UNIVERSIDADE FEDERAL DO RIO DE JANEIRO - UFRJ

CENTRO DE CIÊNCIAS JURÍDICAS E ECONÔMICAS - CCJE

FACULDADE NACIONAL DE DIREITO - FND

ISABELLE CRISTINE SOARES ANTONIO

DIREITO À PRIVACIDADE EM RISCO? REFLEXÕES SOBRE O AVANÇO DAS TECNOLOGIAS DE RECONHECIMENTO FACIAL PELA SEGURANÇA PÚBLICA NO BRASIL

RIO DE JANEIRO

2022

ISABELLE CRISTINE SOARES ANTONIO

DIREITO À PRIVACIDADE EM RISCO? REFLEXÕES SOBRE O AVANÇO DAS TECNOLOGIAS DE RECONHECIMENTO FACIAL PELA SEGURANÇA PÚBLICA NO BRASIL

Monografia de final de curso, elaborada no âmbito da graduação em Direito da Universidade Federal do Rio de Janeiro, como pré-requisito para obtenção do grau de bacharel em Direito, sob a orientação do **Professor Dr. Carlos Alberto Pereira das Neves Bolonha.**

RIO DE JANEIRO

2022

CIP - Catalogação na Publicação

S933d

Soares, Isabelle
DIREITO À PRIVACIDADE EM RISCO? REFLEXÕES SOBRE O AVANÇO DAS TECNOLOGIAS DE RECONHECIMENTO FACIAL PELA SEGURANÇA PÚBLICA NO BRASIL / Isabelle Soares. - Rio de Janeiro, 2022.
69 f.

Orientador: Carlos Alberto Pereira das Neves Bolonha.
Trabalho de conclusão de curso (graduação) - Universidade Federal do Rio de Janeiro, Faculdade Nacional de Direito, Bacharel em Direito, 2022.

1. Direito à Privacidade. 2. Big Data . 3. Segurança Pública. 4. Biometria Facial. 5. Vigilância. I. Pereira das Neves Bolonha, Carlos Alberto , orient. II. Título.

Elaborado pelo Sistema de Geração Automática da UFRJ com os dados fornecidos pelo(a) autor(a), sob a responsabilidade de Miguel Romeu Amorim Neto - CRB-7/6283.

ISABELLE CRISTINE SOARES ANTONIO

DIREITO À PRIVACIDADE EM RISCO? REFLEXÕES SOBRE O AVANÇO DAS TECNOLOGIAS DE RECONHECIMENTO FACIAL PELA SEGURANÇA PÚBLICA NO BRASIL

Monografia de final de curso, elaborada no âmbito da graduação em Direito da Universidade Federal do Rio de Janeiro, como pré-requisito para obtenção do grau de bacharel em Direito, sob a orientação do Professor Dr. Carlos Alberto Pereira das Neves Bolonha.

Data da Aprovação: __ / __ / ____.

Banca Examinadora:

_____

Orientador

_____

Membro da Banca

_____

Membro da Banca

_____

AGRADECIMENTOS

Sempre tive o sonho de estudar na UFRJ, embora não tivesse ciência de qual carreira seguir. Concretizei o sonho aos 17 anos, no curso Engenharia de Alimentos, mas após dois longos anos, não me identifiquei com o curso. Lutei para continuar na área, pois jamais me imaginei fora do campo das engenharias e ciências da natureza, todavia, cá estou eu, me formando em Direito, ouvindo de pessoas queridas que a veia jurídica dentro de mim, era nítida para eles, menos para mim.

Diante disso, só tenho a agradecer, primeiramente a Deus por me trazido a este curso, pois sem Ele, nada disso seria possível.

Agradeço também aos meus amados pais, Anderson e Aparecida, que investiram na minha educação, me deram todo o suporte emocional, financeiro e material, e sempre me motivaram a seguir atrás dos meus sonhos apesar das dificuldades. Esta conquista, eu carrego junto a vocês e este é, certamente, um dos meus maiores orgulhos nesta terra!

Não posso deixar de agradecer ao meu esposo, Luciano, aquele que me apoiou e esteve ao meu lado desde o início deste curso, desde quando ainda éramos namorados. Inclusive, estando ao meu lado no dia em que efetuei a matrícula, infestada pelo medo de odiar este curso que entrei, quase que por um acaso.

Agradeço a todos os professores de todas as fases da minha vida, que deixaram “o conhecimento”, uma grande preciosidade, em minha vida e que muitas vezes não permitiram que eu desistisse quando eu mesma pensava que não era possível.

Por fim, agradeço à UFRJ que me proporcionou amizades incríveis e o contato com pessoas queridas e inspiradoras, além de momentos especiais que ficarão para sempre em minha memória.

“*Era terrivelmente perigoso permitir que os pensamentos vagassem quando se estava em um lugar público ou ao alcance de uma teletela. A menor coisa poderia delatá-lo. Um tique nervoso, um olhar inconsciente de ansiedade, o costume de falar sozinho; qualquer coisa que sugerisse anormalidade, ou algo a esconder. De todo modo, ter uma expressão imprópria (parecer incrédulo quando anunciavam uma vitória, por exemplo) era em si uma ofensa passível de punição. Existia até uma palavra para isso em Novidioma: crimefacial”.*

(George Orwell, 1984)

RESUMO E PALAVRAS-CHAVE

Busca-se apresentar reflexões acerca do uso das tecnologias de reconhecimento facial pela segurança pública brasileira, pensando sobre seus impactos no direito à privacidade dos cidadãos. Através de referenciais teóricos relacionados ao direito à privacidade, à discriminação algorítmica e à vigilância por meio da retenção de dados biométricos pelo poder público, e, tendo como base, a perspectiva histórica do direito à privacidade, as premissas básicas sobre a atuação das novas tecnologias de inteligência artificial, bem como a noção dos conceitos de sociedade e capitalismo de vigilância, visou-se refletir se as novas tecnologias possuem vieses e, se sim, quais efeitos sobre a população, elas trazem consigo quando são implementadas. Portanto, o presente trabalho pretende debater os impactos que as tecnologias de reconhecimento facial podem implicar na sociedade, em especial sobre pessoas marginalizadas, sob o pretexto da preservação segurança. No mais, a pesquisa realizada foi a bibliográfica, no método hipotético-dedutivo e qualitativo.

Palavras-chave: Direito à Privacidade; Vigilância; Biometria Facial; Segurança Pública; Big Data.

ABSTRACT AND KEYWORDS

It seeks to present reflections on the use of facial recognition technologies by Brazilian public security, thinking about its impacts on citizens' right to privacy. Through theoretical references related to the right to privacy, algorithmic discrimination, and surveillance through the retention of biometric data by the government, and, based on the historical perspective of the right to privacy, the basic premises on the performance of new technologies of artificial intelligence, as well as the notion of the concepts of surveillance society and capitalism, the aim was to reflect on whether new technologies have biases and, if so, what effects on the population they bring with them when they are implemented. Therefore, the present work intends to discuss the impacts that facial recognition technologies should have on society, especially on marginalized people, under the pretext of preserving security. In addition, the research carried out was bibliographic, in the hypothetical-deductive and qualitative methods.

Keywords: Right to Privacy; Surveillance; Facial Biometrics; Public security; big data

SUMÁRIO

INTRODUÇÃO

O direito constitucional à privacidade sofreu ao longo do tempo muitas intervenções em razão do advento das tecnologias, conforme o último avança, mais busca-se limitar ou proteger o primeiro. Atualmente, em especial, por meio do uso dos dados, a privacidade dos indivíduos ao redor do mundo tem sido mitigada, não somente pelas empresas privadas, sob a premissa, mas não somente, de obter conhecimento sobre o comportamento do indivíduo com fins até então comerciais, mas também pelos Governos, aos quais em nome da segurança e guerra a criminalidade, buscam propostas para monitorar cada vez mais seus cidadãos, sem estes, terem ciência de como esta vigilância irá acontecer.

Em torno da utilização dos dados pelas "Big Techs", as empresas de tecnologia que dominam o mercado mundial, como, por exemplo, a Google, a Meta, outrora Facebook, que abarca o conglomerado WhatsApp, Facebook e Instagram, discute-se sobre a forma como estas empresas utilizam os dados de seus usuários, tendo em vista a falta de transparência nos processos de recolhimento, tratamento, guarda e descarte dos dados pessoais. Esta sensação de insegurança frente a retenção de dados por essas empresas, pode ter como um dos motivos, a falta de compreensão e conhecimento técnico por parte da população.

Com o escândalo ocorrido entre o Facebook, Donald Trump (ex-presidente dos Estados Unidos) e a Cambridge Analítica [1]— na qual a empresa utilizou os dados dos usuários da rede social, Facebook, criando perfis psicológicos de cada um deles, no intuito de direcionar, através dos algoritmos, mídias e anúncios para influenciar as suas opções de voto nas eleições presidenciais, favorecendo Donald Trump em face de outros candidatos — o debate acerca da utilização dos dados dos usuários por essas empresas se tornou mais sério e latente na sociedade. Uma das razões está na discussão sobre o possível impacto que os algoritmos poderiam causar no comportamento de um indivíduo e afetar toda uma coletividade, não somente em situações

[1] Escândalo de dados entre a rede social Facebook e a empresa Cambridge Analytica — "Foi o escândalo em que houve o vazamento de dados, através da venda, de mais de 50 milhões de usuários da rede social Facebook, obtendo dados não só daqueles que participavam da pesquisa comportamental na rede, mas também de todos os amigos do perfil, sem consentimento das vítimas, para a Cambridge Analytica, empresa que integrou o time de campanha do ex-Presidente Donald Trump, nas eleições de 2016. A empresa que tinha seu negócio voltado à mineração e análise de dados, utilizou os dados, catalogando os seus usuários e disseminando, de forma personalizada, propaganda política positiva em favor de Trump e negativas sobre a adversária do candidato. Este direcionamento de conteúdo tinha o intuito de manipular o comportamento dos eleitores e torná-los mais propensos a probabilidade de serem convencidos (G1, 2018).

simples como ver necessidade, que antes não havia, em comprar um determinado produto, mas, também em situações complexas como na escolha de um candidato político durante as eleições.

Em contrapartida, ainda no âmbito da privacidade e uso de dados, os Estados têm utilizado mais frequentemente as novas tecnologias, em especial, as tecnologias de inteligências artificiais (AI) no intuito de vigiar os cidadãos através da utilização de AI de geolocalização e de biometria (facial e digital). Aparentemente, com a intenção primaz de proteger a segurança dos cidadãos em face da criminalidade, ainda assim, questiona-se se deveria o Estado ter acesso irrestrito a vida privada dos indivíduos.

O governo da República Popular da China, durante a pandemia do coronavírus, instalou câmeras na entrada da casa dos seus cidadãos monitorando os seus acessos, não somente através da geolocalização em aparelhos “smartphones” e bilhões de câmeras de reconhecimento facial, mas também por meio dos agentes do aparelho de repressão do Estado (BBC NEWS BRASIL, 2020; CNN BRASIL, [s.d.]).

Embora o comportamento institucional chinês tenha sofrido críticas por ativistas de direitos humanos (HUMAN RIGHTS WATCH, 2020), alguns países demonstraram interesse neste meio de controle, pois, apesar das acusações de “violações de direitos”, houve a preservação de outros, a saúde e a segurança coletiva, tendo em vista que em poucas semanas o país conseguiu reduzir os casos de contaminação da ordem de milhares para zero em menos de dois meses (BBC NEWS BRASIL, 2020).

Em consonância ao projeto de monitoramento para fins de segurança, no Brasil, segundo matéria da EBC, somente em 2019 já havia 37 cidades que já estavam recorrendo à tecnologia de reconhecimento facial no intuito de reprimir crimes, identificar criminosos, veículos roubados, desaparecidos etc. (AGÊNCIA BRASIL, 2019). Porém, com este crescimento, emergem outras preocupações, pois não são raros, a título de exemplificação, os casos em que pessoas sem qualquer relação com atos criminosos são presas injustamente através do reconhecimento facial nas cidades brasileiras sem o uso destas tecnologias. Igualmente, também foram identificados os mesmos erros no uso da tecnologia de biometria facial para esses fins, e, majoritariamente, tal erro é cometido com principalmente com pessoas não-brancas (AGÊNCIA BRASIL, 2021; BBC MUNDO, 2017).

Ao passo que esta tecnologia avança em território nacional tornando-as cada vez mais em sociedades de vigilância, não só por empresas privadas, mas, em especial, pelas instituições públicas brasileiras, questiona-se se o direito fundamental à privacidade se encontra sob risco

em troca da promessa de mais “segurança”, em especial, nos casos de reconhecimento facial. Seria a mitigação deste direito autônomo um preço válido a se pagar em troca da possibilidade de menos criminalidade nos estados brasileiros?

Logo, o objetivo geral deste trabalho visa refletir se o uso das novas tecnologias, em especial de reconhecimento facial, pelo Estado, para fins de vigilância, pode pôr em risco o direito à privacidade dos cidadãos. A metodologia de pesquisa utilizada classifica-se em pesquisa bibliográfica, descritiva, qualitativa, com finalidade teórica.

Por fim, os objetivos específicos consistem em observar as perspectivas históricas da tutela do direito à privacidade na história moderna, estabelecer premissas básicas acerca do que são as tecnologias de inteligência artificial (AI) e se elas são dotadas de plena neutralidade em suas determinações; refletir brevemente sobre sociedade e capitalismo de vigilância; investigar se existem normas específicas que regulam o uso das tecnologias de reconhecimento facial em âmbito nacional, pelo Estado; e apresentar casos concretos no uso da biometria facial pelo Estado para fins de persecução penal.

Assim, com estes objetivos em mente, pretende-se, no capítulo seguinte, apresentar a história moderna do direito à privacidade e as circunstâncias que levaram as suas modificações, do entendimento como direito de primeira geração; a sua perspectiva mais ampla, exigindo-se a atuação do Estado; ao olhar coletivo da proteção da privacidade e ao momento que nos encontramos atualmente, onde preza-se, também, pela garantia da democracia.

Igualmente, no mesmo capítulo, são apresentados, brevemente, as tentativas de conceituação do direito à privacidade e suas ramificações – direito à vida privada, intimidade, honra e imagem - sob o olhar da Constituição Federal brasileira de 1988.

No terceiro capítulo são apresentadas as premissas básicas sobre os termos relacionados ao universo da tecnologia, a saber, “big data”, algoritmos, biometria facial, inteligência artificial, internet das coisas, dentre outros. Também, neste tópico, algumas problematizações acerca do uso destas máquinas, bem como seus impactos no cotidiano dos indivíduos inseridos em uma sociedade, são iniciadas.

