramitação do Projeto de Lei nº 4.612/2019*. Câmara dos Deputados. Disponível em: https://www.camara.leg.br/propostas-legislativas/2216455. Acesso em: 12 out. 2021.

[175] O PL 4612/2019 tramita em conjunto com o PL 12/2015 que tem um viés mais abrangente, dispondo sobre a utilização de sistemas de verificação biométrica de modo geral e outras providências.

[176] Art. 6º, IX da Lei Geral de Proteção de Dados.

Esse diálogo também se verifica no reconhecimento do tratamento de dados biométricos pelas TRFs como dados sensíveis. Desse modo, o tratamento de dados por meio de TRFs deve ser submetido às regras específicas da LGPD para dados pessoais sensíveis. Além disso, o PL tenta estabelecer novas competências para a Agência Nacional de Proteção de Dados (ANPD), como regulamentação dos dispositivos do referido projeto (art. 4º, III) e a deliberação, na esfera administrativa e em caráter terminativo, sobre a interpretação de suas disposições e dos casos omissos (art. 4º. V).

Há ainda disposições que dialogam com o Código de Defesa do Consumidor, como é o caso do art. 8º, IV, no qual se estabelece a defesa do consumidor como garantia dos afetados pelo uso das TRFs. Inclusive, com relação às garantias, o PL nº 4 .612/2019 também inova ao reservar um capítulo sobre direitos, dentre os quais a transparência e o acesso à informação (art. 7º, §§1º, 2º e 3º), o respeito à privacidade (art. 8, II) e a inviolabilidade da intimidade, da honra e da imagem (art. 8, III).

Apesar das inovações, o projeto é passível de algumas críticas: a despeito da tentativa de dialogar com as normas de proteção de dados, o projeto não considerou as exceções do art. 4º, III, da LGPD. Este artigo dispõe que a LGPD não se aplica ao tratamento de dados pessoais realizados para fins exclusivos de segurança pública, defesa nacional, segurança do Estado e investigações criminais, setores onde o emprego do reconhecimento facial é mais debatido.

Muito embora legislações específicas possam ser adotadas conforme as particularidades e riscos de cada setor,[177] o projeto não parece caminhar para suprir nenhuma dessas lacunas. Pelo contrário, na contramão do que dispõe as exceções do art. 4º, devolve para a própria ANPD o dever de regulamentar algumas disposições.

Embora mencione o uso de TRFs por órgãos e entidades públicas, o PL também não especifica como será a regulamentação para contextos importantes em que o Poder público já faz uso dessas tecnologias, como na segurança pública e investigações criminais, por exemplo. Ademais, apesar de haver um debate presente em relação ao respeito à privacidade, não há um aprofundamento sobre de que modo essa garantia pode ser respeitada. Esse aprofundamento é fundamental, considerando-se que o reconhecimento facial oferece riscos consideráveis para a privacidade dos regulados.

---

[177] Neste sentido, o Anteprojeto de Lei de Proteção de Dados para segurança pública e persecução penal. Ver mais em: BRASIL. A*nteprojeto sobre uso de dados na segurança pública deve ficar pronto em novembro*. Agência Câmara de Notícias, 22 set. 2020. Disponível em: https://www.camara.leg.br/noticias/694562-anteprojeto-sobre-uso-de-dados-na-seguranca-publica-deve-ficar-pronto-em-novembro/. Acesso em: 12 out. 2020.

III.4 – DO NECESSÁRIO DIÁLOGO COM A LEI GERAL DE PROTEÇÃO DE DADOS

A LGPD trouxe muitas repercussões para o ordenamento jurídico brasileiro, resultando no surgimento de um cenário propício para a elaboração de várias normas regulatórias específicas, tanto para o setor privado quanto o público. Assim, para além das exceções do art. 4º, que pedem regulação própria, é possível debater sobre regulação para a Inteligência Artificial, o Reconhecimento facial e Algoritmos com tomada de decisões automatizadas. Não obstante, é preciso também considerar os interesses dos agentes econômicos envolvidos, a assimetria de informações relacionada aos riscos e benefícios das inovações tecnológicas, o que gera um cenário que Bruno Bioni e Maria Luciano denominam de arena regulatória efervescente.[178]

Apesar das inúmeras aplicações no setor privado, é inegável que o reconhecimento facial seja uma tecnologia com propósitos e utilidades muito voltadas para o espectro de atividades excepcionadas pelo art. 4º, III, da LGPD: segurança pública, defesa nacional, segurança do estado, atividades de investigação e repressão de infrações penais. Desse modo, um projeto regulatório abrangente deve considerar essas particularidades e os marcos legais que já foram estabelecidos pela normativa de proteção de dados.

Aliás, a LGPD deixa claro que, apesar das exceções, os princípios por ela estabelecidos deverão ser sempre observados. É o comando do art. 4º, §1º. Vejamos:

> § 1º O tratamento de dados pessoais previsto no inciso III será regido por legislação específica, que deverá prever medidas proporcionais e estritamente necessárias ao atendimento do interesse público, observados o devido processo legal, os princípios gerais de proteção e os direitos do titular previstos nesta Lei.

Nesse sentido, Jacqueline Abreu entende que a LGPD manifesta um compromisso do Estado brasileiro com a proteção às garantias fundamentais diante de riscos da sociedade da informação, os quais devem ser levados em conta mesmo quando o tratamento é feito em nome da segurança pública.[179] Daí a afirmação da autora de que a LGPD não dá carta branca até que lei específica seja

---

[178] OLIVEIRA, Samuel R. apud BIONI, Bruno Ricardo; LUCIANO, Maria. *O princípio da precaução na Regulação de Inteligência artificial: seriam as lei de proteção de dados o seu pontal de entrada*? In: FRAZÃO, Ana; MULHOLLAND, Catlin (Org). *Inteligência Artificial e direito: ética, regulação e responsabilidade*. São Paulo: Thomson Reuters Brasil, 2019, p.22.

[179] ABREU, Jacqueline de Sousa. *Tratamento de dados pessoais para a segurança pública: contornos do Regime Jurídico pós-LGPD*. In: In: DONEDA, Danilo (coord.); SARLET, Ingo Wolfgang (coord.); MENDES, Laura Schertel (coord.); RODRIGUES JUNIOR, Otavio Luiz (coord.) BIONI, Bruno Ricardo (coord.). *Tratado de Proteção de Dados Pessoais*. Rio de Janeiro: Forense, 2021. p. 598.

aprovada, mas sim oferece desde já os parâmetros aplicáveis ao tratamento de dados pessoais envolvendo a segurança pública.[180]

Na LGPD, os princípios estão concentrados no art. 6º, segundo o qual, além da boa-fé, as atividades de tratamento de dados pessoais deverão observar os seguintes princípios: a finalidade, a adequação, a necessidade, o livre acesso, a qualidade dos dados, a transparência, a segurança, a prevenção, a não discriminação e a prestação de contas.

Na perspectiva do princípio da finalidade, um determinado agente responsável pela operação de um sistema de reconhecimento facial deve, desde antes da coleta de informações biométricas, estabelecer para qual finalidade está sendo realizada a operação de tratamento, que também deve ser adequada à finalidade informada. Em consonância com o princípio da necessidade, o agente também deve demonstrar que não dispõe de meios menos gravosos para realizar a operação.

O agente também deve se preocupar com a qualidade das informações sob sua guarda, adotando medidas de segurança adequadas a prevenir danos ao titular. Deve também ser responsabilizado pelos danos que eventualmente causar (prestação de contas). Por último, mas não menos importante, em razão do alto potencial discriminatório envolvido no uso de TRF, o sistema utilizado deve estar em harmonia com o princípio da vedação à discriminação.

Nesse contexto, tanto para o setor público quanto o privado, os princípios da proporcionalidade e os princípios gerais do art. 6º devem ser o ponto de partida regulatório. Samuel Oliveira ao discorrer sobre modelos regulatórios para as TRFs ressalta a importância dos princípios na regulação de tecnologias que evoluem rapidamente. Nesse sentido, afirma Samuel, os estatutos legais devem ser flexíveis o suficiente para atender às novas tecnologias, devendo ter alguns princípios básicos como ponto de origem.[181]

Levando em consideração as exceções do art. 4º, III, no caso do setor privado em geral,[182] as bases legais, especialmente aquelas destinadas ao tratamento de dados pessoais sensíveis, também merecem devida atenção. Isso porque todo o tratamento de dados pessoais sensíveis só pode ser realizado sob as hipóteses do art. 11: com o consentimento do titular, que deve ser fornecido de forma específica e destacada e para finalidades específicas; e sem o consentimento, nas hipóteses elencadas nas alíneas "a" a "g" do mesmo artigo.

---

[180] Ibid. p. 600.
[181] OLIVEIRA, Samuel. Op. cit., 2021. 144.
[182] É forçoso concluir que um agente privado que atue de alguma forma como controlador ou operador em tratamento de dados pessoais para fins das atividades do art. 4, III devem estar sob o regime específico.

É forçoso supor que grande parte dos agentes deve justificar o tratamento de dados biométricos para fins de reconhecimento facial por hipóteses legais que não requerem o consentimento dos titulares, tendo em vista a característica essencial dessas tecnologias de poderem agir à distância e sem a ciência do indivíduo.

Para além dos princípios e das bases legais, conectado com o princípio da transparência e da não discriminação, há outro ponto de diálogo necessário entre uma eventual norma regulatória e a LGPD que reside no direito de revisão estipulado pelo seu art. 20. Também conhecido como direito à explicabilidade, este direito estabelece para o titular dos dados o direito a solicitar a revisão de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem seus interesses.