O Capitalismo de Vigilância discutido por Shoshana Zuboff e a Sociedade de Vigilância discutida por Stéfano Rodotà também compõem o assunto do terceiro capítulo. Adicionalmente, algumas considerações de Zygmunt Bauman e Michel Focault também integram a discussão

deste capítulo, pois trazem perspectivas sobre poder, privacidade e controle que estão diretamente ligados ao contexto de vigilância.

No quarto capítulo, iniciam-se as reflexões sobre o uso das tecnologias de reconhecimento facial, não apenas pelo Estado, mas também por meio de empresas privadas através de apps das grandes “big techs”. Neste capítulo, a discussão iniciada no capítulo anterior acerca da suposta neutralidade das máquinas, tem como recorte o racismo algorítmico e o viés racial destes sistemas. Casos reais são apresentados e o debate sobre a segurança da implementação desta tecnologia para fins de segurança pública, principalmente quando se considera pessoas “não-brancas” é fomentado.

Por fim, no último capítulo, o concentra-se no uso da biometria facial para fins de segurança pública pelo Estado, em território nacional. São expostos alguns casos concretos recentes, o crescimento destes projetos nas cidades brasileiras em poucos anos, e a ausência de legislação específica para tratar do tema, pois, conforme será visto, a Lei Geral de Proteção de Dados, por si só, não é suficiente para tutelar esta matéria.

1. HISTÓRIA MODERNA E CONCEITUAÇÃO DO DIREITO À PRIVACIDADE

No século XIX, a publicação do artigo "The Right to Privacy" por Warren e Brandeis, foi considerado um grande marco do Direito à Privacidade como um instituto jurídico para a doutrina (CANCELIER, 2017, p. 5; FARIAS; FRANCA, 2017, p. 295), em 1890, na *Harvard Law Review*, nos Estados Unidos. Embora houvesse movimentos "preanunciando" o surgimento do que seria o direito à privacidade, foi este artigo que impulsionou o movimento para a visão autônoma deste direito e que, consequentemente, culminou no seu reconhecimento ao status constitucional (BASTOS; PANTOJA; SANTOS, 2021, p. 5; CANCELIER, 2017, p. 5).

A circunstância que teria motivado a construção do artigo, originou-se em razão da divulgação de diversos acontecimentos íntimos ocorridos no casamento da filha de Samuel Warren, publicados nas mídias da época sem qualquer anuência dos interessados (CANCELIER, 2017, p. 5). Na ocasião, fotos da celebração do matrimônio, bem com outros fatos acerca do evento, foram divulgadas em uma matéria jornalística. Assim, os autores viram como necessidade a defesa da proteção da privacidade sob tutela do direito estadunidense (FARIAS; FRANCA, 2017, p. 295).

No mesmo período, outros dois casos nos Estados Unidos, em 1893, também foram relevantes por marcarem os primeiros casos do direito à imagem relacionando ao direito à privacidade, sendo o primeiro, *Mark v. Jaffa*, o qual "culminou no deferimento de uma liminar que visava restringir a publicação da foto do autor do jornal do réu, em um concurso de votação popular" e o caso *Corliss v. Walker*, julgado pelo juiz Colt, onde ele não "concedeu a liminar para restringir a publicação e a venda de um esboço biográfico de George Henry Corliss, engenheiro e inventor, bem como a impressão e a venda de sua fotografia" (BATISTA, 2017b, p. 17).

Ao contrário do primeiro caso, o magistrado entendeu que "Corliss era um homem público que não poderia ter reivindicado tal direito em vida e que, portanto, este também não era passível de ser reivindicado por sua família após sua morte [2]" (BATISTA, 2017b, p. 17).

[2] Neste caso, "o juiz decidiu que Independentemente da questão contratual, creio que a lei seja a de que um indivíduo privado tenha o direito de ser protegido na representação de seu retrato sob qualquer forma, esta sendo uma propriedade, bem como um direito pessoal e pertence à mesma classe de direitos que proíbe a reprodução de um manuscrito ou pintura particular, a publicação de cartas privados ou de conferências orais ministradas por um professor em classe" (Corliss v. Walker apud BATISTA, 2017, p. 17).

Retomando a figura do direito de ser deixado em paz, “The Right to be Alone” , a privacidade, em que pese tenha sua origem na burguesia, esta, não pode ser reduzida ao mero reflexo da era de ouro de um grupo da elite que o pensou no intuito de proteger seus bens imateriais nos mesmos moldes aos quais protegiam seus bens materiais (CANCELIER, 2017, p. 7; RODOTÁ, 2008, p. 16). Mas, deve ser vista como um meio de garantia das liberdades por, também, proteger opiniões minoritárias e pensamentos desarmônicos em oposição aos dominantes (RODOTÁ, 2008, p. 16).

Portanto, a privacidade não deve ser vista como uma proteção apenas para as elites, ainda que seja creditado a eles o seu início. Mas, a privacidade, o direito de ter a sua vida privada e intimida preservada, de não ter a seus passos monitorados constantemente, bem como uma “polícia do pensamento” do livro de Orwell, deve ser uma garantia a todo e qualquer cidadão, independentemente das camadas sociais, pois trata-se, também, de liberdade.

Assim, formou-se um paradoxo: a proteção última da esfera privada não guardaria a privacidade, mas possibilitaria que a fomentação de crenças e pensamentos individuais fossem tornados públicos de forma livre, possibilitando à associação entre os conceitos de privacidade e liberdade (RODOTÁ, 2008, p. 16).

O artigo de Warren e Brandeis futuramente atingiu seu objetivo, pois teve relevante impacto no “reconhecimento da privacidade como direito pela Constituição Norte-Americana” (BASTOS; PANTOJA; SANTOS, 2021, p. 5).

No entanto, na década de 60, impulsionado pelos avanços tecnológicos, construiu-se, influenciado pelo clamor social em torno do caso *Griswold v. Connecticut* [3], o entendimento de que o direito à privacidade não poderia ser mais contemplado apenas na figura do “The let be Alone”, vinculado ao conceito de propriedade e direitos fundamentais da 1ª geração (direitos negativos e de abstenção), mas era indispensável que houvesse a ampliação deste conceito para que o Estado garantisse “minimante a efetividade da proteção da privacidade com a finalidade da busca pelo livre desenvolvimento da personalidade humana” (FARIAS; FRANCA, 2017, p. 296).

[3] Caso Griswold v. Connecticut – caso em que a Suprema Corte reconheceu a inconstitucionalidade de uma lei do estado de Connecticut que proibia o uso de medicamentos contraceptivos, sob o argumento de que essa lei ofendia a privacidade do casal. Foi através deste caso que se entendeu que a Constituição Americana tutela a privacidade, como um direito fundamental. Assim, o status constitucional da privacidade foi alcançado, concretizando-se, assim, o que Warren e Brandeis pleitearam no artigo “The Right to Privacy” em 1890 (FARIAS; FRANCA, 2017, p. 296).

Em meados dos anos 70, o que foi pleiteado em décadas anteriores, veio a ser instrumentalizado por dispositivos normativos nacionais e internacionais. Rodotà, (2008, p. 16) destaca que além da primeira geração de leis sobre a privacidade, inciativas como a da OCDE em 1980, com os Princípios Diretrizes de Privacidade, e do Conselho da Europa em 1981, com a Convenção 108, primeiro instrumento jurídico internacional com caráter vinculante no âmbito da proteção de Dados, são ferramentas jurídicas relevantes que marcam a história da tutela deste instituto.

Ao longo das décadas seguintes, em razão do atentado do dia 11 de setembro de 2001, (Rodotà, 2008, p. 13) nos Estados Unidos, que resultou em milhares de mortos após o sequestro de aviões que colidiram com as Torres do World Trade Center pela organização terrorista e fundamentalista al-Qaeda, é considerado um marco relevante na mudança de panorama do direito à privacidade na sociedade. Em razão do ataque, como uma das respostas ao terror, no âmbito jurídico, criou-se a "Patriot Act", Lei do Ato Patriota, aprovada em 2001, limitadora de diversos direitos e garantias fundamentais em nome da segurança (RODOTÁ, 2008, p. 14; SILVA, 2014, p. 3).

Rodotà (2008, p. 14), destaca que antes deste atentado já havia movimentos para mitigar o direito à privacidade em razão da demanda do mercado por bancos de dados de consumidores com seus comportamentos. Nesta época, o "fim da privacidade" já era preanunciado por estas motivações oriundas do próprio setor privado.

O "USA Patriot Act", que ampliou o significado de terrorismo, foi aprovado logo após seis semanas do atentado. Este documento abriu precedentes significativos para o aumento da vigilância como um "instrumento essencial à manutenção da segurança nacional", ampliou a capacidade de vigilância governamental e urgiu pela "necessidade e vontade das autoridades americanas de facilitar as investigações de terrorismo, melhorar as trocas de informação entre as diversas agências de segurança" (SILVA, 2014, p. 3).

Consequentemente, um extremo sobreveio após o atentado, "a privacidade na era do terror pareceu estar condenada". Em nome da segurança, a privacidade como um direito fundamental passou a ter a figura de um obstáculo ao primeiro. Contudo, sob a visão de Rodotà, a afirmação: "mais privacidade, menos segurança" é uma receita falsa (2008, p. 8) e pode dar ensejo a discriminações, violações de diversos direitos e garantias fundamentais, totalitarismo e muitos outros problemas.

1.1. Direito à privacidade na Constituição da República Federativa do Brasil de 1988

Em relação ao Brasil, é na Constituição de 1988 que a proteção da privacidade começa a ser tutelada.

O direito à privacidade, por opção dos legisladores, tanto na Constituição de 1988, quanto no Código Civil de 2002, não foi instituída de forma expressa, mas positivado sob a forma de vida privada e intimidade. No mais, embora a Constituição se refira ao sigilo e a inviolabilidade do domicílio, ela ainda está se referindo à privacidade. Ademais, ainda segundo Cancelier (2017, p. 7–8):

> (...) fala-se em vida privada ou vida íntima para tratar do mesmo espaço da vida sobre a qual se fala. Algo secreto, sigiloso ou íntimo pode ser relacionado ao mesmo aspecto que se deseja manter em segredo. O privado pode ser íntimo, o íntimo pode ser secreto, o secreto pode ser privado. Ao mesmo tempo, cada um deles poderá assumir - de forma bastante subjetiva - a depender do sujeito da fala, um significado específico (...).

Silva (2021, p. 203), no livro Direito Constitucional brasileiro, ressalta que existem três incisos relacionados à privacidade na Constituição, todos previstos no rol de direitos e garantias fundamentais, no artigo 5.º em seus incisos x, xi e xii.

O segundo inciso (xi), que visa proteger a inviolabilidade do domicílio, estabelece que:

> a casa é asilo inviolável do indivíduo, ninguém nela podendo penetrar sem consentimento do morador, salvo em caso de flagrante delito ou desastre, ou para prestar socorro, ou, durante o dia, por determinação judicial.

Já o terceiro inciso xii, pode se dizer que tutela a comunicação (2021, p. 203) como objeto de proteção, pois dispõe ser:

> inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal.

Por fim, o primeiro inciso (x), que compõe os aspectos ligados à privacidade, dispõe que. “são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação” (SILVA, 2021, p. 203).

1.2. Conceito do direito à privacidade

Neste tópico há uma tentativa de conceituar o direito à privacidade sob a lente das expressões, proteção à intimidade, vida privada, honra e imagem, contidas na Constituição de 1988.

1.2.1. Proteção à intimidade e à vida privada

Conforme observado no tópico anterior, o constituinte optou por recorrer às expressões, vida privada e intimidade, sem as conceituar, não utilizando, portanto, a palavra privacidade propriamente dita. Contudo, ambas expressões se referem ao mesmo contexto, ou seja, à privacidade, ao foro íntimo que pode ser secreto, e ao secreto que também pode ser privado (CANCELIER, 2017, p. 8).

Todavia, este entendimento não é consenso e as distinções entre o que é a vida privada e o que é intimidade "costumam ocupar a literatura jurídica", conforme afirma Silva (2021, p. 204), pois não há critérios concordantes acerca dos elementos necessários para distinguir cada um. No entanto, segundo o mesmo autor, (2021, p. 204), em alguns casos, ele entende da mesma forma que Cancelier, compreendendo que não é fundamental diferenciar estes conceitos, porque "a intimidade, em qualquer uma de suas definições, sempre será um aspecto da vida privada".

Logo, em consonância com os autores citados, aqui entende-se que não importa debruçar-se em longas discussões no que diz respeito a estes termos estabelecidos pelo constituinte, mas sim ao que eles visam proteger de fato, a tutela da privacidade. Sobre o fundamento desta proteção no âmbito do direito brasileiro, Mendes e Gonet trazem as seguintes reflexões:

> (...) estar submetido ao constante crivo da observação alheia dificulta o enfrentamento de novos desafios. A exposição diuturna dos nossos erros, dificuldades e fracassos à crítica e à curiosidade permanentes de terceiros, e ao ridículo público mesmo inibiria toda tentativa de autossuperação. Sem a tranquilidade emocional que se pode auferir da privacidade, não há muito menos como o indivíduo se autoavaliar, medir perspectivas e traçar metas (...) (Gilmar Mendes e Paulo Gonet apud (FARIAS; FRANCA, 2017, p. 298).

A privacidade, deste modo, deve ser vista não somente através da limitação da esfera individual, vinculado apenas ao cuidado do direito de estar só, mas deve, também, ser compreendido de forma a atingir toda a coletividade, um "direito fundamental que auxilia e é auxiliado por outros direitos fundamentais na tutela de liberdade do indivíduo" (FARIAS; FRANCA, 2017, p. 298).

Ademais, além da influência no desenvolvimento coletivo que a proteção à intimidade e vida privada trazem, há, antes de tudo, segundo Cancelier (2017, p. 8), o impacto no próprio indivíduo, porque a privacidade faz parte dele e o apoia na construção como um ser-humano, também em consonância com o que expôs Mendes e Gonet na citação anterior. Portanto, "ter privacidade é fundamental ao indivíduo, não apenas em oposição ao público, mas numa relação interna, visto que não será possível a assunção de seus desejos sem a construção de seu espaço íntimo" (CANCELIER, 2017, p. 8).

1.2.2. Proteção à honra e à imagem

Em relação à proteção à honra e a imagem, previstos no inciso x do art. 5º da Constituição, cabem algumas distinções e considerações, pois, embora, a proteção da honra e da imagem possam estar correlacionados a reputação[4], esta não é a única configuração que essas proteções podem ganhar forma.

Na concepção da honra e imagem tuteladas em conjunto, no âmbito das Teorias afirmativas do direito à imagem, na Teoria do direito à honra[5], entendia-se que havia uma dependência entre o bem jurídico da honra e o em jurídico da imagem, pois caso a última fosse atingida, consequentemente, a primeira também o seria (BATISTA, 2017, p. 29; SILVA, 2021, p. 204).

A título de exemplo, o direito a imagem, na jurisprudência do STF, é majoritariamente empregado em conjunto com a honra, sem a figura de um direito autônomo (SILVA, 2021, p. 204). Entretanto, embora a honra e imagem tenham conceitos que se aproximam, ambos não se confundem e podem ser tutelados de forma restrita (BATISTA, 2017a, p. 29; SILVA, 2021, p. 204). Desta forma, as distinções entre ambos se tornam mais explícitas (SILVA, 2021, p. 204).

Assim, o direito à imagem estaria apenas relacionado à reputação quando os dois são empregados como sinônimos, mas há outra forma sob a qual o direito à imagem pode ser vislumbrado, sendo o caso das "reproduções da imagem de um indivíduo por meios fotográficos

[4] Virgílio Afonso da Silva (2021, p. 204), no livro Direito Constitucional Brasileiro, define a reputação como um conceito eminentemente social e relacionado a forma como os indivíduos são vistos e percebidos por outros indivíduos em uma comunidade.

[5] Em relação ao direito de imagem há as Teorias Negativistas, as quais não reconheciam à imagem como um direito, e as Teorias Afirmativas, que reconheceram a existência do direito à imagem, se dividindo em Teoria do direito à honra; teoria do direito ao próprio corpo; teoria do direito à identidade; teoria do direito à intimidade; teoria do direito à liberdade e a teoria do patrimônio moral da pessoa.

ou reprográficos, filmes ou vídeos, dentre outros[6]", conforme expôs Silva (2021, p. 204), onde este direito opera de forma autônoma, pois o simples fato de reproduzir a imagem, já configura a sua violação.

Considerando os avanços tecnológicos atuais, onde, segundo pesquisa da FGV de 2021 (FGV, 2021), sendo estes dotados de câmeras e vídeos para serem usados em qualquer lugar, a qualquer momento e compartilhados em qualquer instante por conta da internet, o direito à imagem, em sua concepção, *prima facie*, embora permaneça inalterado no sentido do compartilhamento e reprodução da imagem dependerem da autorização de quem aparece, esta proteção se tornou mais complexa e com mais limitações (SILVA, 2021, p. 205).

Silva (2021, p. 204), destaca que nesses casos, "a proteção da imagem não depende de aferição de danos a reputação do indivíduo (...), mas, sim, ao controle que os indivíduos detêm sobre a própria imagem". Este entendimento, está em consonância com a visão atual do direito a imagem como "um direito de natureza autônoma", ou seja, desvinculado de qualquer outro instituto jurídico (BATISTA, 2017, p. 28).

De igual modo, a honra também possui seu aspecto autônomo, relacionada à honra subjetiva, a qual está vinculada "a percepção do indivíduo sobre si mesmo e não a reputação em uma coletividade, honra objetiva" (SILVA, 2021, p. 205).

Atualmente, ambos são reconhecidos como direitos autônomos, mas com a possibilidade de serem empregados em conjunto a depender do caso concreto.

[6] Assim como nos casos Mark v. Jaffa e Corliess v. Walker citados anteriormente.

2. PREMISSAS BÁSICAS ACERCA DE BIG DATA, INTELIGÊNCIA ARTIFICIAL, BIOMETRIA FACIAL E VIGILÂNCIA

Big Data, inteligência artificial e reconhecimento facial, dentre outros, termos que estariam outrora apenas no escopo de obras de literatura de ficção cientifica ou de grandes produções cenográficas das décadas anteriores, como no filme *Minority Report*[7], — onde há em todo o filme tecnologias que reconhecem a face das pessoas, monitorando e controlando a sociedade através da vigilância, no intuito prever e coibir crimes — hoje, são reais e deixaram de ser apenas frutos de pensamentos imaginativos de um período distópico e distantes a nossa realidade.

Em Nova Orleans, nos Estados Unidos, em 2012, um caso real comprova o exposto anteriormente. Há 10 anos, o prefeito da cidade assinou um contrato com uma "startup" mineradora de dados parceira do Pentágono e de demais setores de inteligência ligados ao governo norte-americano, para utilizar inteligência artificial de modo a auxiliar no combate ao crime.

Descobriu-se, ainda, que a Prefeitura colocou detentos em programas de monitoramento especiais por terem sido identificados pelos algoritmos como "possíveis futuros reincidentes no crime". As pessoas colocadas sob este programa de vigilância especial, em nenhum momento foram informados sobre o uso desses dados e nem da sua finalidade.

Para complementar a gravidade do problema, na cidade de Chicago, também nos Estados Unidos, que usou tecnologia semelhante para criar listas de potenciais criminosos, a medida foi criticada sob a alegação de que a polícia teria apenas feito mais do mesmo, ou seja, só tinha se vestido de uma nova roupagem para continuar enquadrando pessoas de um determinado perfil como criminosas.

Além disso, sem evidências concretas de que as pessoas eram realmente associadas a alguma atividade criminosa, um dos critérios para ser enquadrado na lista era apenas o fato de

[7] "No ano de 2054, há um sistema que permite que crimes sejam previstos com precisão, o que faz com que a taxa de assassinatos caia para zero. O problema começa a acontecer quando o detetive John Anderton, um dos principais agentes no combate ao crime naquele cenário, estrelado por Tom Cruise, descobre que foi previsto um assassinato que ele mesmo irá cometer, colocando em dúvida sua reputação ou a confiabilidade do sistema." ("minority report - Pesquisa Google", [s.d.])

morarem em um local violento[8]. Trata-se, portanto, de um problema já evidenciado na prática, em país onde as condenações injustas teriam roubado mais de 20 anos de liberdade de pessoas inocentes[9].

Assim, podemos atestar que estas tecnologias estão cada vez mais presentes cotidianamente em nossa sociedade vigilante, seja através da substituição da digitação de senhas no desbloqueio do *smartphone*, ao acesso a aplicativos de banco e aprovação de transações financeiras; na aprovação de crédito no momento de realizar uma compra ou solicitar um empréstimo; no alerta do aplicativo informando que o ciclo menstrual está se aproximando; ou, até mesmo, pelo Estado através de câmeras de reconhecimento facial espalhadas pelas cidades e instituições privadas e públicas com o intuito primaz de identificar e reprimir possíveis atos criminosos. O rol informado, no entanto, é exemplificativo, pois há infinitas possibilidades nas quais as novas tecnologias estão presentes na vida moderna interferindo em sua privacidade sem que o usuário tenha ciência de seus impactos.

Logo, tendo as questões acima introduzidas e problematizadas, cabe definir a seguir algumas premissas básicas acerca de que tecnologias são essas e que tipo de sociedade estamos fortalecendo em razão de seus usos.

2.1. Big data, dados e algoritmos

O Big Data pode ser definido como a reunião de "small data", ou seja, de pequenos dados, que quando agrupados e combinados, geram informações complexas que possibilitam a geração de conhecimentos capazes de apoiar em decisões e projetar previsões. Estes dados podem ser oriundos de transações econômicas, redes sociais, interações com buscadores online, interações com serviços de streaming, dados governamentais, dados empresariais, do cotidiano e por câmeras de vigilância públicas e privadas (MARTIN, 2020, p. 67; ZUBOFF, 2015) dentre outros.

Igualmente, conforme preceituou Carvalho (2019, p. 50), "os dados estão em todos os lugares", dessa forma, cada página acessada, pelo "smartphone", "tablet" ou computador, envia informações e uma explosão do número de dados gera o que se chama de Big Data. No entanto,

---

[8]Ver em https://link.estadao.com.br/blogs/ligia-aguilhar/policia-usa-inteligencia-artificial-para-prevenir-crimes-eua/ acesso em 08/06/2022 (ESTADÃO, [s.d.])

[9] Ver em https://www.gazetadopovo.com.br/justica/condenacoes-injustas-roubaram-20-mil-anos-de-inocentes-nos-eua-bsb3rajnag8sg1jmcshxsdmvi/ acesso em 08/06/2022 (BALKO, 2018; ESTADÃO, [s.d.])

pensando hoje no contexto do IoT “Internet of Things” onde quase tudo é conectado à internet, a colheita de dados se expande ao nível exponencial, por televisões inteligentes, relógios inteligentes, assistentes virtuais como a Alexa, dentre outros.

Em tempo, na literatura acerca deste tema, encontra-se comumente cinco aspectos que constituem o Big Data, embora alguns destes possam ser considerados ou não, são: “volume, velocidade, variedade, veracidade e valor” (CARVALHO, 2019, p. 50). Outrossim, a título de explicação:

> Inicialmente, Doug Laney (2001) elencou os três primeiros V’s como dimensões do Big Data: “**volume** se refere à grande quantidade de dados, **velocidade** seria aquela com a qual as informações são captadas e transmitidas - muitas vezes em tempo real e ininterruptamente, e **variedade** seria a multiplicidade de tipos de dados e fontes para obtenção destes em larga escala” (GOMES, 2017, p. 20). Além desses três aspectos, acrescentam-se mais dois V’s, a **veracidade**, que seria a confiabilidade, garantindo o máximo possível de consistência nos dados, e o **valor**, que é o benefício/retorno do investimento para as empresas (MARR, 2015 apud CARVALHO, 2019, p. 50, grifo nosso).

Conforme dito anteriormente, a fonte da qual se extraem os dados são retiradas principalmente da chamada Internet das Coisas – IoT “Internet of Things”, em que, literalmente, qualquer coisa pode estar conectada à internet. Ademais, na Internet das Coisas há a habilidade para “adquirir dados por meio da conexão entre coisas e usuários” (CARVALHO, 2019, p. 47–49). No entanto, estas informações podem gerar resultados não só para entes privados, mas também para entes públicos que tem buscado adquirir estas tecnologias como meio de vigiar e controlar seus cidadãos.

Os dados reunidos podem fornecer resultados importantes e leituras do ponto de vista macro, os quais outrora eram invisíveis quando individualizados. Esta junção associada as programações determinadas pelos algoritmos, auxiliam em diversas esferas da sociedade podendo resultar em otimização de tempo de análise, identificação, monitoramento e prevenção de riscos, conforme preceitua Martin (2020, p. 67):

> A **combinação de maior tamanho e complexidade com análises avançadas que tem sido eficaz na melhoria da segurança nacional, tornando mercados mais efetivos, reduzindo riscos de crédito, melhorando pesquisas médicas e facilitando o planejamento urbano** (...) O Big Data, **combina diversas informações** oriundas de diversas pesquisas, criando formas de gerar conhecimento e previsões, bem como fornecer serviços personalizados (...) Assim, governos atendem melhor seus cidadãos, os hospitais são mais seguros, as empresas concedem créditos àqueles anteriormente

> excluídos do mercado, **os agentes da lei capturam mais criminosos** e as nações são mais seguras[10] (tradução e grifo nosso).

Ainda, sobre a relevância da reunião desses dados, também chamados de "o novo petróleo" devido a seu valor de mercado atual, a transparência de seu uso à população por instituições privadas e públicas é algo imprescindível em razão dos efeitos resultantes nesta utilização e por se tratar do direito do indivíduo, à privacidade, à sua imagem, à sua autodeterminação, à igualdade etc.

Segundo Martin, a utilização e aplicação do resultado desses dados colhidos podem impactar em questões básicas da esfera civil, como em um atendimento médico, por exemplo, que embora a tecnologia possa ser benéfica ao trazer informações mais apuradas e rápidas sobre determinados grupos, podendo ser objeto de pesquisas para novos tratamentos médicos, também há o risco de ser utilizada para fins discriminatórios, como, por exemplo, ser cobrado do paciente um valor maior do plano de saúde ou de determinado medicamento em razão da necessidade que ele se encontra no momento e nem tem ciência disso.

Na mesma seara, em relação à concessão de crédito, embora possa ser um auxílio para alcançar pessoas "desbancarizadas", assim, como no exemplo anterior, o resultado destes dados também pode ser mais uma ferramenta discriminatória sobre pessoas já excludentes do mercado financeiro, ao, por exemplo, recusar a abertura de contas de pessoas oriundas de determinada área, ou por ser vizinha de alguma pessoa determinada considerada de risco pela empresa, por residir em um território violento, com domínio de atividades do narcotráfico, por exemplo[11], sem que as pessoas daquela localidade saibam da existência deste critério e razão que motivou a recusa.

---

[10] No original "Big Data, the combination of greater size and complexity of data with advanced analytics, has been effective in improving national security, making marketing more effective, reducing credit risk, improving medical research and facilitating urban planning.(...) Big Data combines information from diverse sources in new ways to create knowledge, make better predictions or tailor services. Governments serve their citizens better, hospitals are safer, firms extend credit to those previously excluded from the market, law enforcers catch more criminals and nations are safer" (MARTIN, 2020, p. 67).

[11] Em instituições financeiras, por determinação do BACEN, através da Lei 3987, devem ser feitos os processos de diligência prévia, também chamado de "Due Diligences", antes de se iniciar uma parceria, um contrato com um fornecedor ou a entrada de um novo cliente. Estes processos de diligência prévia, com apenas um dado, como o CPF, são possíveis através dos "bureaus" de monitoramento, que por meio do Big Data, reúnem relatórios completos sobre um indivíduo. Neles, é possível ter acesso a diversas informações da vida de uma pessoa (Dados como endereço, número de telefone, processos, dívidas, imagens, filiação, formação, renda etc.) sem que ele tenha ciência do fato, é comum que pessoas sejam rejeitadas, por critérios diversos sem que eles tenham ciência do que motivou tal negativa ou um maior monitoramento.

Por fim, embora existam inúmeros cenários onde esta utilização de dados pode trazer benesses e malefícios, no âmbito da segurança pública, em que pese estas tecnologias possam ser usadas para encontrar pessoas desparecidas e monitorar apenados em regime semiaberto, como propôs a Vara de Execuções Penais de Belo Horizonte, esta, também, como nos casos anteriores, e conforme já exemplificado no início deste capítulo, podem ser utilizadas em caráter discriminatório, reforçando a marginalização e criminalização de determinados grupos minoritários de uma sociedade, tendo em vista que tais tecnologias são dotadas de vieses[12] (BARROS, 2020; MENDES; MATTIUZZO, 2019), e não são neutras, como se acredita no imaginário social, e passíveis de muitos erros.

Em tempo, ainda sobre a noção do que é o Big Data, este grande amontoado de dados não teria condições humanas de ser processado manualmente, até mesmo porque a previsão de produção de dados criados, copiados, tratados e consumidos globalmente somente no ano de 2020 foi da ordem de 64,2 "zettabytes" e a previsão, até 2025, é que este volume ultrapasse o montante de 180 "zettabytes"[13] (STATISTA, [s.d.]).