O §1º do art. 20 acrescenta ainda que o controlador deverá fornecer, sempre que solicitadas, informações claras e adequadas a respeito dos critérios e dos procedimentos utilizados para a decisão automatizada, observados os segredos comercial e industrial. Aqui se verifica um desafio regulatório evidente que é o de se buscar equilibrar os interesses dos indivíduos frente aos interesses dos agentes econômicos, muito em razão de que as TRFs, como vimos, são baseadas em algoritmos não só construídos em linguagem pouco acessível, mas também protegidos pelo segredo comercial.

Além dos problemas de ordem técnica envolvidos nas TRFs, como a opacidade, problemas de acurácia e enviesamento, os interesses dos agentes econômicos também são questões relevantes. Do mesmo modo, não se pode ignorar o poder desses agentes no desenvolvimento de algoritmos. Não é à toa, que Ana Frazão entende que a regulação de dados pessoais constitui uma forma de endereçar os riscos do poder crescente das grandes plataformas sobre os cidadãos.[183]

Enquanto se discute a redução de assimetrias de poder frente aos consumidores e pequenas empresas por meio da regulação de grandes agentes de tecnologia,[184] são as normas de proteção de dados uma base inicial de amparo aos indivíduos. Nesse sentido, Frazão também afirma que, como importante medida para endereçar diversos problemas graves decorrentes do capitalismo de vigilância, a tutela dos dados pessoais é mais do que uma mera proteção da individualidade ou da intimidade.[185]

---

[183] FRAZÃO, Ana. Op. cit.,2020. p. 43.
[184] Em junho de 2021, o Comitê Judiciário da Câmara dos Estados Unidos divulgou uma agenda antimonopólio com foco na redução do poder das *big techs*. Ver mais em: UNITED STATES OF AMERICA. *House Lawmakers Release Anti-Monopoly Agenda for "A Stronger Online Economy: Opportunity, Innovation, Choice":* Bipartisan legislation will restore competition to digital marketplace and rein in largest tech platforms. House of Representatives, Washington, 11 jun. 2022. Disponível em: https://judiciary.house.gov/news/documentsingle.aspx?DocumentID=4591. Acesso em: 8 mar. 2022.
[185] Ibid. p. 31.

III.4.1 – A Proteção de Dados como um Direito Fundamental

As legislações de proteção de dados têm avançado pelo mundo conforme preocupações crescentes com a privacidade dos indivíduos, que decorrem de um mundo que é *superconectado* e que evidencia cada vez mais a importância de se proteger os dados pessoais. O direito à proteção de dados começou a se consolidar na Europa a partir de uma decisão do Tribunal Constitucional alemão[186] no caso do censo demográfico de 1983 (*Volkszählungsurteil*)[187]. Nessa decisão, foi reconhecido o direito à autodeterminação informativa, devolvendo ao indivíduo o poder de decidir acerca do seu fluxo informacional.[188]

A disciplina da proteção de dados ganhou novos contornos com a Diretiva 95/46/CE de 1995, que instituiu um quadro regulamentar a fim de estabelecer um equilíbrio entre um nível elevado de proteção da vida privada das pessoas e a livre circulação de dados pessoais no interior da União Europeia.[189] Em 2018, o escândalo *Cambridge Analytica* pôs à prova o arcabouço de proteção da privacidade e dos dados dos indivíduos disponível no mundo, especialmente nos Estados Unidos e na Europa, que estavam no centro do escândalo. No mesmo ano, surge na Europa o Regulamento Geral de Proteção de Dados (GDPR)[190] revogando a Diretiva 95/46/CE e, nos Estados Unidos, o *California Consumer Private Act* (CCPA).[191]

Nessa esteira, é aprovada no Brasil a Lei Geral de Proteção de Dados – Lei nº 13.709/2018. Já em debate desde 2012,[192] o Projeto de Lei originário passou por inúmeras discussões e alterações,

---

[186] Segundo Fabiano Menke, esta decisão foi tão impactante e consistiu num verdadeiro marco da proteção de dados, por ter fixado várias diretrizes desta disciplina que influenciaram legislações, doutrina e jurisprudência de diversos países. MENKE, Fabiano. *A proteção de dados e o direito fundamental à garantia da confidencialidade e da integridade dos sistemas técnico-informacionais no direito alemão*. In. Revista Jurídica Luso Brasileira, Lisboa, Ano 5 (2019), nº1. p. 701-809. 2019. Disponível em: https://www.cidp.pt/publicacao/revista-juridica-lusobrasileira-ano-5-2019-n-1/186. Acesso em: 3 de mar. 2022.

[187] TRIBUNAL Constitucional Federal. *Volkszählungsurteil.* Acórdão do Primeiro Senado de 15 de dezembro de 1983 - 1 BvR 209/83, parágrafos 1 215. Disponível em:https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/DE/1983/12/rs19831215_1bvr020983.html. Acesso em: 3 de mar. 2022.

[188] SCHWABE, Hürgen. MARTINS, Leonardo. *Cinquenta anos de Jurisprudência do Tribunal Constitucional Alemão*. Montevideo: Konrad Adenauer Stiftung, 2005. p. 237.

[189] O texto da Diretiva 95/46/CE pode ser consultado em português no endereço: https://eur-lex.europa.eu/legal-content/PT/LSU/?uri=celex:31995L0046. Acesso em 3 de mar. 2022.

[190] Ver mais em: https://gdpr-info.eu/. Acesso em 3 de mar. 2022.

[191] Ver mais em: https://oag.ca.gov/privacy/ccpa. Acesso em: 3 de mar. 2022.

[192] O projeto de lei que deu origem à LGPD foi o PL n º 4.060/2012, contudo, conforme aponta Danilo Doneda, em 2005, as discussões do tema de proteção de dados no Mercosul, no Subgrupo de Trabalho nº13 (SGT13), foram o estopim que deu origem a um discreto, porém crescente, debate sobre o tema pelo governo brasileiro. Ver mais em: DONEDA, Danilo. *Panorama histórico da proteção de dados pessoais*. In: In: DONEDA, Danilo (coord.); SARLET, Ingo Wolfgang (coord.); MENDES, Laura Schertel (coord.); RODRIGUES JUNIOR, Otavio Luiz (coord.) BIONI, Bruno Ricardo (coord.). *Tratado de Proteção de Dados Pessoais*. Rio de Janeiro: Forense, 2021. p. 15-16.

chegando a incorporar muitos dos conceitos do regulamento europeu.[193] Com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural, a LGPD introduziu no ordenamento jurídico brasileiro uma série de novos institutos e princípios.

Mister lembrar que, antes do surgimento da LGPD, algumas leis setoriais já endereçavam algumas questões relativas à privacidade e à proteção de dados, como a Lei de Acesso à Informação, Código de Defesa do Consumidor e Marco Civil da Internet. Contudo, foi com a LGPD que o direito à proteção de dados se consolidou no Brasil, representando um marco histórico para a proteção de liberdades individuais. Um novo marco seria alcançado em 10 de fevereiro de 2022 com a promulgação da PEC nº 115, que deu status constitucional ao direito à proteção de dados. A emenda incluiu no art. 5º o inciso LXXIX, segundo o qual é assegurado, nos termos da lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais.[194]

Como vimos no tópico III. 4, a LGPD traz reflexos diretos para o uso de tecnologias de reconhecimento facial, ao estabelecer princípios que devem ser observados para todo o tratamento de dados pessoais e ao definir dados biométricos como categorias especiais de dados. Contudo, na perspectiva regulatória das TRFs, o reconhecimento à proteção de dados como um direito fundamental representa um novo paradigma, pois qualquer projeto regulatório já deve ser desenvolvido orientado pela proteção de dados como um direito fundamental.

Temos visto como as TRFs podem afetar os indivíduos, violando sua intimidade, dignidade, negando serviços ou impedindo sua locomoção por espaços públicos. Sendo o conjunto de direitos fundamentais a razão de ser do Estado Regulador,[195] que possui como pressuposto que a regulação tem por finalidade preeminente a proteção de direitos fundamentais,[196] um projeto regulatório de TRFs também deve não só observar a proteção de dados como também suas conexões com outros direitos fundamentais e com princípios constitucionais, em especial a dignidade da pessoa humana (1º, III), a igualdade (3º, III, e art. 5º, caput), a não discriminação (3º, III), a intimidade (5º, X), o sigilo de dados (5º, XII) e a livre locomoção (XV).

---

[193] BRASIL. PL nº 4.060/2012. Câmara dos Deputados. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=548066. Acesso em: 3 de mar. 2022.

[194] Além de incluir a proteção de dados no rol de direitos fundamentais na Constituição Federal, a PEC nº 115 também fixou competência privativa da União para legislar sobre proteção e tratamento de dados pessoais. Ver mais em: BRASIL, *Emenda Constitucional nº 115*. Presidência da República, 10 fev. 2022. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/Emendas/Emc/emc115.htm#art1. Acesso em: 3 de mar. 2022.

[195] ARANHA, Mário Iório. *Manual de Direito Regulatório*: Fundamentos de Direito Regulatório. 3ª. ed. Londres: Laccademia Publishing, 2015. n.p. [E-book]

[196] Ibid. n.p.

III.4.2 – Dados Biométricos de Reconhecimento Facial a Partir de Dados Disponíveis Publicamente

A LGPD institui um regime especial para os chamados dados pessoais sensíveis. Seu art. 5º, II os define como dados pessoais sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural.

Conforme Regina Ruaro e Gabrielle Sarlet, o conjunto dessas informações compõe os perfis ou as identidades digitais, possuindo valor político e, sobretudo, econômico, uma vez que podem ser a matéria-prima para novas formas de controle [...], especialmente mediante o uso de algoritmo, de inteligência artificial e *big data*.[197] A utilização indevida de dados pessoais sensíveis pode, portanto, levar ao cerceamento de liberdades fundamentais e, por esse motivo, como vimos supra, a LGPD estabelece um rol específico de hipóteses legais que regulam o tratamento dos dados que integram essa categoria.

Os dados biométricos (digital, íris, reconhecimento facial etc.), como categoria de dados pessoais sensíveis, ganham relevância sobretudo porque, como temos visto no decorrer deste trabalho, são os mais diretamente relacionados com a identificação de um titular, não precisando de qualquer associação com outras informações para este fim. Não por outra razão, são a opção mais utilizada como alternativa às antigas senhas.[198]

A normativa brasileira de proteção de dados não traz o conceito de dados biométricos, o que demanda análise diante de um caso concreto. O GDPR, por sua vez, define os dados biométricos como dados pessoais resultantes de um tratamento técnico específico relativo às características físicas, fisiológicas ou comportamentais de uma pessoa singular que permitam ou confirmem a identificação única dessa pessoa singular, nomeadamente imagens faciais ou dados dactiloscópicos.[199]

---

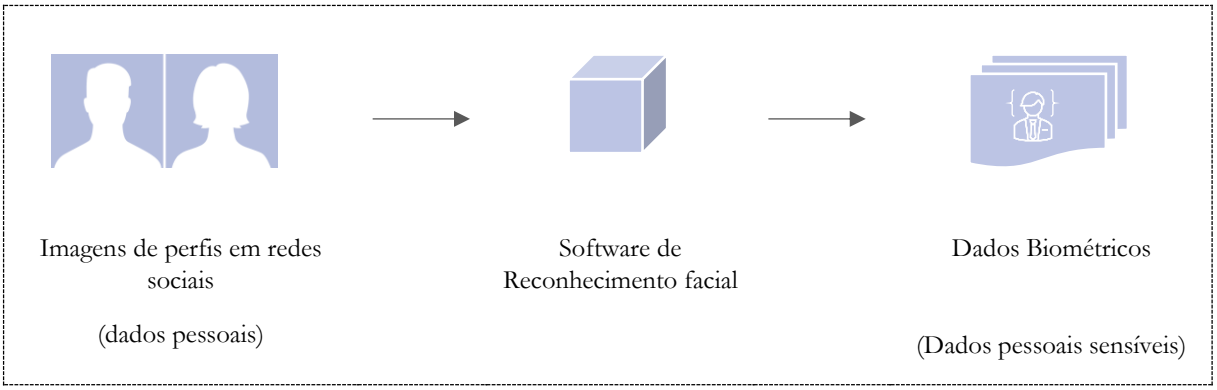
[197] RUARO, Regina Linden. SARLET, Gabrielle B. Sales. *O direito fundamental à proteção de dados sensíveis no sistema normativo brasileiro*: uma análise acerca das hipóteses de tratamento e da obrigatoriedade do consentimento livre, esclarecido e informado sob o enfoque da Lei Geral de Proteção de Dados (LGPD) – Lei 13.709/2018. In: DONEDA, Danilo (coord.); SARLET, Ingo Wolfgang (coord.); MENDES, Laura Schertel (coord.); RODRIGUES JUNIOR, Otavio Luiz (coord.) BIONI, Bruno Ricardo (coord.). Tratado de Proteção de Dados Pessoais. Rio de Janeiro: Forense, 2021. p. 182.

[198] Em recente precedente do TJSP, a 17ª Câmara de Direito Privado de Justiça do Tribunal de São Paulo entendeu que a biometria facial Biometria facial é uma forma válida de manifestação de vontade apta a suprir a falta de assinatura na formalização de contrato eletrônico. Ver mais em: SÃO PAULO. Tribunal de Justiça de São Paulo. 17ª Câmara de Direito Privado de Justiça do Tribunal de São Paulo. Apelação Cível nº 1005329-07.2021.8.26.0077. DACLARATÓRIA DE INEXISTÊNCIA DE DÉBITO CC. REPETIÇÃO DE INDÉBITO E IDENIZAÇÃO POR DANO MORAL. Empréstimo consignado não reconhecido pela autora. **Demonstrada a regularidade da contratação realizada por meio eletrônico** (grifo nosso) .... Apelante: Banco C6 Consignado S/A. Apelada: Cleia Braga Silva. Afonso Bráz. Relator: São Paulo, 20 jan. 2022.

[199] Art. 4, item 14 do GDPR.

Partindo do conceito europeu, uma mera imagem publicada em uma rede social não atrairia o regime especial de proteção, mas sim, caso posteriormente fosse utilizada por ferramenta de reconhecimento facial. Em síntese, no exemplo dado, no momento da coleta, os dados não são sensíveis, mas passam a ser a partir do tratamento técnico realizado pela ferramenta de reconhecimento facial. Logo, a mera coleta poderia em tese se dar por qualquer das hipóteses do art. 7º da LGPD, que autoriza o tratamento de dados pessoais comuns. Já o seu processamento por uma TRF demandaria uma justificativa legal pelas hipóteses do art. 11, visto que resultariam em dados biométricos.

Figura 4 - Coleta de dados de redes sociais por empresa de reconhecimento facial



Fonte: elaborado pelo autor

Dados como as imagens de perfis de redes sociais são dados manifestamente públicos. Como bem explica Giovanna Tavares, embora não sejam conceituados pela LGPD, uma definição de dados tornados manifestamente públicos pelo titular pode ser extraída a partir de uma leitura sistemática da LGPD sendo, portanto, aqueles dados tornados públicos única e exclusivamente por seus titulares e não por terceiros[200] e ainda realisticamente acessíveis ao público geral, como aqueles que um usuário publica em sua rede social.[201]

Considerando o conceito de dados tornados manifestamente públicos pelo titular e considerando ainda que softwares de reconhecimento facial utilizam, também, imagens extraídas de redes sociais para compor suas bases de dados,[202] é preciso atenção a dois detalhes importantes: o primeiro é que a LGPD estabelece que, para o dados pessoais (comuns), especificamente aqueles

[200] TAVARES, Giovanna Milanez. *O tratamento de dados pessoais disponíveis publicamente e os limites impostos pela LGPD*. Rio de Janeiro: Editora Processo. 2022.p. 73.
[201] Ibid. p. 77.
[202] Ver sobre o software *Clearview AI* no Item II.5.

tornados manifestamente públicos pelo titular, é dispensada a exigência do consentimento, resguardados os direitos do titular e os princípios previstos na lei (art. 7, §4º).

O segundo detalhe é que, além da dispensa de consentimento, a LGPD estabelece ainda que o tratamento posterior de dados tornados manifestamente públicos pelo titular poderá ser realizado para novas finalidades, observados os propósitos legítimos e específicos para o novo tratamento e a preservação dos direitos do titular, assim como os fundamentos e os princípios da LGPD (art. 7, §7º).

Para Tavares, tanto o §4º quanto o §7º do art. 7 da LGPD representam critérios específicos para o tratamento de dados tornados manifestamente públicos pelo titular: tratamento primário equivalente e tratamento posterior compatível, respectivamente.[203] Isso implica dizer que a coleta, por terceiros, de imagens de perfis em redes sociais para fins de reconhecimento facial violaria as disposições da LGPD tendo em vista que o tratamento primário não seria equivalente ao tratamento informado ao titular durante o fornecimento das informações. Tampouco o tratamento posterior seria compatível, pois é razoável supor que não se pode esperar que, ao fornecer imagem para identificação pessoal em rede social, um usuário médio espere que ela seja utilizada por terceiros para fins de reconhecimento facial.

Para além da coleta, na situação hipotética exposta acima, qualquer operação de tratamento [204] envolvida no processamento técnico realizado por ferramenta de reconhecimento facial conferiria status especial às imagens extraídas de redes sociais, atraindo a incidência do regime especial dos dados sensíveis do art. 11 da LGPD. Ocorre que as exceções conferidas nos §§ 4º e 7º do art. 7º não se repetem no art. 11. Portanto, é possível concluir que TRFs, cuja base de dados é composta por imagens extraídas por terceiros a partir de redes sociais, como é o caso do já mencionado *Clearview AI*,[205] não poderiam operar no Brasil.

III.5 – TRAZENDO A QUESTÃO RACIAL PARA O DEBATE

Não há como promover um debate sobre regulação do reconhecimento facial sem levar em consideração a questão racial, sobretudo no Brasil, onde o racismo é prática embutida nas estruturas

---

[203] TAVARES, Giovanna Milanez. Op. Cit, 2022. p. 134.

[204] Segundo o art. 5º, X da LGPD operação de tratamento é toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração;

[205] Item II.5.

sociais. Levantamentos preliminares apontam que mais de 90% das apreensões realizadas por reconhecimento facial no Brasil são de pessoas negras. Nesse contexto, um projeto regulatório abrangente deve passar pelo debate sobre o viés discriminatório racial não só da tecnologia como também das próprias políticas de segurança pública.

Também não se pode negligenciar a desigualdade racial que há no processo legislativo. Segundo o Observatório do Legislativo Brasileiro, em relatório sobre a legislatura 2019 e 2022, a sub-representação dos negros ainda é aguda na Câmara dos Deputados levando a um impacto negativo expressivo sobre a capacidade estatal de reverter o cenário alarmante de desigualdade racial no Brasil. O Observatório aponta que os negros são sub-representados nas comissões permanentes de maior impacto sobre a atividade legislativa e na função de relatoria, uma das mais importantes no processo legislativo. Outro ponto alarmante diz respeito à tramitação de projetos propostos por parlamentares negros, que entram nas comissões em proporção semelhante à dos brancos, mas têm menos relatores designados e pareceres emitidos.[206]

Nessa perspectiva, ao reconhecemos que a tecnologia pode ser racista, em parte por ser majoritariamente desenvolvida por brancos, é forçoso supor que um projeto regulatório construído no mesmo molde pode incorrer no risco de não endereçar adequadamente as questões raciais. O PL nº 4.612/2019, por exemplo, dispõe sobre a não discriminação, mas não traz qualquer detalhamento sobre a questão.