Facilitando a compreensão, por exemplo, o YouTube que é a segunda maior plataforma acessada da internet, atrás apenas da Google, dona do YouTube, recebe milhares de "uploads" de vídeos diariamente sobre inúmeros assuntos, contudo, se estes assuntos são disponibilizados sem quaisquer critérios, ou seja, de forma aleatória, sem que seus usuários encontrem suas preferências fácil e rapidamente, de nada adianta (KAUFMAN; SANTAELLA, 2020, p. 4).

É nesta seleção de conteúdos personalizada "a gosto do freguês" que consta o ingrediente de sucesso resultante em grande parte do valor das receitas financeiras das gigantes

[12] No site Progra(m)aria, encontramos a seguinte definição e categorização do que são os vieses dentro do âmbito da programação "São, portanto, mecanismos do cérebro para realizar rapidamente associações, com base nas experiências e cenários vivenciados pela pessoa e herança ancestral, que pode levar a tomada de decisões conhecidas e seguras. Ainda assim, os vieses não necessariamente funcionam da mesma forma. (...) Existem vários tipos de vieses. Alguns dos mais conhecidos são: i) Viés de afinidade: tendência a avaliar melhor o que é similar a coisas conhecidas para nós; ii) Viés de percepção: quando as pessoas acreditam e reforçam estereótipos sem base concreta em fatos; iii) Viés confirmatório: disposição para buscar informações que confirmem nossas hipóteses e ignorem as que contradigam; iv) Efeito de auréola (efeito halo): propensão de ter mais disposição a avaliar positivamente o restante das informações a partir de uma única informação positiva ou agradável; v) Viés de grupo: seguir o padrão de um grupo, levando à concordância de uma mesma ideia" (PROGRAMARIA, 2020). Para efeitos deste trabalho, o viés de percepção e o de grupo mais se aplicam neste caso, onde estereótipos e padrão de grupo "efeito manada" podem ser reforçados através de quem programa os algoritmos e implementa estas tecnologias no mercado.

[13] Um Zettabyte é uma unidade de informação ou memória. Ele corresponde a 1.000.000.000.000.000.000.000, ou seja, equivale a 1 sextilhão de bytes, que, em notação científica, poderia ser escrito assim: 10^{21} bytes – ou seja, 10 elevado à 21ª potência (SIQUEIRA, 2012).

empresas de tecnologia. Assim, apenas com a infinitude de filmes, sites, fotos, dados, sem outro ingrediente que traz alguma determinação ou previsão de interesses, não basta!

O ingrediente são os sistemas algoritmos que formam a receita de sucesso que se tem hoje. Uma indústria que movimenta bilhões e bilhões de reais anualmente não somente no Brasil, mas em todo o mundo[14].

Os sistemas algoritmos utilizam os dados agrupados do Big Data para trazer resultados sobre um determinado problema e, até mesmo, preditivos. Logo, tratam-se um conjunto de instruções organizadas de forma sequencial e lógica, ou seja, em etapas, que determina como algo deve ser previamente feito, de modo a executar uma tarefa ou solucionar um problema (MENDES; MATTIUZZO, 2019, p. 3; PORTO; ROLIM, 2022, p. 6; SILVA, 2022, p. 16).

Os algoritmos também podem ser comparados a uma receita de bolo, contendo o "passo-a-passo" determinado pelo programador, o chef, para a solução de uma atividade, podendo estes, ser mais ou menos complexos, ou, chamados simples ou inteligentes. São nestas determinações "step-by-step" feita pelos programadores que os vieses são introduzidos e a conhecida e difundida neutralidade da máquina torna-se apenas uma utopia.

A definição de dados trazida por Buolamwini, cientista de dados e PhD no MIT, ressalta este ponto do enviesamento e sua relação com a história: ela diz que "as tecnologias de inteligência artificial se baseiam em dados e os dados são um reflexo da história, assim, o passado está marcado em nossos algoritmos" (KANTAYYA, 2020).

Igualmente, O' Neil vai dizer que: "algoritmo é o uso de um dado histórico para prever o futuro"[15] (KANTAYYA, 2020). Assim, ela ressalta o poder existente por trás deste sistema, poder este conferido aos donos dos códigos sobre as demais pessoas, sem qualquer simetria nesta balança.

Não há contraditório, não há devido processo legal e o Big Data segue decidindo a vida das pessoas sem serem considerados os vieses que estabelecem estas decisões — como a seleção e a rejeição de um candidato ao emprego por um sistema de recrutamento; pela liberação

[14] "O número de empresas de tecnologia, no Brasil, disparou nos últimos anos e em 2020 houve um recorde de abertura e faturamento de negócios do setor, segundo dados de uma pesquisa da Associação Catarinense de Tecnologia (ACATE) em parceria com a Neoway. O Tech Report, estudo das duas empresas, mostra que o faturamento das empresas de tecnologia em 2020 foi de 426,9 bilhões de reais, o que equivale a 5,6% do PIB nacional" (EXAME, 2021).

[15] No original, "using historical information to make a predicition about the future" (SHALINI KANTAYYA, 2020).

de um crédito para compras ou até mesmo nas chances de um indivíduo ser reincidente, na prática de um crime, resultando na determinação pelo sistema do tempo "ideal" para o cumprimento de uma pena. Conforme O' Neil adverte: temos que estar sempre alerta aos vieses em todo e qualquer processo.

Consideradas as questões acima, é inegável que haja proposta de conscientização e entendimento da responsabilidade àqueles que programam esses algoritmos, compreendendo que no resultado destas projeções há pessoas reais que serão seriamente impactadas na "vida real" por uma possível discriminação algorítmica:

> **Responsabilidade** (ou accountability), sob o ponto de vista da FAT-ML[16], está ligada à ideia de que, ao projetar sistemas algorítmicos, é preciso ter em mente que pessoas serão afetadas pelo processo decisório e que, dessa forma, é necessário, em certa medida, oferecer alternativas para eventual reparação de danos — tanto ao nível individual quanto ao nível coletivo. Essa ideia está relacionada aos princípios da ACM[17] de **conscientização** — o qual se concentra, principalmente, em tornar os engenheiros e usuários de algoritmos conscientes das possíveis consequências de seu uso, especialmente dos enviesamentos que podem surgir a partir deles — e de fiscalização e reparação –, de acordo com os quais os reguladores deveriam adotar mecanismos que permitam que os indivíduos afetados pelas decisões tomadas pelos algoritmos questionem e reparem os possíveis danos causados (MENDES; MATTIUZZO, 2019, p. 18).

Por fim, retomando ao conceito de algoritmo, eles podem ser classificados como algoritmos simples ou inteligentes, embora ambos tratem, analisem e comparem os dados selecionando-os constantemente no intuito de obter um resultado, há uma diferença entre eles. Os primeiros "são códigos computacionais escritos para resolver problemas específicos" e os segundos são programados, especificamente para a resolução de problemas, também chamados "inteligência artificial ou *machine learning*" (MEIRELES, 2021, p. 2). É em relação a este último, os algoritmos inteligentes, que o próximo tópico tratará algumas tentativas de conceituação e reflexões acerca desta tecnologia.

---

[16] A Fairness, Accountability and Transparency in Machine Learning Organization ("FAT-ML em seu acrônimo em inglês) é uma instituição composta por um grupo de acadêmicos que visaram instituir princípios que nortearam os processos decisórios algoritimos" (MENDES; MATTIUZZO, 2019, p. 18).

[17] Association for Computing Machinery (Associação de Máquinas de Computação, ou ACM, em seu acrônimo em inglês), é uma instituição criada com a mesma finalidade da FAT-ML (MENDES; MATTIUZZO, 2019, p. 18).

2.2. Inteligência artificial (AI) e “machine learning”

Em que pese a inexistência de consenso sobre a definição de inteligência artificial (*artificial inteligence* - AI) (OLIVEIRA; COSTA, 2019, p. 4), esta relaciona-se ao aprendizado obtido por sistemas e máquinas ao executar tarefas que “imitam” a inteligência humana e podendo se aprimorar constantemente por meio das interações com os dados que coletam (ORACLE, [s.d.]).

A AI pode, conjuntamente, ser definida como “a possibilidade de uma máquina, por meio de algoritmos, adquirir capacidade cognitiva semelhantes ao de um ser humano” (SILVA; MAIRINK, 2019, p. 65), similares ao aprendizado. Além disso, pode ser dividida em três principais categorias: “Machine Learning”; "Deep Learning” e “Natural Language Processing” (TACCA; ROCHA, 2018, p. 60).

Quando nos referimos ao “Machine Learning*”,* estamos dispondo sobre a frente mais utilizada pela AI, sendo basicamente o aprendizado da máquina, a qual “se adapta e aprende na medida em que as informações vão sendo por ela acumuladas” (TACCA; ROCHA, 2018, p. 60). O’ Neil, vai definir *machine learning “como* um sistema de pontuação que pontua a probabilidade do que você vai fazer”[18] (KANTAYYA, 2020).

É este tipo de inteligência que proporciona o aprimoramento e o desenvolvimento de sistemas capazes de aprender e aumentar conhecimentos através das experiências com dados, ainda que não tenham sido programados com este desígnio (TACCA; ROCHA, 2018, p. 60).

Isto posto, em cada interação, a AI recebe dados e adquire a capacidade de fazer previsões cada vez mais sofisticadas e precisas. Um exemplo, ainda no âmbito do YouTube, mas que também pode ser aplicado às demais redes sociais e plataformas de *streaming*, ocorre por meio da recomendação conteúdos de acordo com os quais possivelmente gostaríamos de assistir (CARVALHO, 2019, p. 52). Uma das controvérsias em torno deste tipo de programação consiste na possibilidade de nos enclausurar em bolhas sociais, pois acessaríamos mais e mais de nós mesmos, reforçando a reprodução de que cremos e de nossos possíveis preconceitos.

Como vimos anteriormente, os algoritmos não possuem os filtros éticos e morais que os humanos possuem, assim, se não houver a devida atenção a estes problemas, a discriminação por meio de algoritmos de aprendizado, que serão mais detalhadas nos capítulos seguintes, não

[18] No original, ”a scoring system that scores the probability of what you’re about to do”.

só forçarão estes vieses discriminatórios, como também favorecerão seu crescimento no mundo "real" através da vigilância.

A outra categoria da AI é a tecnologia do "Natural Language Processing", a qual "possibilita que os computadores possam analisar, entender e concluir com base na fala". Desse modo, "as traduções, analises de sentimentos, dentre outras, são o espectro de suas aplicações" (TACCA; ROCHA, 2018, p. 60).

Por fim, a última categoria é o "Deep Learning", o aprendizado profundo da máquina, que através das redes neurais profundas, observa detalhes que levariam anos para serem observados e, assim, corrigidos e modificados por humanos:

> (...) a percepção e a assimilação de múltiplos e complexos comportamentos e padrões. De forma intuitiva, **o sistema descobre táticas para solução dos problemas que talvez o talento humano tenha levado muito tempo para aperfeiçoar.** A partir dessa percepção, o sistema está apto a apresentar resultados para inúmeras tarefas, inclusive as relacionadas ao direito, assemelhando-se com extrema precisão com aquelas tarefas desempenhadas pelos seres humanos (TACCA; ROCHA, 2018, p. 60).

Ademais, complementando a tentativa de conceituação da AI de *"*Deep Learning*"* são as que:

> (...) utilizam redes neurais profundas e dependem de muitos dados para o treinamento. Tal técnica permite, por exemplo, que o celular organize as fotos capturadas, classificando lugares, pessoas e animais, assim como as marcações antecipadas de pessoas em fotos nas redes sociais" (CARVALHO, 2019, p. 52).

Portanto, considerando as suas funções e aplicações, na prática, entende-se que o *"*Deep Learning" em conjunto com o "Machine Learning" no âmbito das tecnologias de Inteligência Artificial são essenciais para o desenvolvimento das tecnologias de reconhecimento facial, também conhecidas como biometria facial.

2.3. Tecnologia de reconhecimento facial ou biometria facial

A tecnologia de Reconhecimento facial trata-se de um sistema tecnológico viabilizado através da inteligência artificial e suas ramificações, conforme citado anteriormente. A identificação dos rostos é viabilizada por meio de algoritmos de "machine learning", desenvolvidos para registrar e calcular pontos da face, milimetrando matematicamente as suas distâncias, por meio de uma análise profunda dos detalhes do rosto de um indivíduo — distância

entre nariz, olhos, boca etc. — mapeando tais características específicas torna-se possível a identificação.

Nesta tecnologia, o rosto humano é transformado em uma fórmula matemática, armazenada em uma base dados, e, assim, as características que eram analógicas transformam-se em dados.

O aplicativo Google Fotos e o Twitter, por exemplo, fazem uso desta tecnologia. O Facebook já utilizou, mas descontinuou a ferramenta devido a controvérsias que serão explicadas nos capítulos seguintes. No entanto, a ideia da ferramenta consiste em: quanto mais fotos são salvas na base de dados destes aplicativos e redes socais, mais aprimoradas essas máquinas ficam ao fazer a seleção para identificação dos indivíduos.

Dentre as tecnologias apresentadas, no artigo de Martin, como exemplos de usos benéficos e questionáveis do Big Data, o Reconhecimento Facial e o uso de GPS, são considerados. Sob o ponto de vista benéfico de ambos, respectivamente, são apresentados como arquétipo a possibilidade de localizar potenciais terroristas em eventos esportivos de grande escala e a previsão de tráfego e direções no mapa.

No entanto, como pontos controversos, são apresentados o uso pelas mídias sociais para identificar pessoas em fotos, sem a autorização, e a perseguição baseada pela localização, sendo os "smartphones" um tipo de farol do local onde a pessoa está fixa (MARTIN, 2020, p. 68). Todavia, tais controvérsias, principalmente no que tange ao Brasil, serão tratadas nos capítulos seguintes.

Sobre sua utilização, as tecnologias de reconhecimento facial são usufruídas para duas finalidades: autenticação, onde a tecnologia visa saber se você é quem você diz ser e a identificação, onde a pergunta da tecnologia consiste em saber "quem você é?"[19]

Por isso, as premissas citadas neste capítulo importam, pois, se relacionam. Os algoritmos se fundamentam no Big Data, ou seja, no conjunto de dados oriundos de diversas esferas, para fazer suas determinações e predições. As determinações e predições ocorrem através da inteligência artificial, mais especificamente, através do subgênero aprendizado da máquina ou *machine learning*, tecnologia que permite que as máquinas aprendam ou

[19] Matéria por meio de Vídeo do Youtube onde o Jornal Folha de São Paulo explica de forma didática o que é o Reconhecimento Facial e como ele pode impactar na vida das pessoas. Ver em https://www.youtube.com/watch?v=7HuUsntdgWk (FOLHA DE S.PAULO, 2021).

aprimorem o conhecimento, em razão das programações determinadas por padrões previstos nos algoritmos que se alimentam das bases de dados.