De acordo com a ficha de tramitação do referido projeto, que tramita conjuntamente com o PL nº 12/2015, já houve audiência pública para discutir o projeto pela Comissão de Ciência e Tecnologia, Comunicação e Informática (CCTCI), mas pelo requerimento da audiência verifica-se que foram convidadas apenas entidades técnicas: SERPRO, Polícia Federal, Associação Nacional de Certificação Digital (ANCD), Associação Nacional de Autoridades de Certificação Digital (ANACD).[207]

Verifica-se, portanto, a falta da inclusão de um debate racial necessário na discussão do PL nº 4.612/2019. Diferente tem sido a experiência americana onde, como vimos no início deste capítulo, o movimento *Black Live Matters* teve impacto essencial na decisão das *big techs* de pressionar o estado americano por regulação. Além disso, o congresso americano tem tentado endereçar as reivindicações

---

[206] FERES JUNIOR, João; GERSHON, Debora; MEIRELES, Fernando. *A Produção Legislativa de Brancos e Negros na Câmara*. OBSERVATÓRIO DO LEGISLATIVO BRASILEIRO, 15 fev. 2021. Disponível em: https://olb.org.br/a-producao-legislativa-de-brancos-e-negros-na-camara/. Acesso em: 17 out. 2021.

[207] Ficha de tramitação do Projeto de Lei nº 12/2015 no qual está apensado o projeto de Lei nº 4.612/2019. Disponível em: https://www.camara.leg.br/propostas-legislativas/944254. Acesso em: 17 out. 2021.

raciais nas discussões sobre regulação, realizando uma série de audiências sobre o impacto das TRFs nos direitos e liberdades civis visando enfrentar o temor de discriminação racial no uso da tecnologia.[208]

A participação social no processo legislativo é fundamental em uma sociedade democrática. Desse modo, levando em consideração as interseções entre a debate racial e a vigilância estatal, é interessante que a instrução e análise de proposições regulatórias conte com uma participação ampla da sociedade por meio de audiências públicas, com espaço reservado não só para os especialistas em tecnologia e proteção de dados, mas também por órgãos e entidades dedicados na luta por igualdade racial.

III.6 – DESAFIOS REGULATÓRIOS

Até aqui, foi possível compreender minimamente os mecanismos essenciais envolvidos no processo de reconhecimento facial por meio da explanação quanto à suas etapas básicas, resumidas nos processos de identificação e reconhecimento do rosto humano. Também foram destacados os problemas de ordem técnica comuns às TRFs em geral.

Ademais, diante do efervescente cenário regulatório que tem se formado no Brasil, muito em razão da relativamente recente LGPD, foram analisados alguns Projetos de Lei de iniciativa estadual e federal. Por fim, a partir de um recorte sobre um ponto de partida inicial para a regulação das TRFs, sem a pretensão de apontar um desenho ideal, adiante serão enumerados alguns desafios que devem ser enfrentados pelo regulador na escolha de um modelo regulatório adequado.

O potencial discriminatório das TRFs deve ser uma preocupação nas discussões. Ao longo do presente trabalho vimos diversos exemplos de situações discriminatórias resultantes do uso do reconhecimento facial, que tem como característica fundamental o processamento de informações muito ligadas ao racismo, como as feições humanas e a cor da pele. Não é à toa que, a exemplo do GDPR,[209] a LGPD criou uma categoria especial de dados pessoais no qual estão inseridos os dados biométricos, a categoria dos dados pessoais sensíveis.

---

[208] Audiência realizada no Congresso americano sobre o reconhecimento facial e seus impactos nas liberdades civis. A transcrição pode ser baixada em: UNITED STATES OF AMERICA. *House Hearing, 116th Congress - Facial recognition technology: part i its impact on our civil rights and liberties*. GOVINFO, 22 maio 2019. Disponível em: https://www.govinfo.gov/app/details/CHRG-116hhrg36663/summary. Acesso em: 17 out. 2021.

[209] O GDPR é o regulamento europeu da proteção de dados. É norma que inspirou fortemente a LGPD no Brasil. O Art. 9 do GDPR versa sobre o processamento de categorias especiais de dados pessoais definidos no seu art. 4.

A tecnologia não pode ser utilizada para reforçar as desigualdades existentes na sociedade. O racismo no Brasil está em todos os níveis da sociedade brasileira. Desse modo, a questão racial não pode ficar de fora do debate. Logo, a discussão acerca do potencial discriminatório das TRFs requer necessariamente o envolvimento de diversos atores da sociedade civil, com participação imprescindível daqueles que atuam em prol da igualdade racial.

Os problemas de ordem técnica envolvidos na tecnologia não podem ser negligenciados no debate. Um projeto de lei sobre reconhecimento facial deve abordar os riscos de ordem técnica envolvidos na utilização das TRFs. Como abordado no capítulo anterior, o enviesamento dos dados, acurácia dos algoritmos durante o processo de detecção da face, correlacionamentos ilegítimos e opacidade produzem resultados nefastos para os indivíduos. É possível discutir, por exemplo, que os algoritmos utilizados por essas tecnologias sejam periodicamente submetidos a órgãos de qualidade para testes visando monitorar, medir e corrigir o preconceito racial embutidos nos seus códigos.[210]

A opacidade é igualmente preocupante especialmente porque afeta os indivíduos na fruição de seus direitos, a sociedade na compreensão dos seus efeitos e o legislador na elaboração de leis. Essa falta de transparência acerca das estruturas internas das TRFs revela uma assimetria de informações danosa entre programadores e legisladores, intérpretes e aplicadores da lei. É o que se pode verificar nos casos de propositura de Projetos de Lei com falta de embasamento técnico, como vimos no tópico III.3 deste capítulo. Nesse sentido, Frank Pasquale entende que os algoritmos podem ser mais responsáveis, respeitando os direitos de justiça e dignidade pelos quais as gerações lutaram. Para o autor, esse desafio não é técnico, mas político,[211] e o primeiro passo é a lei, que capacita as pessoas a ver e desafiar o que os algoritmos estão dizendo sobre nós.[212]

A depender da finalidade do uso do reconhecimento facial e considerando as exceções do art. 4º da LGPD, o art. 20 da mesma Lei pode auxiliar no enfrentamento da opacidade dessas tecnologias. O referido dispositivo define o chamado direito de revisão de decisão ou direito à explicabilidade, no qual o titular de dados tem direito de solicitar a revisão de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem seus interesses, incluídas as decisões destinadas a definir o seu perfil pessoal, profissional, de consumo e de crédito ou os aspectos de sua personalidade.

---

[210] Nos Estados Unidos essa testagem é realizada pelo *National Institute of Standards and Technology - NIST*, equivalente ao Instituto Nacional de Metrologia, Qualidade e Tecnologia - INMETRO no Brasil.

[211] Ao discutir a transparência de algoritmos Frank Pasquale vai além da sugestão de testagem de algoritmos. PASQUALE. Frank. *Algorithms are producing profiles of you. What do they say? You probably don't have the right to know*. Disponível em: https://aeon.co/essays/judge-jury-and-executioner-the-unaccountable-algorithm. Acesso em: 8 dez. 2021.

[212] Ibid. n.p.

Ademais, como destacado anteriormente, como princípio geral da proteção de dados, a transparência (art. 6º, VI) deve ser observado mesmo nas situações excepcionadas pelo art. 4º. Conclui-se, portanto, que é indispensável que um projeto regulatório vise estabelecer um diálogo com a LGPD. Sobretudo nas situações de implementação de TRFs para fins de segurança pública, esse diálogo é importante para que se busque equilibrar corretamente os interesses entre privacidade e segurança e ainda, conforme Samuel Oliveira, visando a garantia dos direitos dos titulares de dados pessoais, a fim de impedir tratamentos irregulares ou abusivos por parte do poder público.[213]

Ainda sobre o art. 20 da LGPD, um eventual projeto regulatório pode trazer de volta a regra de ouro nas decisões automatizadas. Vetado pelo Presidente da República na LGPD, o §3º do art. 20 instituía que a revisão de decisões automatizadas deveria ser realizada por pessoa natural, conforme previsto em regulamentação da autoridade nacional, levando em consideração a natureza e o porte da entidade ou o volume de operações de tratamento de dados.[214] Parece razoável concluir que falhas no processo de reconhecimento facial devam ser revisadas por uma pessoa natural a fim de evitar uma validação por outro algoritmo.[215]

A exemplo do PL nº 4.612/2019 analisado supra, que contém dispositivos que conversam com o CDC, é interessante que um projeto regulatório busque dialogar com outras normas do ordenamento jurídico que, desde antes da LGPD, já tratavam de assuntos relacionados ao tratamento de dados pessoais, como os já mencionados CDC, Lei de Acesso à Informação, Lei do Cadastro Positivo e Marco Civil da Internet.

Muito embora a LGPD represente um avanço importantíssimo para a defesa de direitos fundamentais e tenha trazido grandes repercussões para o direito brasileiro, conforme aponta Ana Frazão, ela sozinha não é suficiente para endereçar os problemas do tratamento de dados pessoais.[216]

---

[213] OLIVEIRA, Samuel. Op. cit. 2021. p. 149.

[214] Nas razões de veto o Presidente da República alegou que a propositura legislativa, ao dispor que toda e qualquer decisão baseada unicamente no tratamento automatizado seja suscetível de revisão humana, contraria o interesse público, tendo em vista que tal exigência inviabilizará os modelos atuais de planos de negócios de muitas empresas, notadamente das startups, bem como impacta na análise de risco de crédito e de novos modelos de negócios de instituições financeiras, gerando efeito negativo na oferta de crédito aos consumidores, tanto no que diz respeito à qualidade das garantias, ao volume de crédito contratado e à composição de preços, com reflexos, ainda, nos índices de inflação e na condução da política monetária. Ver mais em: BRASIL. *Mensagem nº 288*. PRESIDÊNCIA DA REPÚBLICA, 8 de jul. 2019. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2019/Msg/VEP/VEP-288.htm. Acesso em: 8 dez. 2021.