Por fim, conforme expôs, Broussard, autora do livro “Artificial Unintelligence”, no documentário Coded Bias (KANTAYYA, 2020), muito da noção que temos de tecnologia de inteligência artificial vem das ficções científicas. Assim, há a construção de uma visão da indústria hollywoodiana, inspirada em personalidades como o Exterminador do futuro, “Eu, Robô”, dentre outros, onde eles são independentes, “tornam-se quase humanos” com potencial para dominar o mundo.

No entanto, Broussard destaca que essa visão é imaginária, pois a IA é simplesmente matemática. Logo, são eles, os programadores, que imputam nas máquinas o “pensamento mágico” e, como todas as pessoas, eles também detêm vieses e transportam-nos para as suas programações.

Deixar este tipo de visão explicita é importante para desmistificarmos esse imaginário de independência e neutralidade, sustentada por pequeno grupo homogêneo detentor dominante da indústria das Big Tech. Visão esta que somente favorece os detentores do poder e os isenta de suas responsabilidades em âmbito judicial e administrativos, em razão dos resultados problemáticos na vida das pessoas, dentro da sociedade real.

2.4. Sociedade de vigilância e capitalismo de vigilância

Quando nos referimos à cultura de vigilância, estamos tratando deste fenômeno em que nós, seres-humanos, estamos nos tornando cada vez mais habituados à vigilância em nosso cotidiano, tanto em locais privados quanto em locais públicos.

Aliás, cedemos os nossos dados quando concordamos com os termos de uso, utilizamos os aplicativos e utilitários que facilitam o nosso dia-a-dia ou apenas por circularmos nos espaços onde as máquinas estão presentes (KOERNER, 2021, p. 1), através de câmeras de vigilância, rastreamento de GPS ou das nossas interações diretas com as redes sociais (SAMPAIO et al., 2021).

Quando utilizamos os “gadgets”, dispositivos que os dispositivos eletrônicos portáteis conectados à internet, nós produzimos a matéria-prima que permite o a predição, a modificação

e o aperfeiçoamento dessas ferramentas, que, sem prejuízo, também poderiam ser chamados de sistemas de monitoramento, os quais, são alimentados através da vida comum.

Os dispositivos tecnológicos "coletam, armazenam, transmitem e analisam" (SAMPAIO et al., 2021, p. 5) nossas respostas e ações que, consequentemente, geram inúmeros dados. Não obstante, o recolhimento de dados não figura apenas no polo passivo, mas também atua no polo ativo pelos próprios indivíduos que de forma ativa compartilham a sua vida em troca de recompensas e notoriedade, "desde o engajamento nas redes sociais, avisos de acidentes ou crimes às instituições de segurança e emergências" (SAMPAIO et al., 2021, p. 5).

Ainda que estes dados possam ser recolhidos da população de maneira ativa ou passiva independentemente do meio, a liberdade de escolha, segundo alguns autores, tem sido viciada. A "manipulação dos indivíduos em sua liberdade de escolha, a violação de sua 'privacidade' e a veiculação de *fake news* colocam o sistema constitucional com seus mecanismos de proteção dos direitos e da democracia em posição de risco (SAMPAIO; FURBINO; ASSIS BOCCHINO, 2021, p. 511).

Zuboff (2021), inclusive irá dizer que a capacidade preditiva dos sistemas algorítmicos consiste, também, na capacidade que eles detêm de modificar o nosso comportamento. Assim, influenciando as nossas crenças, convicções e hábitos de consumo para os fins que eles pretendem, fica mais fácil prever o que iremos realizar. Não por um "misticismo", mas pela manipulação do comportamento.

Inicialmente, o que se propôs através da tecnologia era a possibilidade de ganho de conforto, por meio do uso de aplicativos e utilitários gratuitos (SAMPAIO et al., 2021, p. 511; SAMPAIO; FURBINO; ASSIS BOCCHINO, 2021, p. 5). No entanto, o cenário mudou, sem que os usuários dessem conta do que poderia estar em jogo, em contrapartida. Conforme exposto no documentário "O Dilema das Redes" exibido na Netflix, plataforma de *streaming* de vídeos, se o produto é de graça, isso significa que você é produto.

Desse modo, embora se propague uma aparência de neutralidade dessas plataformas, esta visão, mais uma vez destaca-se que não há como prevalecer, pois, estas, "recebem incentivos para moldar o comportamento e interesses dos usuários e as informações destinadas a eles" (SAMPAIO et al., 2021, p. 9).

A Google LLC., fundada em 1998, portanto com menos de 25 anos de mercado é atualmente uma das 15 empresas mais valiosas do mundo, detentora de um valor de mercado

aproximado em US$ 1,58 trilhões[20] (FORBES, 2022). A empresa foi a pioneira na utilização dos rastros digitais ou "Digital footprint" — considerados à época como lixos virtuais —, e os transformou em uma mercadoria altamente rentável (SAMPAIO; FURBINO; ASSIS BOCCHINO, 2021, p. 511).

Esse meio de extrair dados, antes inexplorado, foi amplamente utilizado pela Google e este *modus operandi* rapidamente deixou de ser algo exclusivo da companhia, expandindo-se para outras empresas do segmento (SAMPAIO; FURBINO; ASSIS BOCCHINO, 2021, p. 511–512).

Trata-se de um sistema autossustentável, dado que é através dessa rotina de vigilância, "da qual se extrai lucro e poder" (SAMPAIO et al., 2021, p. 5) que o capitalismo de vigilância obtém sua fonte para existir. É essa cultura de vigilância da sociedade que facilita, normaliza e até normatiza o capitalismo de vigilância, trocando a liberdade e a privacidade pela sensação de segurança e praticidade. É o ser humano transformado em um aglomerado de dados que "pode e deve ser explorado" de modo a se obter lucro sem considerar quaisquer direitos e garantais fundamentais no processo (SAMPAIO et al., 2021, p. 9).

Capitalismo de vigilância pode ser compreendido como uma nova face do capitalismo financeiro (SAMPAIO; FURBINO; ASSIS BOCCHINO, 2021, p. 517), na qual a vida cotidiana torna-se uma matéria-prima em forma de dados, para comercialização, originando novos "desafios civilizacionais" impostos (CARVALHO, 2019, p. 19; KOERNER, 2021, p. 1; ZUBOFF, 2015).

Estes desafios existem não somente porque as empresas privadas as exploram, mas também porque entes estatais se valem das máquinas para "expropriação da experiência humana processando-a e mercantilizando-a como dados comportamentais" (KOERNER, 2021, p. 1). Logo, "o capitalismo de vigilância se utiliza de toda a experiência humana como matéria-prima gratuita a ser traduzida em dados comportamentais" (CARVALHO, 2019, p. 58).

Em acordo com as definições citadas, conforme preceitua Carvalho, (2019, p. 53)

> Capitalismo de vigilância seria uma mutação do capitalismo que utiliza a imensurável quantidade de dados do Big Data, adquiridos através da vigilância e fornecidos gratuitamente pelos usuários às empresas de tecnologia que, através das técnicas

[20] Encontrado na matéria da Forbes, onde apresentou quais são as maiores empresas do mundo em 2022 Leia mais em: https://forbes.com.br/forbes-money/2022/05/forbes-global-2000-veja-quais-sao-as-maiores-empresas-do-mundo-em-2022/

> vistas, transforma a matéria-prima (informações) em produto altamente lucrativo (dados tratados), no atual estágio da modernidade.

Por conseguinte, em razão da vigilância permear diversas esferas da vida do indivíduo, (inclusive por meio de *gadgets* que monitoram processos fisiológicos, bonecas que extraem dados das crianças, dispositivos 'vestíveis' ou implantáveis no corpo), a internet que emergiu como um motor de democratização de acesso à informação e ao conhecimento, "passou a elaborar instrumentos para modificar e conformar os nossos comportamentos" (KOERNER, 2021, p. 1), como algo rentável. Porquanto, há o fortalecimento da ideia de que este modelo de capitalismo pode pôr diversos direitos e garantias em riscos, porque:

> Gostos, sentimentos, projetos, hábitos, posições políticas, posições religiosas etc., são as informações geradas pelo homem moderno, ainda na forma de dados em estado bruto. O uso da tecnologia refina e extrai dos dados para que eles se tornem predição de comportamentos, ou seja, para atuarem na previsibilidade dos passos do usuário. Com isso, **as empresas vendem a possibilidade de influência sobre os usuários, porém, muitas vezes partem de informações que o usuário não permitiu a finalidade utilizada** (CARVALHO, 2019, p. 55).

Através da extração destes pequenos dados reunidos e conformados em "Big Data", após o processamento de dados por meio das tecnologias de inteligência artificial, estes, podem ser categorizados e. assim, podendo ser comercializados após traçarem o perfil (CARVALHO, 2019, p. 56).

A partir deste processo, é possível concluir que "a privacidade é cara e um novo perfil que possa mostrar para empresas o que o usuário deseja, influenciando e modificando o comportamento é a melhor propaganda para se atingir o lucro" (CARVALHO, 2019, p. 56). Assim, os dados oriundos da vigilância, em curto período, tornam-se fonte de riqueza. Um "novo petróleo", com a vantagem de ser renovável, inesgotável e de gerar subprodutos ainda não dimensionáveis (SAMPAIO et al., 2021, p. 6; SAMPAIO; FURBINO; ASSIS BOCCHINO, 2021, p. 512).

Carvalho (2019, p. 53), comparou as visões de Michel Foucault e Zygmunt Bauman a respeito da vigilância. Para Foucault, a vigilância seria vista sob aspecto negativo, um meio "disciplinar associado a ideia do modelo panóptico, que envolve colocar alguém no centro para vigiar, exercendo soberania sobre os indivíduos". Todavia, na visão do filósofo Bauman (CARVALHO, 2019, p. 53), a ideia de Focault nos dias atuais estaria obsoleta, pois, o próprio indivíduo também se expõe de forma ativa, ou seja,

> O homem moderno não mais se esconde, ele se expõe, **e a ideia de constante vigilância faz com que ela molde e iniba a forma de ser aceito dentro daquele meio**. As pessoas que cercam as outras se tornam os carcereiros nas normas sociais do que seria aceitável ou não, que é cedido pelo medo da exclusão (CARVALHO, 2019, p. 53, grifo nosso).

Na mesma seara, Koerner (2021, p. 2, grifo nosso), acerca do capitalismo de vigilância, expõe esta modalidade contrária ao viés liberal, ao moldar a nossa personalidade e nossos comportamentos, quebrando a nossa confiança uns nos outros ao sermos monitorados em todo o tempo, bem como outros problemas:

> A tese central é que o capitalismo de vigilância configura um regime, ou ordem econômica, contrário às bases da civilização liberal. A instalação em curso do poder instrumental afetaria nossos sentimentos e formas de vida, por corroer a confiança nos outros, quebrar reciprocidades e esvaziar a nossa capacidade de criar compromissos e de construir perspectivas compartilhadas de futuro, eliminando nossa autonomia ou livre vontade. **Ele é distinto do totalitarismo, pois é operado por empresas,** adota meios de modificação "soft" dos comportamentos, e sua finalidade é o lucro**. Ele se afasta do capitalismo de mercado porque pretende a informação total e a certeza sobre comportamentos e processos sociais,** quebra as reciprocidades entre empresas, empregados e consumidores**, e projeta um novo coletivismo com exclusão social, exploração do trabalho precário e indiferença radical em relação à sociedade. Seria um golpe a partir de cima, dirigido contra o mercado**, que impôs unilateralmente o controle do conhecimento e declarou sua própria legitimidade. **Uma tirania que se alimentaria das pessoas e que implicaria a obliteração da política.**

Ainda que haja a participação ativa, muitos desses indivíduos o fazem por não ter a verdadeira ciência de como as empresas e os governos operam no tratamento desses dados. "A extração desses dados, gratuitamente, na maioria das vezes, iniciou-se de forma silente, obscura e sem despertar atenção" (SAMPAIO; FURBINO; ASSIS BOCCHINO, 2021, p. 512) da população, semelhantes a verdadeiras "caixas-pretas".

Em um estudo dos termos de Serviços contratuais das 14 principais plataformas de mídias sociais, feito em 2018, por Nicolas Suzor, identificou-se os Temos são elaborados no intuito de proteger exclusivamente os "interesses comerciais das próprias plataformas" (SAMPAIO; FURBINO; ASSIS BOCCHINO, 2021, p. 521). Outro risco nesse modelo de operação pelas empresas é que a linguagem constitucional, no contexto norte-americano, não estaria adaptada para este cenário resultando em mais vulnerabilidade dos indivíduos (SAMPAIO; FURBINO; ASSIS BOCCHINO, 2021, p. 521).

Outra questão, é que é "necessária uma aparelhagem de alta qualidade, com grande força de resfriamento e energia elétrica, além de especialistas qualificados em conhecimentos

técnicos específicos para a realização de análises preditivas, mineração de dados, etc.” para este tipo de análise complexa de dados. Com isso, torna-se ainda mais distante o relacionamento da empresa e de seus usuários devido à alta complexidade deste processo. Como o objetivo final é o lucro, há pouco interesse pelas empresas em criar medidas que verdadeiramente protejam a privacidade dos usuários e transpareçam as suas formas de tratamento e utilização (SAMPAIO et al., 2021, p. 8).

Na mesma esteira, Frank Pasquale (2015, apud CARVALHO, 2019, p. 59), acerca da extração e utilização de dados dos cidadãos pelas instituições públicas e privadas, através da vigilância, destaca que:

> (...) os dados pessoais dos cidadãos têm sido utilizados tanto por governos como por grandes empresas para a criação do que chama de “espelho de sentido único”, possibilitando que tais agentes saibam tudo dos cidadãos, enquanto a recíproca não é verdadeira. Tudo acontece através da vigilância e monitoramento constantes sobre a vida dos indivíduos, levando ao capitalismo de vigilância, cuja principal consequência é a consolidação de uma sociedade também de vigilância.