[215] Essa regra de ouro é motivo de grande debate nas tecnologias de inteligência artificial de modo geral. A Austrália, por exemplo, adotou em 2018 a revisão de decisões automatizadas adversas por pessoas naturais a fim de evitar que a tecnologia dê a palavra final sobre a negativa de direitos. Ver mais em: WROE, David. *Top official's 'golden rule': in border protection, computer won't ever say no.* The Sydney Morning Herald, 13 jul. 2018. Disponível em: https://www.smh.com.au/politics/federal/top-official-s-golden-rule-in-border-protection-computer-won-t-ever-say-no-20180712-p4zr3i.html. Acesso em: 8 dez. 2021.

[216] FRAZÃO, Ana. *Objetivos e alcance da Lei Geral de Proteção de Dados*. In: TEMPEDINO, Gustavo, OLIVA, Milena. *Lei Geral de Proteção de Dados e duas repercussões no Direito brasileiro*. 2ª Edição. Thomson Reuters, Revista dos Tribunais, 2020. p.

A elevação da proteção de dados ao status de direito fundamental, por si só, também não resolve todos os problemas da proteção de dados e, sem sombra de dúvida, traz um desafio ainda maior para os legisladores na regulação das TRFs. Contudo, é importante que a proteção de dados como direito fundamental seja vista não como um entrave, mas sim como um dos fins da regulação.

CONCLUSÃO

A vigilância está liquefeita de tal modo na sociedade que nos encontramos em certa medida acostumados a ela. Quando muito a questionamos, o fazemos em relação ao excesso de câmeras ao nosso redor, quando na verdade somos constantemente vigiados por diversos meios. Contudo, muito mais preocupante que a quantidade de dispositivos que compõem a rede de vigilância são os mistérios que envolvem suas estruturas e seus processos de tomada de decisão sobre aspectos essenciais de nossas vidas.

A partir daí, decidir pela regulação, suspensão ou banimento do reconhecimento facial faz mais sentido se tiver como ponto de partida o questionamento quanto aos mecanismos por traz dessas tecnologias e se possuímos mecanismos suficientes de proteção que nos assegure o respeito às garantias mínimas de uma sociedade democrática.

Tanto a vigilância estatal quanto a privada souberam se beneficiar ao máximo da abundância do substrato mais importante das sociedades digitais: nossos dados. Para maximizar os ganhos de capital anunciados pelo Capitalismo de Vigilância era mais urgente cumprir a promessa de entregar mais capacidade de processamento de maiores volumes de dados e em maiores velocidades que cumprir a promessa de resolver os problemas que foram surgindo em torno da falsa objetividade na tecnologia. Aliás, cumprir essa última promessa se tornou menos imediata em um mundo que passou a se pautar por correlacionamento e por inferências.

Diante dos desafios iniciais que o avanço tecnológico impôs, em um primeiro momento, foi legítima a preocupação com a privacidade e com a proteção dos dados, direitos que ainda estamos tentando entender como tutelar. Mas o que se viu depois, foi o surgimento de ameaças a direitos que compõem a base de uma sociedade democrática. E não só a nossa participação política foi posta à prova como também os processos democráticos de escolha.

Acompanhado de problemas relacionados à acurácia de seus resultados, da opacidade características de seus mecanismos internos e do enviesamento no seu suprimento de dados, o reconhecimento facial trouxe novos elementos de preocupação, notadamente em razão de ser uma

tecnologia que capta aspectos essenciais da nossa individualidade: nosso rosto e, com ele, nossas emoções. Isso porque, assim como outras tecnologias, o reconhecimento facial se mostrou capaz de reproduzir as mesmas desigualdades do mundo real por meio comportamentos discriminatórios e racistas. As preocupações em torno do reconhecimento facial são pertinentes, especialmente porque não se pode conviver com tecnologias que reproduzem práticas antidemocráticas, como o racismo.

Em razão de operarem sobre dados com características muito particulares, enquanto não se define uma regulação adequada e que enderece corretamente os seus problemas, são as normas de proteção de dados um ferramental inicial para proteção dos indivíduos. No Brasil, a LGPD não só fornece as bases legais para justificar o tratamento de dados pessoais sensíveis por meios de TRFs como também fornece mecanismos para se questionar seus resultados, que independente das exceções que a própria Lei traz, deve se orientar por seus princípios, máxime o da não discriminação.

As TRFs atendem tanto aos propósitos da vigilância comercial quanto da vigilância estatal, que as emprega principalmente na defesa nacional, segurança do estado e atividades de investigação e repressão de infrações penais, justamente as situações excepcionadas pela LGPD. A exceção não foi à toa. Essas atividades, muito relacionadas ao poder de repressão estatal, demandam uma regulação mais específica para o tratamento de dados. Além desses setores pendentes de regulação específica, a LGPD abriu caminhos para uma série de regulações setoriais na área da tecnologia como, por exemplo, tecnologias gerais biométricas e inteligência artificial.

Em que pese, nos últimos anos tenha havido no Brasil diversos projetos de leis voltados para a regulação dessas tecnologias, vimos que a maioria são somente autorizativos, com o intuito de impor a sua utilização em determinados contextos. As propostas federais mais abrangentes, isto é, com propósito autorizativo, mas também delimitador, os PLs nº 21/2020 e nº 4.612/2019, embora representem um sinal positivo na mudança de postura do legislador, não abordam questões de ordem técnica nem questões sociais importantes, como a racial. Enquanto nenhum projeto é aprovado, grupos sociais mais vulneráveis são os que mais sofrem seus efeitos, em especial os negros, como vem mostrando relatórios de redes de observatórios do uso atual dessas tecnologias.

No caso da vigilância comercial, muito embora o ordenamento jurídico brasileiro seja dotado de um conjunto de normas setoriais apto a proteger em alguma medida os titulares de dados, o alto potencial discriminatório dessas tecnologias somados aos problemas relacionados à opacidade típica de suas estruturas internas revelam uma necessidade igualmente urgente de uma regulação adequada. Essa regulação deve buscar conversar com o ordenamento jurídico, sobretudo com as normas de proteção de dados, se apoiando na proteção de dados como um direito fundamental e nas suas relações

com outros direitos constitucionais. Por último, deve ainda considerar a natureza e as especificidades das TRFs frente as demais tecnologias.

A partir do tema analisado no presente trabalho, foi possível concluir que a implementação e uso de TRFs demandam uma regulação própria muito em razão das particularidades dessas tecnologias e dos riscos para a sociedade, suas instituições e a própria democracia. São muitos os desafios a serem enfrentados pelo legislador na busca de um modelo regulatório que enderece corretamente as questões problemáticas atinentes ao reconhecimento facial, em especial em uma sociedade ainda fortemente marcada pelo racismo. A sociedade civil, em especial as entidades atuantes na defesa de igualdade racial, não pode ser negligenciada nesse processo.

REFERÊNCIAS

ABREU, Jacqueline de Sousa. *Tratamento de dados pessoais para a segurança pública: contornos do Regime Jurídico pós-LGPD*. In: In: DONEDA, Danilo (coord.); SARLET, Ingo Wolfgang (coord.); MENDES, Laura Schertel (coord.); RODRIGUES JUNIOR, Otavio Luiz (coord.) BIONI, Bruno Ricardo (coord.). *Tratado de Proteção de Dados Pessoais*. Rio de Janeiro: Forense, 2021. p. 598.

ACCESS NOW. *Ban Biometric Surveillance*. Access Now, 07 jun. 2021. Disponível em: https://www.accessnow.org/ban-biometric-surveillance. Acesso em: 4 out. 2021.

AEROPORTOS *testam sistema de reconhecimento facial para facilitar embarque*. Globo, 21 dez. 2020. Disponível em: https://g1.globo.com/economia/tecnologia/noticia/2020/12/21/aeroportos-testam-sistema-de-reconhecimento-facial-para-facilitar-embarque.ghtml. Acesso em: 15 de jun. 2021.

AMAZON *face-detection technology shows gender and racial bias, researchers say*. Cbs News, 25 jan. 2019. Disponível em: https://www.cbsnews.com/news/amazon-face-detection-technology-shows-gender-racial-bias-researchers-say/. Acesso em 26 de out. de 2021.

ANGWIN, JULIA. ET. AL. *Machine Bias:* There's software used across the country to predict future criminals. And it's biased against blacks. Pro Publica, 23 maio 2016. Disponível em: https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing. Acesso em: 12 fev. 2021

ANOTHER *Arrest, and Jail Time, Due to a Bad Facial Recognition Match*. Nytimes**.** Disponível em**:** https://www.nytimes.com/2020/12/29/technology/facial-recognition-misidentify-jail.html**.** Acesso em**:** 13 ago. 2021.

ARANHA, Mário Iório. *Manual de Direito Regulatório*: Fundamentos de Direito Regulatório. 3ª. ed. Londres: Laccademia Publishing, 2015. n.p. [E-book]

BAN FACIAL RECOGNITION. *Ban Facial Recognition.* Disponível em: https://www.banfacialrecognition.com. Acesso em: 4 out. 2021.

BANERJEE, Pradipta Kumar. DATTA, Asit Kumar. DATTA, Madhura. *Face Detection and Recognition:* Theory and Practice. Boca Raton, FL: Taylar & Francis Group, 2016.

BAUMAN, Zygmunt. LYON, David. *Vigilância líquida: diálogos com David Lyon*. Zahar, 2014. p. 5 a 17.

BIONI, Bruno Ricardo. *Proteção de dados pessoais:* a função e os limites do consentimento. Rio de Janeiro: Forense, 2019.