Portanto, o reconhecimento e a aplicabilidade efetiva da proteção de dados como um direito fundamental ao cidadão, não deve ser ignorado:

> A regulação social dos mercados, à imposição de limites ao modo como informações são processadas e negociadas, ao esforço por dar mais poder às pessoas no controle do fluxo de informações gerado por elas próprias, mas manejados por grandes corporações” (...). Além disso, “é uma questão de democracia e de equilíbrio de poder. Portanto, a proteção de dados pessoais insere-se na gama de direitos da personalidade, imprescindível para a LGPD que todos os controladores de dados sejam vigiados, na medida em que vigiam seus usuários, ou seja, é preciso que tenhamos clareza sobre a forma como sedemos nossas informações pessoais, sobre como essas informações são utilizadas e ainda carecemos de uma compreensão sobre como isso nos afeta. Para além da tutela da privacidade, a sociedade de vigilância precisa de uma contrapartida jurídica que proteja o indivíduo na totalidade de sua personalidade, hoje amplamente digitalizada (CARVALHO, 2019, p. 59; COSTA; DE OLIVEIRA, 2020, p. 11; RODOTÁ, 2008)

A população deve estar atenta e informada sobre as “nuances” que o totalitarismo carrega consigo. Não cabe, simplesmente, confiar absolutamente no governo A ou B, ou acreditar que o representante X ou Y jamais faria nada arbitrário. A proteção à privacidade, bem como outros direitos e garantias fundamentais, devem ser preservadas e de forma justa para todos (KANTAYYA, 2020).

Certamente, não haverá nenhuma garantia se o Estado atuar à margem da lei, vigiando, colhendo os dados e controlando seus cidadãos em todo tempo através das câmeras de reconhecimento que são como “caixas-pretas”, as quais nem mesmo aqueles que as criam,

sabem descrever totalmente o processo decisório que elas contêm. Como haverá segurança desta forma?

Por fim, considerando que o avanço do uso de tais tecnologias é um caminho que só tende a expandir, a perspectiva é que mais e mais pessoas sejam expostas a este modelo de controle sob o pretexto de garantia da segurança. Dessarte, é imperioso que a legislação acompanhe esses movimentos e vise regulamentar de forma específica, em especial no que tange às tecnologias de reconhecimento facial que tem sido contratada cada vez mais por entes federativos do Brasil, tutelando as garantias e os direitos fundamentais dos cidadãos e a devida responsabilização na utilização destes dados por estes agentes, quer sejam públicos ou privados. A privacidade é cara e não pode ser negligenciada.

3. DIREITO À PRIVACIDADE E AS TECNOLOGIAS DE RECONHECIMENTO FACIAL: REFLEXÕES

Através do Caso Snowden[21], em 2013, tornou-se possível ter um vislumbre de quais níveis a vigilância por agentes governamentais, apoiados por empresas privadas, podem alcançar sob a premissa da guerra ao terrorismo e à violência.

Trata-se do escândalo em que foram vazadas informações de espionagem pela Agência de Segurança Nacional do Governo Norte-Americano (NSA), onde eles, "sob a justificativa de garantir a segurança do país contra o terrorismo, por meio de sistemas de monitoramento telemático, interceptou as comunicações eletrônicas não apenas de suspeitos, mas de pessoas, autoridades e instituições de vários países[22]" (FALK; RODRIGUES, 2015, p. 10), sem quaisquer notificações às partes do que estava ocorrendo.

Inclusive, o Brasil foi um dos países afetados pela espionagem desta agência norte-americana, a presidente Dilma Rousseff e demais assessores, ministros, parlamentares e diplomatas brasileiros ligados ao governo[23] , foram alguns dos vigiados.

Outro caso de vigilância estatal ao nível internacional, é o que foi chamado popularmente de sistema de crédito social (*social scoring*)[24], criado e implementado na China. Segundo o governo, "pretende-se verificar a 'fidelidade' dos 1,3 bilhões de cidadãos chineses aos princípios e valores do Estado" (MULHOLLAND, 2018, p. 16).

Em um modelo que poderia ser denominado "Orwelliano", aos moldes do livro 1984, o programa chinês possibilitará a categorização e a separação das atitudes de seus cidadãos,

---

[21] O caso Edward Snowden confirma a validade da noção teórica desenvolvida por Zygmunt Bauman. "Em meados de 2013, o jornal britânico The Guardian publicou uma série de matérias assinadas pelo ex-advogado e jornalista Glenn Greenwald que desvendavam a vigilância ilimitada praticada pela National Security Agency (NSA), a Agência de Segurança Nacional norte-americana. Tais reportagens revelaram ao mundo que a inteligência do país estava espionando em larga escala. O material para tais reportagens foi propiciado pelo jovem Edward Snowden, então com 29 anos. Snowden exercia o cargo de analista de segurança em uma empresa contratada pela NSA" (FALK; RODRIGUES, 2015, p. 10).

[22] "Os programas utilizados pela NSA na atividade de espionagem (PRISM, Upstream e XKeyscore) apresentavam uma capacidade gigantesca de interceptação, armazenamento e catalogação de dados. Tal capacidade alcança não apenas quase todo o tráfego mundial da internet como também é capaz de interceptar todos os dados armazenados em servidores das gigantes empresas de tecnologia da informação. O sistema denominado XKeyscore, por exemplo, permite que funcionários da NSA analisem em tempo real e retroativamente todas as público e privado, nacional e internacional, dissolvem fronteiras e limites" (FALK; RODRIGUES, 2015, p. 10).

[23] Ver em: https://g1.globo.com/politica/noticia/2015/07/lista-revela-29-integrantes-do-governo-dilma-espionados-pelos-eua.html (G1; GLOBONEWS, 2015)

[24] Ver em: https://www.bbc.com/portuguese/internacional-42033007 (BBC MUNDO, 2017)

marcados como positivos ou negativos de acordo com o critério do Estado, conferindo-lhe pontos. Assim, cada pessoa terá uma pontuação individual que poderá permitir ou proibir o "direito ao acesso a determinadas políticas públicas, que incluem desde a prestação de serviços médico-hospitalares até a indicação de escolas em que os filhos devem ser matriculados" (MULHOLLAND, 2018, p. 16).

Ainda, pretende-se, através do sistema "forjar um ambiente de opinião pública em que manter a confiança é gloriosa. Fortalecer a sinceridade nos assuntos do governo, a sinceridade comercial, a sinceridade social e a construção da credibilidade judicial" (MULHOLLAND, 2018, p. 161–162).

Este projeto permite a verificação da disciplina dos corpos, na prática, através da vigilância estatal. Ressalta-se que a forma como tais critérios são estabelecidos e o resultado da pontuação final não é transparente para as pessoas, tanto físicas, quanto jurídicas, que após o ano de 2020, passaram a ser obrigatoriamente monitoradas e incluídas neste sistema de pontos para realizar quaisquer atividades.

Em ambos os casos supracitados, há a ampla administração não consentida da extração e análise dos dados dos indivíduos pelo Estado (MULHOLLAND, 2018, p. 162), sob a premissa de "segurança", "sinceridade", "credibilidade", dentre outros, para sustentar a violação da privacidade, do direito à imagem de demais garantias fundamentais das pessoas, quer estejam em seu território, ou não, inclusive.

Em razão de situações semelhantes a estas, "em que podem estar presentes potenciais violações de direitos fundamentais, dadas as características e a natureza desses dados sensíveis" (MULHOLLAND, 2018, p. 162) colhidos de forma compulsória, dados tais que caracterizam e identificam uma pessoa, que regulamentações, como a *General Data Protection Regulation* (GDPR), Lei Geral de Proteção de Dados Pessoais (LGPD) e demais Convenções, Leis e Tratados internacionais sobre esta matéria, tornam-se uma espécie de ferramenta de controle ao poder do Estado que não deve ser descartada.

Todavia, para este trabalho, tratar-se-á acerca da LGPD e a sua tutela da proteção de dados frente ao uso das tecnologias de reconhecimento facial pela segurança pública, no que tange ao contexto brasileiro.

3.1. A tecnologia de reconhecimento facial: uma solução ou um problema?

É inegável que as tecnologias de inteligência artificial estão mudando o nosso cotidiano. Embora existam vantagens em seus usos, há, também, controvérsias que não podem ser ignoradas. As controvérsias, em suma, giram em torno dos conflitos éticos e morais na sua aplicação. Logo, é evidente, a necessidade da elaboração de estudos considerando seus impactos negativos, sem desconsiderar seus benefícios (LUDERMIR, 2021, p. 90).

A biometria facial, assim como em quaisquer outras tecnologias oriundas da inteligência artificial, carrega em si impactos. De forma positiva, a título de exemplo, ela pode auxiliar no encontro de pessoas desaparecidas; facilitar "login" em aplicativos; e permitir acesso a locais restritos sem a necessidade de memorizar inúmeras senhas.

É certo que uma das grandes vantagens no uso das tecnologias de AI consiste na possibilidade de a operação ocorrer de maneira ininterrupta e automática, permitindo que os humanos obtenham mais tempo para lidar com outras tarefas. No mais, também podem mitigar riscos, ao evitar que o ser humano esteja vulnerável em atividades de risco, tendo em vista que as ferramentas executarão a operação (LUDERMIR, 2021, p. 90).

Igualmente, a IA atua "como meio de substituição do ser humano no desenvolvimento de tarefas possíveis", com ênfase na economia do tempo, segundo Silva e Mairink (2019, p. 69) descreveram:

> Por se tratar de um meio de facilitação do cotidiano, a inteligência artificial traz diversas vantagens quanto ao seu uso. Sendo uma inovação tecnológica, que são modernizações apresentadas para solucionar algum tipo de problema, e para o caso da inteligência artificial o maior deles: tempo. Hoje em dia 24 horas não são mais suficientes para que se resolvam os desafios diários que enfrentamos desde o acordar ao adormecer. E como seres dotados de necessidades básicas, como: ir ao banheiro, se alimentar e ter descansos contínuos; é necessário sempre parar o trabalho e continuar diversas vezes, as pausas Inter jornadas e intrajornadas, o que acaba, por vezes, ocasionando atrasos. Contudo, diferentemente de um ser humano, uma máquina não precisa parar. Esta é uma vantagem clara: o trabalho não precisa ser interrompido em nenhum momento.

Além da economia do tempo, a segurança e ordem social são alguns dos alvos a serem atingidos por estas ferramentas. Como essas tecnologias operam de forma ininterrupta, ao contrário de um ser-humano, no caso do reconhecimento biométrico facial, por câmeras de vigilância, possibilita o monitoramento das ações da população em qualquer tempo.

Na China, por exemplo, há este tipo de câmera na porta das casas dos cidadãos e às vezes até dentro delas (BBC NEWS BRASIL, 2020). Em que pese não haja regulação nacional

sobre o tema, as câmeras estão presentes, observando “eles atravessarem a rua, entrarem em um ‘shopping’, jantarem em um restaurante, entrarem em um ônibus ou mesmo se sentarem em uma sala de aula”, um cenário quase semelhante ao descrito por George Orwell (1949), onde as pessoas eram observadas por enormes “teletelas” dentro de suas casas.

Os impactos negativos, contudo, no uso das tecnologias de inteligência artificial, podem resultar em situações como a citada acima, onde há total violação da privacidade dos cidadãos, como na perda de vagas de emprego, na qual há a tendência de que funções menos complexas e menos qualificadas sejam substituídas por máquinas (LUDERMIR, 2021). Outros exemplos, no campo da ética e moral na segurança pública são: “a possibilidade de uso de armas poderosas e automáticas, a invasão da nossa privacidade, a falta de transparência de como as nossas informações estão sendo utilizadas, a falta de explicações de como os sistemas de IA chegam as suas conclusões” (LUDERMIR, 2021, p. 90–91).

Ainda no contexto dos conflitos éticos e morais, Silva e Marink (2019, p. 70) ressaltam que as IAs são projetadas para operar segundo as coordenadas de quem as programou. Para eles, o problema em si não se resume na programação em si, mas no fato dela não acompanhar as mudanças e o contexto da sociedade em que se vive, gerando a probabilidade da emersão problemas com “proporções inimagináveis” até então.

Mirando ao passado, em períodos violentos e terríveis da história — nazismo, escravidão, exclusão de mulheres e negros ao voto, dentre outros —, se houvessem máquinas de AI naquela época, sendo elas programadas de modo a responder às questões morais imperantes; hoje, estas máquinas estariam “lutando para reestabelecer a escravidão” ou o holocausto, ou abolir a conquista feminista ao direito do voto (SILVA; MAIRINK, 2019, p. 70).

A problematização não se finda no período atual, pois, ainda que, no campo das especulações, não podemos garantir que de uma hora para outras as IAs raciocinem de modo que:

> ... os seres humanos pensam ser moral matar insetos irritantes, em parte porque o cérebro dos insetos é tão primitivo. Mas o cérebro humano é primitivo em comparação com os meus poderes, por isso deve ser moral matar os seres humanos (RUSSEL e NORVIG, 2013, p. 1194) 11 apud (SILVA; MAIRINK, 2019, p. 70).

Estas considerações, embora sejam imaginárias, são relevantes por demostrarem que estamos lidando com algo novo, uma inteligência ainda desconhecida acerca de todo o seu

processo operacional e ainda não se tem ideia de quais circunstâncias podem ocorrer sob ausência de controle. Ademais, inclusive os especialistas que atuam na área, em sua grande maioria, não conseguem detalhar e explicar como que as máquinas, através dos algoritmos, chegaram a tal resultado.

Logo, tendo em vista não haver exatamente o que se esperar do porvir, a previsão de riscos e quais efeitos poderia haver sobre as novas gerações, são afetadas (SILVA; MAIRINK, 2019, p. 70).

Na aplicação da Lei — *Law Enforcement* —, há, também, os ônus e os bônus no uso destas tecnologias pelo Estado, como "acessar registros telefônicos para identificar possíveis suspeitos em um assalto, acessar *smartphone* sem mandado; identificando suspeitos por hábitos de navegação na *web*"[25] (MARTIN, 2020, p. 68) e utilizar o aprendizado da máquina no reconhecimento facial para identificação de suspeitos e criminosos.

Ainda sobre o fruir da biometria facial pelo Estado no âmbito da segurança pública, alguns casos que aconteceram no exterior podem traçar considerações importantes, para se pensar sobre a sua utilização em larga escala sem que seus riscos sejam reflexionados.

Em 2020, a Amazon.com, Inc., detentora da tecnologia de reconhecimento facial *Rekognition*, suspendeu seu uso pelas forças de segurança dos EUA por 1 ano, inicialmente, prorrogados para mais tempo no ano seguinte[26] (ESTADO DE MINAS, 2021; G1, 2020).

A decisão pela suspensão ocorreu logo após outra gigante da indústria de tecnologia, a IBM, anunciar "em uma carta ao Congresso dos Estados Unidos o encerramento da divisão de pesquisa em reconhecimento facial" o que resultou em uma pressão sobre as demais empresas que utilizavam a comercializavam a biometria facial às forças de segurança.