BIONI, Bruno Ricardo; LUCIANO, Maria. *O princípio da precaução na Regulação de Inteligência artificial:* seriam as leis de proteção de dados o seu pontal de entrada? In: FRAZÃO, Ana; MULHOLLAND, Catlin (Org). *Inteligência Artificial e direito*: ética, regulação e responsabilidade. São Paulo: Thomson Reuters Brasil, 2019, p.22.

BLEDSOE, W. BROWNING, I. *Pattern recognition and reading by machine*. IRE-AIEE-ACM computer conference (IRE-AIEE-ACM '59 (Eastern)). Association for Computing Machinery, New York, NY, USA, 225–232. DOI: https://doi.org/10.1145/1460299.1460326. 1959.

BONAT, Débora. HARTMANN PEIXOTO, Fabiano. *Racionalidade no Direito:* inteligência artificial e precedentes. 1ª ed. Alteridades, 2020. n.p.

BOYER, Robert S. *Automated Reasoning:* Essays in Honor of Woody Bledsoe. Kluwer Academic Publishers, 1991

BRASIL. *Guia de boas práticas*. Lei Geral de Proteção de Dados (LGPD). Comitê Central de Governança de Dados, 16 jun. 2021. Disponível em: https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/guias/guia_lgpd.pdf. Acesso em: 18 jan. 2021. p.54.

BRASIL. *Estratégia Brasileira de Inteligência Artificial* - EBIA. Ministério da Ciência, Tecnologia e Inovações. Disponível em: https://www.gov.br/mcti/pt-br/acompanhe-o-mcti/transformacaodigital/arquivosinteligenciaartificial/ia_estrategia_documento_referencia_4-979_2021.pdf. Acesso em: 7 out. 2021.

BRASIL. *PL nº 1.969/2021*. Câmara dos Deputados. Disponível em: https://www.camacra.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2284814. Acesso em: 7 out. 2021.

BRASIL. *PL nº 4.612/2019*. Câmara dos Deputados. Disponível em: https://www.camara.leg.br/propostas-legislativas/2216455. Acesso em: 12 out. 2021.

BRASIL. PL nº 12/2015. Câmara dos Deputados. Disponível em: https://www.camara.leg.br/propostas-legislativas/944254. Acesso em: 17 out. 2021

BRASIL. PL nº 4.060/2012. Câmara dos Deputados. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=548066. Acesso em: 3 de mar. 2022.

BRASIL. *Projeto de Lei sobre uso de Inteligência Artificial avança no Congresso*. Ministério da Economia. 29 set. 2021. Disponível em: https://www.gov.br/economia/pt-br/assuntos/noticias/2021/setembro/projeto-de-lei-sobre-uso-de-inteligencia-artificial-avanca-no-congresso. Acesso em: 7 out. 2021.

BRASIL. *Anteprojeto sobre uso de dados na segurança pública deve ficar pronto em novembro*. Agência Câmara de Notícias, 22 set. 2020. Disponível em: https://www.camara.leg.br/noticias/694562-anteprojeto-sobre-uso-de-dados-na-seguranca-publica-deve-ficar-pronto-em-novembro. Acesso em: 12 out. 2020.

BRASIL. *Mensagem nº 288*. Presidência da República, 8 de jul. 2019. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2019/Msg/VEP/VEP-288.htm. Acesso em: 8 dez. 2021.

BRASIL, *Emenda Constitucional nº 115*. Presidência da República, 10 fev. 2022. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/Emendas/Emc/emc115.htm#art1. Acesso em: 3 de mar. 2022.

CAO, Z. Yin, Q. ZHOU, E. *Naive-Deep Face Recognition:* Touching the Limit of LFW Benchmark or Not?. Cornell, 2015.

CITRON, Danielle Keats. *Technological Due Process*. Washington University Law Review. nº. 1249. Volume 85, 2008. Disponível em: https://openscholarship.wustl.edu/law_lawreview/vol85/iss6/2. Acesso em: 29 out. 2021.

CODED BIAS. Direção: Shalini Kantayya. Produção: Shalini Kantayya. Co-Produção: Sabine Hoffman. China, Estados Unidos, Gra Bretênia: 7ª Emire Media, 2020. *Streaming*.

COTE, Jackson. *Springfield City Council passes facial recognition moratorium*. Masslive, 25 fev. 2020. Disponível em: https://www.masslive.com/springfield/2020/02/springfield-city-council-passes-facial-recognition-moratorium.html. Acesso em: 4 out. 2021.

CRUMPLER, William. *How Accurate are Facial Recognition Systems* – and Why Does It Matter?. CSIS. 2020. Disponível em: https://www.csis.org/blogs/technology-policy-blog/how-accurate-are-facial-recognition-systems-%E2%80%93-and-why-does-it-matter. Acesso em: 20 de jun. 2021.

CRUMPLER, William. LEWIS, James A., *Questions about Facial Recognition*. Center For Strategic and International Studies (Csis), 2021. Disponível em: www.jstor.org/stable/resrep28766. Acesso em: 19 jun. 2021.

DINANT, J.-M., Lazaro, C., Poullet Y., Lefever, N. and Rouvroy, A. *Application of Convention 108 to the Profiling Mechanism* - Some ideas for the future work of the consultative committee (T-PD), Doc. T-PD 01, p. 3.

DEVICH-CYRIL, Malkia. *Defund Facial Recognition*. The Atlantic, 5 jun. 2020. Disponível em: https://www.theatlantic.com/technology/archive/2020/07/defund-facial-recognition/613771/. Acesso em: 30 set. 2021.

DOCUMENTO *de Identificação sofrerá mudança*. Ponto Inicial. Porto Alegre, RS. Agosto de 2006.

DONEDA, Danilo. *Panorama histórico da proteção de dados pessoais*. In: In: DONEDA, Danilo (coord.); SARLET, Ingo Wolfgang (coord.); MENDES, Laura Schertel (coord.); RODRIGUES JUNIOR, Otavio Luiz (coord.) BIONI, Bruno Ricardo (coord.). *Tratado de Proteção de Dados Pessoais*. Rio de Janeiro: Forense, 2021.

ECI nº (2021) 000001. *Initiative de la société civile en vue d'une interdiction des pratiques de surveillance biométrique de masse*. Site Oficial da União Européia, 1 de jul. 2021. Disponível em: https://europa.eu/citizens-initiative/initiatives/details/2021/000001_fr. Acesso em: 4 out. 2021.

Dr. EKMAN'S *Work*: A timeline of achievements. Disponível em: https://www.paulekman.com/about/paul-ekman. Acesso em: 08 jun. 2021.

EUBANKS, Virginia. *Automating Inequality:* How High-Tech Tools Profile, Police, and Punish the Poor. St. Martin's Press, 2018.

EUROPEAN DATA PROTECTION BOARD. *Parecer conjunto nº 05/2021 do EDPB e EDPS*, p.2. EDPB. Disponível em: https://edpb.europa.eu/system/files/2021-06/edpb-edps_joint_opinion_ai_regulation_en.pdf. Acesso em: 4 out. 2021.

FAVARO, Iasmine. VERGILI, Gabriela. RIELLI, Mariana. ZANATTA., Rafael et. al. *Banimento, moratória, regulação: os movimentos em torno do reconhecimento facial*. Observatório Privacidade – Dataprivacy BrasiL, 6 fev. 2020. Disponível em: https://www.observatorioprivacidade.com.br/2020/02/06/banimento-moratoria-regulacao-os-movimentos-em-torno-do-reconhecimento-facial. Acesso em: 4 out. 2021.

FERES JUNIOR, João; GERSHON, Debora; MEIRELES, Fernando. *A Produção Legislativa de Brancos e Negros na Câmara*. Observatório do Legislativo brasileiro, 15 fev. 2021. Disponível em: https://olb.org.br/a-producao-legislativa-de-brancos-e-negros-na-camara/. Acesso em: 17 out. 2021.

FORAGIDO *da Justiça é preso com ajuda do reconhecimento facial*. Uol, 20 mar. 2021. Disponível em: https://atarde.uol.com.br/bahia/salvador/noticias/2161780-foragido-da-justica-e-preso-com-ajuda-do-reconhecimento-facial. Acesso em: 15 jun. 2021.

FRAZÃO, Ana. *Dados, estatísticas e algoritmos. Perspectivas e riscos da sua crescente utilização*. Jota, 28 de jun. 2017. Disponível em: https://www.jota.info/opiniao-e-analise/colunas/constituicao-empresa-e-mercado/dados-estatisticas-e-algoritmos-28062017. Acesso em: 17 ago. 2021.

FRAZÃO, Ana. *Discriminação algorítmica. Compreendendo o que são os julgamentos algorítmicos e o seu alcance na atualidade. Parte I*. Jota, 16 jun. 2021. Disponível em: https://www.jota.info/opiniao-e-analise/colunas/constituicao-empresa-e-mercado/discriminacao-algoritmica-16062021?amp. Acesso em: 26 out. 2021.

FRAZÃO, Ana. *Fundamentos da proteção de dados pessoais. Noções introdutórias para a compreensão da importância da Lei Geral de Proteção de Dados*. In: TEMPEDINO, Gustavo, OLIVA, Milena. *Lei Geral de Proteção de Dados e duas repercussões no Direito brasileiro*. 2ª Edição. Thomson Reuters, Revista dos Tribunais, 2020.

FRAZÃO, Ana. *Objetivos e alcance da Lei Geral de Proteção de Dados*. In: TEMPEDINO, Gustavo, OLIVA, Milena. *Lei Geral de Proteção de Dados e duas repercussões no Direito brasileiro*. 2ª Edição. Thomson Reuters, Revista dos Tribunais, 2020.