Pós o feito, a empresa de Jeff Bezos reafirmaram a determinação, sob a mesma orientação da IBM, e decidiu por meio de nota que: "a suspensão persistiria até que haja normativos eficientes tratando sobre as regras e usos desta tecnologia". No entanto, a postura da empresa, frente as acusações de falhas no sistema, foi desanimadora.

Em 2020, a pesquisadora e cientista da computação, Buolamwini, PhD do MIT — Instituto de Tecnologia de Massachusetts, um dos maiores institutos da área do mundo —,

[25] No texto original, "Machine learning to identify burglar; accessing phone records to identify potential suspects in a mugging" e "Machine learning to identify burglar; accessing phone records to identify potential suspects in a mugging" (MARTIN, 2020, p. 68).

enviou um dossiê à Amazon e às outras “Big Techs” sobre os problemas encontrados em suas tecnologias de reconhecimento facial na identificação de pessoas não brancas.

A pesquisadora identificou que os sistemas eram dotados de vieses racistas e sexistas. Toda a pesquisa surgiu, após a cientista, não ter seu rosto conhecido pelas APIs de reconhecimento facial destas empresas. Ela precisava da API destas empresas para criar um projeto da faculdade. Diante das falhas do sistema, ela pensou diversas hipóteses, fez vários testes, até que pegou uma máscara branca, colocou sobre seu rosto e apresentou-se frente a câmera. Após a máscara, o sistema identificou um rosto.

Através deste episódio que ela começou a refletir sobre a suscetibilidade das tecnologias aos nossos vieses, de como seria estar inserido em uma sociedade onde as IA governam cada vez mais as nossas liberdades e como isso impactaria na vida das pessoas caso elas realmente fossem discriminatórias (KANTAYYA, 2020).

A matéria publicada teve grande repercussão nas mídias da época e em resposta ao ocorrido, o Vice-presidente da Amazon publicou no site da empresa uma matéria descredibilizando as pesquisas acadêmicas feitas pela pesquisadora e suas parceiras, bem como as desqualificaram com argumentos rasos.

Buolamwini relatou que isso não era novidade para ela, como mulher negra inserida no setor da tecnologia, ser desacreditada e subestimada, ainda que apresente argumentos teóricos e acadêmicos consistentes.

Há um problema a ser enfrentado, pois, a base de dados que alimenta esses algoritmos é fundamental para a forma de operação destas máquinas.

Após apresentar as questões à Corte Americana, vários estados americanos proibiram a utilização das câmeras de recolhimento biométrico facial em seus territórios. A busca atual da Liga da Justiça dos Algoritmos (fundada por Buolamwini, composta por outras mulheres cientistas que lutam por uma sociedade onde a tecnologia seja utilizada não só por todos, mas para todos), é que estas tecnologias sejam proibidas ao nível federal nos Estados Unidos.

A IBM, ao contrário da empresa citada anteriormente, ao se deparar com o mesmo problema, não somente suspendeu a atividade da comercialização da tecnologia ao Estado para fins de segurança pública, como encerrou a área de pesquisa que tratava do tema, além de com a carta, pedir pela reforma da polícia.

No teor conteúdo da carta, o presidente da empresa destacou que a medida se relaciona com a posição de se opor ao uso das tecnologias para monitorar e vigiar a população. Todavia, a atitude da empresa foi questionada, pois, ao contrário das concorrentes, eles se encontravam atrás no avanço da exploração desta linha de pesquisa, com uma receita ínfima na área[27].

Outro caso relevante e recente ocorreu também no Estado norte-americano, mais precisamente em Illinois. Em razão das normativas legais específicas sobre proteção da privacidade e informações biométricas na região, a Google LLC. foi acionada judicialmente por causa da função de reconhecimento facial, existente no Google Fotos, a qual utiliza a IA para reconhecer e identificar a foto de usuários em fotos e vídeos guardados no serviço[28].

Como resultado, a empresa aceitou em fazer um acordo no valor de US$ 100 milhões (aproximadamente R$ 486 milhões de reais) a título de indenização, aos habitantes do estado, além de ter se comprometido a notificar seus usuários "sobre a coleta de dados para o reconhecimento fácil em imagens e vídeos".

No acordo, previu-se que todas as pessoas que residiram em Illinois entre 1º de maio de 2015 e 25 de abril de 2022 têm direito a serem ressarcidos pela companhia, com os valores variando entre US$ 200 (R$ 972,8) e US$ 400 (R$ 1,9 mil), dependendo de quantos indivíduos recorrerem à Justiça para obter a indenização[29].

Desde 2008, em Illinois, há a vedação às empresas para coletarem e armazenarem quaisquer dados biométricos de seus usuários, sem eles serem notificados sobre a motivação para qual estão realizando essa ação ou por quanto tempo pretendem armazenar esses dados, sejam elas amostras de voz, impressões digitais ou geometria do rosto.

A principal reclamação dos usuários de Illinois quanto ao Google Fotos, consistiu na coleta de seus dados biométricos faciais para identificá-los sem que houvesse a notificação deste ato e por não disponibilizar as "políticas de retenção de dados adotadas para os utilizadores". Mediante a violação, a empresa concordou em aceitar o acordo para findar a ação.

Importa ressaltar que este episódio com as "Big Techs" e a Justiça de Illinois se enfrentando por questões sobre a tutela da privacidade, não é novo. Um ano antes, em 2021, a

---

[27] Ver mais: https://g1.globo.com/economia/tecnologia/noticia/2020/06/09/ibm-encerra-area-de-pesquisa-em-reconhecimento-facial-e-pede-reforma-da-policia.ghtml (G1, [s.d.])

[28] Ver mais: https://canaltech.com.br/seguranca/google-vai-pagar-us-100-mi-por-violacao-de-privacidade-em-reconhecimento-facial-218244/ (CANALTECH, 2022)

[29] Ver mais: https://www.theverge.com/2022/6/6/23156198/google-class-action-face-grouping-biometric-information-illinois-privacy-act (THE VERGE, 2022)

empresa Facebook, agora META, teve que pagar US$ 650 milhões (proximamente R$ 3,1 bilhões) aos habitantes do estado por causa da ferramenta de sugestões de marcação na rede social, a qual utilizava tecnologia de reconhecimento facial para analisar as fotos de usuários da plataforma de modo a sugerir a presença deles em imagens de outros usuários. Atualmente, a ferramenta foi descontinuada pela empresa.

Nota-se, portanto, através dos casos acima que a decisão por esta tecnologia deve ser levada sob cautela. As empresas, literalmente, optaram pela descontinuidade de seu uso em cidades dos EUA.

Estas ações podem demonstrar que as vantagens destas tecnologias, podem não compensar os riscos relacionados ao seu uso. Inclusive, estas suspensões, vieram, também, em razão de diversos casos de racismo algoritmo, onde houve pessoas negras sendo identificadas como gorilas no Google Fotos, rostos de mulheres pretas não identificadas no sistema de reconhecimento facial da Amazon, confusão de gênero de mulheres pretas, inserção das câmeras de reconhecimento em bairros de maioria hispânica e negra, entre outros casos.

Outro dado importante, acerca da mitigação da privacidade por meio do controle estatal, provém da organização inglesa, Big Brother Watch, no Reino Unido, que objetiva alertar a população contra a vigilância estatal, violações de privacidade e ameaças às liberdades civis[30]. Em seu site, eles trazem o seguinte alerta:

> A polícia e as empresas privadas no Reino Unido estão lançando silenciosamente câmeras de vigilância de reconhecimento facial, tirando 'impressões faciais' de milhões de pessoas - muitas vezes sem você saber disso. São dados biométricos tão sensíveis quanto uma impressão digital. A Polícia Metropolitana está planejando lançá-lo em toda a capital. **Esta é uma enorme expansão do estado de vigilância – e estabelece um precedente perigoso em todo o mundo.** Devemos parar com essa vigilância perigosamente autoritária agora (BIG BROTHER WATCH, [s.d.]).

Na mesma página, eles advertem sobre supermercados em Londres que também estão usufruindo desta tecnologia secretamente sem ciência de seus clientes e de quais são os propósitos por detrás da coleta destes dados.

De acordo com a ONG, entre 2016 e 2022, a taxa de imprecisão do sistema de reconhecimento facial da Polícia londrina ficou em cerca de 86%, resultando em mais 3.000 mil pessoas identificadas erroneamente, mas mesmo com tantas falhas, a política de vigilância

[30] Ver em: https://bigbrotherwatch.org.uk/ - website da organização sem fins lucrativos.

em massa continua em expansão sem haver qualquer regulamentação específica tratando do tema.

No documentário Coded Bias o qual investiga o viés nos algoritmos depois da pesquisa feita por Buolamwini (KANTAYYA, 2020), há duas cenas que expressam esta cultura da sociedade de vigilância, em Londres, exatamente no lugar onde é o cenário do livro de George Orwell.

A primeira cena ocorre quando um homem é multado em 90 libras por tampar o rosto ao passar em um local onde estavam as câmeras de reconhecimento facial usadas pela polícia. O homem decidiu esconder seu rosto, após ser informado na saída do metrô pela ONG que havia câmeras recolhendo dados biométricos naquele local. Contudo, por esconder o rosto, a polícia foi atrás dele e o cercou. Após questionar essa obrigatoriedade, foi multado sob o pretexto de ofensa à ordem pública, mesmo sem haver fundamentação legal para a ação punitiva do estado.

O outro caso é de um adolescente negro, de 14 anos, com uniforme escolar, que andava com seus amigos na rua. Nela, ela não sabia, mas havia câmeras de reconhecimento facial que o apontaram como suspeito, diante disso, vários policiais à paisana o cercaram, levaram-no para um local mais isolado e lhe fizeram diversas indagações e recolhimentos de dados.

Após cerca de 15 minutos, o adolescente foi liberado, pois, o sistema errou na identificação, e, ainda em choque, constrangido, sem ter ciência do que acontecera, a ONG que já observava a situação, abordou o jovem e lhe explicou sobre o ocorrido.

Portanto, em que pese as tecnologias de reconhecimento facial têm sido apresentadas como uma solução de apoio à segurança pública, aos brasileiros, através do monitoramento e identificação de criminosos, foragidos da justiça e pessoas desaparecidas, existem ainda muitas questões que devem ser pensadas antes de sua implementação em massa como tem sido implementada no Brasil.

Ademais, embora a biometria facial pareça ser de grande auxílio, pouco se sabe sobre como são tratados esses dados colhidos, como se dá o seu armazenamento e quais são critérios estabelecidos a fim de um resultado.

Tais reflexões não podem ser ignoradas, ainda mais quando se observa o contexto da realidade brasileira, pois essas tecnologias são importadas dos EUA, Reino Unido e China, que como se observa, apresentam questões delicadas no campo ético e moral com impactos na

marginalização de grupos de minoritários nos EUA e Reino Unido, e os “Uyghurs” na China, grupo étnico perseguido pelas autoridades, através, também, desta tecnologia.

Não se deve olvidar que ao importarmos tais tecnologias que apresentam inúmeras falhas, considerando os contextos locais daquelas regiões e a sua programação; como não pensar nas implicações que estas tecnologias podem gerar neste país, composto majoritariamente por pessoas pardas e negras, que já são perseguidas e, em simultâneo, excluídas de apreciação ao direito pelo Estado constantemente, levando-os para a prisão, muitas vezes, com base apenas no reconhecimento fotográfico?

3.1.1. Vigilância negra e racismo algorítmico

Neste tópico não se pretende aprofundar e esgotar definições sobre o que é o racismo e todos os seus fatores históricos que culminaram no cenário atual em nossa sociedade. Para o fim deste estudo, contudo, importa compreender o racismo como um “fenômeno social indesejável”, impactante em diversas esferas da coletividade, sem excluir o âmbito tecnológico. Pois, este fenômeno não se faz ausente nas IAs e, através delas, pode fortalecer discriminações a “grupos historicamente marginalizados” (PORTO; ROLIM, 2022, p. 3).

Inicialmente, parte-se da premissa de que é necessário que se “reconheça a existência do racismo e, paralelamente à sua desconstrução, deve-se buscar identificar as circunstâncias em que a subjugação dos indivíduos negros ocorre simplesmente em razão da cor da sua pele” (PORTO; ROLIM, 2022, p. 5).

Diante dessa ciência, parte-se para a compreensão da segunda premissa, a existência dos efeitos do racismo estrutural: “no Brasil, o modo de produção escravocrata gerou reflexos sentidos até os dias de hoje, principalmente no tratamento do negro(PORTO; ROLIM, 2022, p. 4). No entanto, estes reflexos não são sentidos apenas na realidade brasileira, mas é possível, infelizmente, observar esses impactos em outras partes do mundo.

Por fim, a última premissa a ser compreendida é a de que as tecnologias de IAs são carregadas de vieses. Embora se tenha acreditado que fossem neutras e isentas de vieses, a realidade atesta o oposto, em especial no que tange ao uso das tecnologias de reconhecimento facial (PORTO; ROLIM, 2022, p. 5).

Casos que demonstram a reafirmação deste fenômeno social indesejável ligado as tecnologias de biometria facial estão cada vez mais crescentes, tanto no contexto nacional, quanto no contexto mundial.

Em relação ao cenário brasileiro, já houve prisões feitas injustamente com base nestas câmeras de vigilância espalhadas por algumas das principais capitais do país que serão detalhadas no capítulo seguinte. No entanto, por hora, serão analisados os casos ocorridos no exterior, oriundos de alguns dos países de onde o Brasil tem importado, sem regulamentação específica sobre o tema para fins de segurança pública, esta tecnologia.

A neutralidade da máquina é uma fantasia: ela é programada por pessoas reais e pessoas reais carregam vieses consigo. Ademais, ainda que a AI aprenda com os humanos e seus dados continuamente através da interação, o problema não deixa de persistir.

O caso da (robô) virtual Tay, criada pela Microsoft, em 2016, exemplifica este fenômeno, porque em menos de 24 horas, ela aprendeu com os usuários da rede a ser racista, misógina e xenofóbica, fazendo comentários de apoio ao racismo, a segregação, a Hitler e ao ódio aos judeus, após 16h de seu lançamento [31].

“Quanto mais você conversa com Tay, mais esperta ela fica”, foi o proposto pela Microsoft, no entanto, o resultado foi catastrófico e a ferramenta restou descontinuada. (PORTO; ROLIM, 2022, p. 8). Esse episódio aponta que a inteligência artificial aprende e aprende muito rápido, sem quaisquer filtros éticos ou morais.