FUJIMOTO, Mônica Tiemy, MATTIUZZO, Marcela, MENDES, Laura Schertel. *Discriminação Algorítmica à Luz da Lei Geral de Proteção de Dados*. In: DONEDA, Danilo (coord.); SARLET, Ingo Wolfgang (coord.); MENDES, Laura Schertel (coord.); RODRIGUES JUNIOR, Otavio Luiz (coord.) BIONI, Bruno Ricardo (coord.). *Tratado de Proteção de Dados Pessoais*. Rio de Janeiro: Forense, 2021.

GABBATT, Adam. MORRIS, Sam. *AI can tell Republicans from Democrats* – but can you? Take our quiz. The Guardian, 12 set. 2017. Disponível em: https://www.theguardian.com/technology/2017/sep/12/artificial-intelligence-republicans-democrats-quiz. Acesso em: 15 mar. 2022.

GREENE, Jay. *Microsoft won't sell police its facial-recognition technology, following similar moves by Amazon and IBM*. WASHINGTON POST, 11 jun. 2020. Disponível em: https://www.washingtonpost.com/technology/2020/06/11/microsoft-facial-recognition. Acesso em: 30 set. 2021.

GREEGARD, Samuel. *What is Artificial Intelligence & How Does It Work?*. Datamation, 24 maio 2019. Disponível em: https://www.datamation.com/artificial-intelligence/what-is-artificial-intelligence. Acesso em: 27 jan. 2022.

GROSS, Ralph et al. *Multi-PIE*. 2008 8th IEEE International Conference on Automatic Face & Gesture Recognition, 2008, pp. 1-8, doi: 10.1109/AFGR.2008.4813399.

GUARIGLIA, Mathew. *Victory! California Governor Signs A.B. 1215*. Eletronic Frontier Foundation, 9 out. 2019. Disponível em: https://www.eff.org/deeplinks/2019/10/victory-california-governor-signs-ab-1215. Acesso em: 4 out. 2021.

HARTMANN PEIXOTO, Fabiano. *Direito e Inteligência artificial*. Coleção Inteligência Artificial e Jurisdição. Volume 2. DR.IA. Brasília, 2020. https://orcid.org/0000-0002-6502-9897. ISBN nº 978-65-00-08585-3. Disponível em: http://www.dria.unb.br. doi: 10.29327/521174. p. 26.

HARTMANN PEIXOTO, Fabiano. *Inteligência artificial e direito:* convergência ética e estratégica. 1ª ed. Curitiba: Alteridade Editora, 2020. p. 192.

HEILWEIL, Rebecca. *Why it matters that IBM is getting out of the facial recognition business*. Vox, 10 jun. 2020. Disponível em: https://www.vox.com/recode/2020/6/10/21285658/ibm-facial-recognition-technology-bias-business. Acesso em: 30 set. 2021.

HERRERA, Sebastian. *Tech Giants' New Appeal to Governments:* Please Regulate Us. Wall Street Journal. 27 jan. 2020. Disponível em: https://www.wsj.com/articles/tech-giants-new-appeal-to-governments-please-regulate-us-11580126502. Acesso em: 7 out. 2021.

HIGHEST *to Lowest* - Prison Population Total. WPB – World Prison Brief. Disponível em: https://www.prisonstudies.org/highest-to-lowest/prison-population-total?field_region_taxonomy_tid=All. Acesso em: 11 fev. 2022.

INSTITUTO IGARAPÉ. *Reconhecimento facial no Brasil*. Instituto Igarapé. Disponível em: https://igarape.org.br/infografico-reconhecimento-facial-no-brasil. Acesso em: 15 jun. 2021.

INSTITUTO DE REFERÊNCIA EM INTERNET E SOCIEDADE. *Inteligência Artificial no Brasil:* a Estratégia Brasileira de Inteligência Artificial (EBIA) e o Projeto de Lei nº 21/2020. Irisbh, 5 out. 2021. Disponível em: https://irisbh.com.br/inteligencia-artificial-no-brasil-a-estrategia-brasileira-de-inteligencia-artificial-ebia-e-o-projeto-de-lei-no-21-2020/. Acesso em: 12 out. 2021.

JOBIN, Nelson Franco. *Sob o olhar do Grande Irmão:* Recursos eletrônicos ajudam o Estado a fiscalizar seus cidadãos e emprestam à democracia britânica um sombrio manto solitário. Jornal do Brasil. Rio de Janeiro: 2 ago. 1998. p. 17.

Kashmir, Hill. *The Secretive Company That Might End Privacy as We Know It*. The New York Times, New York. 18 jan. 2020. Disponível em: https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html. Acesso em: 18 ago. 2021.

KRUEGLE, Herman. *CCTV surveillance:* analog and digital video practices and technology. 2ª ed. Elsevier, 2007. p. 9 e 14-16

LABORATÓRIO DE POLÍTICAS PÚBLICAS E INTERNET. *Nota Técnica Substitutivo ao PL 21/2020*. LAPIN, 28 set. 2021. Disponível em: http://lapin.org.br/2021/09/28/nota-tecnica-pl-21-2020/. Acesso em: 12 out. 2021.

LANDA, Manuel de. *War in the Age of Intelligent Machines*. New York: Zone Books, 1991.

LARSON, Ron. FARBER, Betsy. *Estatística aplicada*. Tradução: Luciane Ferreira Pauleti Vianna. 4ª ed. São Paulo: Person Prentice Hall, 2010.

LEVIN, Sam. *New AI can guess whether you're gay or straight from a photograph*. The Guardian, 8 set. 2017. Disponível em: https://www.theguardian.com/technology/2017/sep/07/new-artificial-intelligence-can-tell-whether-youre-gay-or-straight-from-a-photograph. Acesso em: 15 mar. 2022.

LINDOSO, Maria Cristine Branco. *Discriminação de gênero no tratamento automatizado de dados pessoais* – Como a automatização incorpora vieses de gênero e perpetua a discriminação de mulheres. Rio de Janeiro: Processo, 2021.

LILLY, Jacob R. *Nation Security at What Price?* A Look into Civil Liberty Concerns in the Information Age under the USA Patriot Act In: *Information ethics*: privacy, property, and power. Edited by Adam D. Moore. 1. ed. Seattle and London: University of Washington Press, 2005. p. 417.

MARKLEY *lead colleagues on legislation to ban government use of facial recognition, other biometric technology*. MARKEY, 15 jun. 2021. Disponível em: https://www.markey.senate.gov/news/press-releases/senators-markey-merkley-lead-colleagues-on-legislation-to-ban-government-use-of-facial-recognition-other-biometric-technology. Acesso em: 4 out. 2021.

MARKOFF, John. *Remember Big Brother? Now he's a company man*. The New York Times, 31 jan 1991. Disponível em: https://www.nytimes.com/1991/03/31/weekinreview/ideas-trends-remember-big-brother-now-he-s-a-company-man.html. Acesso em: 15 mar. 2022.

MAYER-SCHÖNBERGER, Viktor. CUKIER, Keneth. *Big Data:* the essential guide to work, life and learning in the age of insight. London: John Murray Publishers, 2017

MAYER-SCHÖNBERGER, Viktor. CUKIER, Keneth. *Big Data:* como extrair volume, variedade, velocidade e valor da avalanche de informação cotidiana. Tradução: Paulo Polzonoff Junior. 1. ed. Rio de Janeiro: Elsevier, 2013. p. 37.

MAZUI, Guilherme. *"No Brasil, não existe racismo", diz Mourão sobre assassinato de homem negro em supermercado.* Portal G1, 20 nov. 2020. Disponível em:

https://g1.globo.com/politica/noticia/2020/11/20/mourao-lamenta-assassinato-de-homem-negro-em-mercado-mas-diz-que-no-brasil-nao-existe-racismo.ghtml . Acesso em: 23 ago. 2021.

MENDES, Laura Schertel. *Privacidade, Proteção de dados e defesa do consumidor:* linhas gerais de um novo direito fundamental. São Paulo: ed. Saraiva. 2014. n.p.

MENKE, Fabiano. *A proteção de dados e o direito fundamental à garantia da confidencialidade e da integridade dos sistemas técnico-informacionais no direito alemão*. In. Revista Jurídica Luso Brasileira, Lisboa, Ano 5 (2019), nº1. p. 701-809. 2019.

MILENA, Lilian. *Kabengele Munanga, o antropólogo que desmistificou a democracia racial no Brasil*. Carta Maior, 15 maio 2019. Disponível em: https://www.cartamaior.com.br/?/Editoria/DireitosHumanos/Kabengele-Munanga-o-antropologo-quedesmistificou-a-democracia-racial-no-Brasil/5/44091. Acesso em: 23 ago. 2021.

MUNANGA, Kabengele. *Teoria social e relações raciais no Brasil contemporâneo*. Cadernos Penesb, Niterói, n. 12, 2010. p. 169-203. Disponível em: https://www.mprj.mp.br/documents/20184/172682/teoria_social_relacoes_sociais_brasil_contemporaneo.pdf. Acesso em: 23 ago. 2021.

The NEW YORK STATE SENATE. *Assembly Bill A6787D. 2019-2020 Legislative Session.* The New York State Senate. Disponível em: https://www.nysenate.gov/legislation/bills/2019/a6787. Acesso em: 4 out. 2021.

NUMBER *of Internet users, 2017*. Our World In Data. Disponível em: https://ourworldindata.org/grapher/internet-users-by-world-region?time=1990..latest&country=Europe+%26+Central+Asia~East+Asia+%26+Pacific~Latin+America+%26+Caribbean~South+Asia~North+America~Middle+East+%26+North+Africa~Sub-Saharan+Africa. Acesso em: 15 jun. 2021.

NOBLE, Safiya. *Algorithms of oppression:* how search engines reinforce racism. New York: New York University Press, 2018.

NUNES, Pablo. *O algoritmo e racismo nosso de cada dia*: Reconhecimento facial aposta no encarceramento e pune preferencialmente população negra. PIAUÍ, 2 jan. 2021. Disponíel em: https://piaui.folha.uol.com.br/o-algoritmo-e-racismo-nosso-de-cada-dia. Acesso em: 24 jul. 2021.

NUNES, Pablo. *Exclusivo: levantamento revela que 90,5% dos presos por monitoramento facial no Brasil são negros*. The Intercept Brasil. 21 nov. 2019. Disponível em: https://theintercept.com/2019/11/21/presos-monitoramento-facial-brasil-negros/. Acesso em: 19 ago. 2021.

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

O'NEIL, Cathy. *Algoritmos de destruição em massa:* como o big data aumenta a desigualdade e ameaça à democracia. 1ª edição. Tradução: Rafael Abraham, Santo André, SP: Ed. Rua do Sabão, 2020.

OMRON *Announces "OKAO Vision Face Recognition Sensor",World's First Face Recognition Technology for Mobile Phones*. 28 fev. 2005. Disponível em: https://www.omron.com/global/en/media/press/2005/02/n_280205.html. Acesso em: 11 jun. de 2021.

O'REILLY, Tim. *What Is Web 2.0:* Design Patterns and Business Models for the Next Generation of Software. O'REILLY, 30 set. 2005. Disponível em: https://www.oreilly.com/pub/a/web2/archive/what-is-web-20.html?page=1. Acesso em: 21 out. 2021.

ORWELL, George. *1984*. Tradução: Claudio Carina, Sonia Carvalho. São Paulo: Citadel, 2021.
NG, Alfred. *How China uses facial recognition to control human behavior*. Cnet, 11 ago. 2020. Disponível em: https://www.cnet.com/news/in-china-facial-recognition-public-shaming-and-control-go-hand-in-hand/. Acesso em: 4 out. 2021.

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

PASQUALE, Frank. *Algorithms are producing profiles of you. What do they say? You probably don't have the right to know*. Disponível em: https://aeon.co/essays/judge-jury-and-executioner-the-unaccountable-algorithm. Acesso em: 8 dez. 2021.

PRECONCEITO racial como o maior fator de desemprego. O Jornal, Rio de Janeiro, 14 jun. 1959. Segunda Seção. p. 9. Disponível em: http://memoria.bn.br/DocReader/110523_05/76038. Acesso em: 22 de ago. 2021

PROJETO *de marco legal da IA no Brasil é pouco consistente e pode ser inútil, dizem especialistas*. Jornal Unesp. 29 jul. 2021. Disponível em: https://jornal.unesp.br/2021/07/29/projeto-de-marco-legal-da-ia-no-brasil-e-pouco-consistente-e-pode-ser-inutil-dizem-especialistas/. Acesso em: 12 out. 2021.

PENTLAND, Alex. TURK, Matthew. *Eigenfaces for Recognition*. J Cogn Neurosci 1991; 3 (1): 71–86. Disponível em: https://doi.org/10.1162/jocn.1991.3.1.71. Acesso em: 5 jun. 2021.

RAMOS, Silvia (coord.). *Retratos da Violência* – Cinco meses de monitoramento, análises e descobertas. Rio de Janeiro: Rede de Observatórios da Segurança/CESeC, nov. 2019. p. 69.

REICH, Robert B. *Supercapitalismo*: como o capitalismo tem transformado os negócios, a democracia e o cotidiano. Rio de Janeiro: Elsevier, 2008.

RESOURCE CENTRE. *Yahoo! lawsuit (re China)*. Business & Human Rights, 1 abr. 2007. Disponível em: https://www.business-humanrights.org/en/latest-news/yahoo-lawsuit-re-china. Acesso em: 11 fev. 2022.

RIBEIRO, Djamila. *Discutir democracia é discutir antirracismo*. Roda Viva - Tv Cultura, 9 nov. 2020. Disponível em: https://www.youtube.com/watch?v=jn1AtnzTql8. Acesso em: 29 out. 2021.

RODOTÀ, Stefano. *A vida na sociedade de vigilância* – a privacidade hoje. Organização, seleção e apresentação de Maria Celina Bodin de Moraes. Tradução: Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008.

ROSE, Adam. *Are Face-Detection Cameras Racist?*. Time, 22 jan. 2010. Disponível em: http://content.time.com/time/business/article/0,8599,1954643,00.html. Acesso em: 18 ago. 2021.

RUARO, Regina Linden. SARLET, Gabrielle B. Sales. *O direito fundamental à proteção de dados sensíveis no sistema normativo brasileiro*: uma análise acerca das hipóteses de tratamento e da obrigatoriedade do consentimento livre, esclarecido e informado sob o enfoque da Lei Geral de Proteção de Dados (LGPD) – Lei 13.709/2018. In: DONEDA, Danilo (coord.); SARLET, Ingo Wolfgang (coord.); MENDES, Laura Schertel (coord.); RODRIGUES JUNIOR, Otavio Luiz (coord.) BIONI, Bruno Ricardo (coord.). *Tratado de Proteção de Dados Pessoais*. Rio de Janeiro: Forense, 2021. p. 182

SCHWABE, Hürgen. MARTINS, Leonardo. *Cinquenta anos de Jurisprudência do Tribunal Constitucional Alemão*. Montevideo: Konrad Adenauer Stiftung, 2005. p. 237.

SÃO PAULO. Tribunal de Justiça de São Paulo. 17ª Câmara de Direito Privado de Justiça do Tribunal de São Paulo. Apelação Cível nº 1005329-07.2021.8.26.0077. Apelante: Banco C6 Consignado S/A. Apelada: Cleia Braga Silva. Afonso Bráz. Relator: São Paulo, 20 jan. 2022.

SILVA, Mariah Rafaela. VARON, Joana. *Reconhecimento Facial no Setor Público e Identidade Trans*: tecnopolíticas de controle e ameaça à diversidade de gênero em suas interseccionalidades de raça, classe e território. Coding Rights, 27 de jan. 2021. Disponível em: https://codingrights.org/docs/rec-facial-id-trans.pdf. Acesso em: 03 de mar. 2022.

SILVA, Tarcizio. *Racismo Algorítmico*: Inteligência artificial e discriminação nas redes digitais. São Paulo: Edições Sesc SP, 1ª ed. 2022. n.p. [*E-book*].

SILVA, Tarcizio. *Racismo Algorítmico em Plataformas Digitais*: microagressões e discriminação em código. Disponível em: https://lavits.org/wp-content/uploads/2019/12/Silva-2019-LAVITSS.pdf. Acesso em: 10 mar. 2022.

SIMONITE, Tom. *Behind the Rise of China's Facial-Recognition Giants*. Wired, 8 mar. 2019. Disponível em: https://www.wired.com/story/behind-rise-chinas-facial-recognition-giants. Acesso em 04 out. 2021.

SOLOVE, Daniel J. *The Digital Person:* technology and privacy in the information age. Ex. Machina, 2004

SOLOVE, Daniel J. *Why Privacy Matters Even if You Have "Nothing to Hide"*. The Chronicle Of Higher Education, 15 maio 2011. Disponível em: http://www.uvm.edu/~dguber/POLS21/articles/solove.htm. Acesso em: 16 de out. 2021.

SHEAD, Sam. *Chinese residents worry about rise of facial recognition*. BBC, 5 dez. 2019. Disponível em: https://www.bbc.com/news/technology-50674909. Acesso em: 4 out. 2021.

SHENZHEN, Chai Hua in. *Nation to set up standard for facial recognition technology*. China Daily, 11 dez. 2019. Disponível em: https://global.chinadaily.com.cn/a/201912/11/WS5df043b6a310cf3e3557d50c.html. Acesso em: 4 out. 2021.

STAN, L. JAIN, Anil K. *Introduction. In: Handbook of Face Recognition*. Edited by STAN, L. JAIN, Anil K. 2ª ed. London: Springer. 2011.

TAVARES, Giovanna Milanez. *O tratamento de dados pessoais disponíveis publicamente e os limites impostos pela LGPD*. Rio de Janeiro: Editora Processo. 2022.

UNITED NATIONS. *Impact of new technologies on the promotion and protection of human rights in the context of assemblies, including peaceful protests: Report of the United Nations High Commissioner for Human Rights*. United Nations, 24 jun. 2020. p. 15. Disponível em: https://undocs.org/A/HRC/44/24. Acesso em: 30 set. 2021.

UNITED STATES OF AMERICA. *Diversity in high tech*: Executive Summary. U.s. Equal Employment Opportunity Comission. Disponível em: https://www.eeoc.gov/special-report/diversity-high-tech. Acesso em: 24 jul. 2021.

UNITED STATES OF AMERICA. *House hearing, 116th congress - Facial Recognition Technology:* part i its impact on our civil rights and liberties. Govinfo, 22 maio 2019. Disponível em: https://www.govinfo.gov/app/details/CHRG-116hhrg36663/summary. Acesso em: 17 out. 2021.

UNITED STATES OF AMERICA. *House Lawmakers Release Anti-Monopoly Agenda for "A Stronger Online Economy: Opportunity, Innovation, Choice"*. House of Representatives, 11 jun. 2022. Disponível em: https://judiciary.house.gov/news/documentsingle.aspx?DocumentID=4591. Acesso em: 8 mar. 2022.

WROE, David. *Top official's 'golden rule': in border protection, computer won't ever say no*. The Sydney Morning Herald, 13 jul. 2018. Disponível em: https://www.smh.com.au/politics/federal/top-official-s-golden-rule-in-border-protection-computer-won-t-ever-say-no-20180712-p4zr3i.html. Acesso em: 8 dez. 2021.

ZUBBOF, Shoshana. *A Era do Capitalismo de Vigilância*. Editora Intrínseca. 1ª ed. 2021.