No ramo do reconhecimento facial, um programador chamado Jacky Alciné, se deparou com a sua imagem e a de sua namorada marcadas com a “tag” “gorilas” no Google Fotos (EL PAÍS, 2018). Apesar da divulgação do caso por Alciné, advertindo à grave falha cometida pelo sistema, as ações da empresa se limitaram em retirar a “tag” da base dados e realizar uma justificativa de que o sistema de reconhecimento facial da empresa é considerado a melhor do mercado, sem prometer nenhuma ação concreta para aprimorar e aperfeiçoar a base de dados do aplicativo (SILVA, 2020, p. 10).

Alciné, também atuante na área de tecnologia, indagou em sua rede social: "Que tipo de dados de amostras de imagens coletadas que resultaria nisto?" referindo-se categorização do sistema colocando-o, com a sua parceira, ambos negros, como gorilas.

---

[31] Ver Mais em: https://veja.abril.com.br/tecnologia/exposto-a-internet-robo-da-microsoft-vira-racista-em-1-dia/ (VEJA, 2016)

Outro caso relacionado a associação de "tags" estranhas a pessoas negras é exemplificado por Silva, onde relata sobre o "projeto de interrogação de APIs de visão computacional e bancos de imagens ao comparar como sites de bancos de imagens como Shutterstock representam fotos de diferentes países". Neste caso, o neutro seria a pessoa branca, a base "padrão" pela qual os algoritmos foram programados a identificar.

> O estudo identificou que diversas fotos de mulheres com cabelos crespos volumosos foram marcadas com a tag 'wig', que significa 'peruca'. Este erro possivelmente é resultante de uma base de treinamento mais rica em fotos de pessoas brancas em contexto de apropriação cultural-estética – como a prática de usar perucas afro como fantasias em festas e carnaval (...) onde esta ideia de neutralidade é marcada socialmente como a percepção dos desenvolvedores (SILVA, 2020, p. 10–11).

Além desse, outro experimento é citado pelo mesmo autor, o "Experimento do Rhue", relacionado ao reconhecimento de imagens e categorização de expressões faciais nos sistemas da Microsoft e Face++. As expressões seriam a Raiva, o Medo, a Surpresa, o Nojo e a Tristeza, para serem categorizadas de acordo com a imagem apresentada.

Como base para a pesquisa, foram apresentadas imagens de atletas negros e brancos. No resultado, às pessoas negras eram atribuídas constantemente "expressões/emoções negativas" (SILVA, 2020, p. 11), ao contrário do que ocorria com pessoas brancas. Assim, Rhue (SILVA, 2020, p. 11) concluiu que "o uso de reconhecimento facial pode formalizar estereótipos preexistentes em algoritmos, automaticamente incorporando-os na vida cotidiana".

O caso do *FaceApp*, famoso por envelhecer selfies, também se popularizou em razão de uma polêmica. No aplicativo editor de fotos há a função e embelezamento, no intuito de "melhorar" a foto de seus usuários, todavia, como resultado, o aplicativo também clareava a pele de pessoas não-brancas e alterava seus traços para se assemelharem aos traços caucasianos, afinando o nariz e os lábios[32]. Esta ferramenta, que pretendia trazer "a sua melhor versão" (MUNDO NEGRO, 2019), gerou "resultados aberrantes em fotos de pessoas negras ou indianas, por exemplo" (SILVA, 2020, p. 11).

Após a divulgação da falha, o CEO do aplicativo, aduziu se tratar de um "um infeliz efeito colateral da rede neural subjacente causado pelo conjunto de dados de treinamento, não comportamento esperado" (SILVA, 2020, p. 11). Todavia, como nos casos anteriores e nos próximos que serão apresentados, a base de dados que alimenta os algoritmos de inteligência

[32] Ver mais em: https://mundonegro.inf.br/sua-melhor-versao-apps-que-mudam-o-rosto-revelam-o-racismo-clareando-pessoas-negras/ (MUNDO NEGRO, 2019)

artificial são essenciais para o desempenho da máquina. Dessarte, é inegável que os dados recebidos como “padrão” do que é belo, foi definido por um determinado grupo étnico em detrimento de outros, selecionados por pessoas com vieses reais.

Silva (2020, p. 11), após tratar desses casos, retoma a falsa crença da neutralidade do algoritmo, pois alegações como as do CEO do “FaceApp*”,* afastam a responsabilidade deles na construção da máquina e reforçam esse panorama de total independência da máquina, o que não é verdade, dado que são engenheiros, programadores e cientistas de dados, que alimentam e selecionam os dados de treinamento para operação do sistema.

Bento (SILVA, 2020, p. 11) reflete que a invisibilidade de pessoas pretas é um "elemento importante da identidade do branco: ele não vê o negro. Uma reflexão sobre relações raciais pode explicitar um desconforto do branco diante da paradoxal constatação que ele não vê, não lembra, nunca pensou nos negros".

Através da resposta, ou melhor, da ausência de respostas que os representantes das grandes *Big Techs*, bem como de outros aplicativos que utilizam a tecnologia de reconhecimento facial, tem dado a pessoas negras, assevera que o cerne dessas empresas, como alvo para consumidores finais, ao nível global, são apenas os brancos.

Por fim, ainda sobre o *FaceApp*, após alguns anos da desculpa feita pelo presidente da empresa, atestou-se que o problema de embranquecimento ainda permanece (SILVA, 2020, p. 11).

Embora alguns destes casos estejam relacionados as empresas de tecnologia privadas, estas se conversam, e muito, com o impasse da vigilância estatal, já que muitas destas empresas são contratadas pelo governo para fins de segurança pública no desenvolvimento de “sistemas para vigilância e policiamento, biometria e reconhecimento facial”, portanto, “o potencial de impactos fatais contra a vida de grupos ‘racializados’ parece já ser óbvia” (SILVA, 2020, p. 12).

A título de exemplo de impacto fatal contra a vida de pessoas não negras por estas tecnologias, um estudo feito por Benjamin Wilson, Judy Hoffman, Jamie Morgenstern, constata este feito, no qual, após analisarem 8 tipos de sistemas de reconhecimento facial utilizados em carros automáticos, previram que:

> a acurácia na identificação de pessoas com pele escura poderia ser 5% menor, resultando em potenciais atropelamentos. Os autores concluem a necessidade de se olhar para o “real problema que pode surgir se este tipo de fonte de viés de captura

> não for considerado antes de distribuir estes tipos de modelos de reconhecimento (WILSON, HOFFMAN e MORGENSTERN, 2019, p.9, trad. Livre, apud (SILVA, 2020, p. 12)

A proposta dos pesquisadores era a de investigar "se sistemas de detecção de objetos de última geração têm desempenho preditivo equitativo em pedestres com diferentes tons de pele"[33] (WILSON; HOFFMAN; MORGENSTERN, 2019). Lamentavelmente, o resultado expôs mais uma modalidade de risco para grupos étnicos minoritários, em razão da menor acurácia na identificação, ou seja, mais um meio para potencializar as desigualdades.

Em consonância com o parágrafo anterior, no que tange aos impactos reais causados sobre a vida de pessoas reais, através do racismo algorítmico, importa destacar o resultado do estudo do "Correctional Offender Management Profiling for Alternative Sanctions" (COMPAS), um software atuante no sistema penal dos EUA, onde (PORTO; ROLIM, 2022, p. 8):

> após o exame de mais de 10.000 (dez mil) casos, se reconheceu viés racial grave na estimativa do risco do avaliado, pois 'os réus negros tinham muito mais probabilidade do que os réus brancos de serem julgados incorretamente como correndo um risco maior de reincidência, enquanto os réus brancos tinham mais probabilidade do que os réus negros de serem marcados incorretamente como de baixo risco'.

Outro estudo feito pelo *National Institute of Standards and Technology* (NIST), onde analisaram diversas tecnologias de reconhecimento facial nos EUA, concluiu-se que:

> os sistemas de reconhecimento facial, como regra, apresentam diferenças na capacidade de um algoritmo de cruzar duas imagens segundo a variação demográfica. Constatou-se, ainda, maior probabilidade de falsos positivos em relação a indivíduos negros e asiáticos (...) e "menores taxas de falso positivo para caucasianos e asiáticos" (PORTO; ROLIM, 2022, p. 9).

Ademais, destacando mais uma vez que o Brasil também importa a tecnologia de países asiáticos para integrar o escopo da segurança pública, evidencia-se que o problema para pessoas pretas não se finda com a contração da ferramenta oriunda da China. O sistema ainda continua excludente para pessoas pretas, com apresentando menores risco de erros para pessoas não-pretas.

---

[33] No original: "In this work, we investigate whether state-of-the-art object detection systems have equitable predictive performance on pedestrians with different skin tones" (WILSON; HOFFMAN; MORGENSTERN, 2019).

Todos os casos citados, intensificam o fato de a invisibilidade negra estar sendo construída, também, nos algoritmos, mídias e demais tecnologias. Silva (2020, p. 12), aponta que a invisibilidade branca, ao contrário da negra, traz outro conceito, “pois se vincula à sua padronização e referência como universal”.

Como O’ Neil (KANTAYYA, 2020) salientou, as tecnologias de inteligência artificial têm ocupado diversas esferas da sociedade, decidindo sobre as nossas vidas e, seus resultados, considerados como verdades sem subjetividades.

Mesmo com todas as controvérsias supracitadas, as tecnologias de reconhecimento facial têm crescido no Brasil, pela administração pública, oriundos, principalmente, dos países já citados. Não há, atualmente, um sistema brasileiro, o que pode culminar em problemas maiores em razão de uma provável “menor aptidão dos programas utilizados para se atingir as finalidades pretendidas” (PORTO; ROLIM, 2022, p. 9), tendo em conta as realidades e características da sociedade brasileira.

Por fim, este capítulo trouxe para a discussão se as tecnologias de reconhecimento facial podem ser mais um instrumento propulsor da mitigação do direito à privacidade, com mais discriminações e injustiças, sem possibilidade de contraditório, pois estas nem são comunicadas de tais perfilamentos e controles, e muito menos, ampla defesa, pois, como é possível ter justiça através de um sistema em que os critérios dos seus processos decisórios são desconhecidos até mesmo para quem o produziu?

4. AVANÇO DAS TECNOLOGIAS DE RECONHECIMENTO FACIAL NO BRASIL PELA SEGURANÇA PÚBLICA

O uso das tecnologias de reconhecimento facial no Brasil para fins de controle não é um fenômeno recente, apesar de o tema, sob perspectiva regulatória, ter adquirido maior repercussão. Sobretudo, pela expansão das discussões sobre a segurança pública, um dos centros do debate político nacional atual.

Foi em Ilhéus, na Bahia, no ano de 2011, que tudo se iniciou em terras brasileiras. Nesta cidade, houve o primeiro caso do uso das tecnologias de reconhecimento facial para fins de controle. A proposta era a de prevenir e identificar fraudes nos transportes públicos baianos (INSTITUTO IGARAPÉ, [s.d.]).

No entanto, a inserção desta IA não findou ali. Ao longo dos anos foi se expandindo e permeando as cidades brasileiras. Segundo dados do Instituto Igarapé (INSTITUTO IGARAPÉ, [s.d.]), até o ano de 2019, havia 37 cidades com câmeras de vigilância ativas no Brasil, sendo que cerca de mais da metade foram instaladas apenas no período entre 2018 e 2019, para os fins de segurança pública, transporte e controle de fronteiras (AGÊNCIA BRASIL, 2019).

Não é sem razão que a Agência Brasileira de Inteligência Nacional (ABIN) se manifestou, em 2019, em defesa da utilização da biometria facial, bem como de outras tecnologias, para fins de vigilância e repressão à violência.

Contudo, em que pese a ABIN defenda o uso destas tecnologias, especialistas na área dos direitos humanos apontam riscos em sua implementação. Como resposta, Filipe Soares, integrante do Gabinete de Segurança Institucional da Presidência da República e oficial de inteligência da ABIN, argumentou que a população é despreocupada no que tange à vigilância por empresas privadas, como Google, Facebook, entre outras, mas é resoluta a este uso pelo (SENADO FEDERAL, 2019).

Todavia, é cediço que a administração pública é regida pelo princípio da legalidade, devendo agir somente debaixo do que está previsto em lei, fora deste âmbito, é ilícito. Ao contrário do foro privado, onde é lícito fazer tudo o que a lei não proíbe, como o caso das *big techs* citadas pelo representante da Abin.

Ademais, ainda que as empresas privadas tenham se aproveitado, ao longo dos anos, da ausência de regulação específica para extrair os dados de seus usuários, isto não é salvaguarda para que o Estado venha agir desta maneira. Na verdade, deveria agir para garantir e proteger os cidadãos de possíveis violações da privacidade, bem como outros direitos, causadas por estas instituições privadas.

Portanto, a cautela deve prevalecer sobre estas implementações pela administração pública em esfera nacional, pois como vimos nos capítulos anteriores, existem questões éticas e morais delicadas e controvérsias em sua implementação que não podem ser, simplesmente, ignoradas.

O cadastro de Identificação Civil Nacional (ICN), instituído pela Lei n° 13.444, de 11 de maio de 2017, um projeto em implementação no Brasil que vai em consonância com o cenário de sociedade de vigilância, tem como objetivo identificar o brasileiro em suas relações com a sociedade e com os órgãos e entidades governamentais e privados. Dessarte, de forma simultânea e em tempo real, seria possível monitorar "transeuntes anônimos em logradouros públicos através da comparação de pontos faciais registrado no banco de imagens, aplicação esta denominada vigilância facial" (OLIVEIRA et al., 2022, p. 6).

Em São Paulo, a biometria facial é usada nos transportes públicos desde 2017, de modo a combater fraudes, assim como na Bahia (ARAÚJO; CARDOSO; PAULA, 2021, p. 3; SILVA; FRANQUEIRA; HARTMANN, 2021, p. 9). O que, em uma cidade da magnitude de São Paulo, onde a maior parte da população utiliza os transportes públicos e percorre grandes distâncias diariamente, pode representar uma limitação considerável à privacidade e à locomoção de pessoas vulneráveis, considerando que nenhum sistema é isento de falhas (ARAÚJO; CARDOSO; PAULA, 2021, p. 3).

Ainda em São Paulo, no ano de 2018, a concessionária de Metrô ViaQuatro implementou a biometria coletando os dados faciais, em suas estações, com o fito de captar as reações dos transeuntes na linha (SILVA; FRANQUEIRA; HARTMANN, 2021, p. 9), ainda que sem o devido consentimento e informação aos que tinham seus dados coletados.

O sistema, que captava através das portas "as emoções dos usuários, além do gênero e faixa etária dos passageiros posicionados em frente ao sensor" (COSTA, 2020, p. 19; PORTO; ROLIM, 2022, p. 14), foi objeto de uma ação civil pública (nº 1090663-42.2018.8.26.0100), apresentada pelo Instituto Brasileiro de Defesa do Consumidor (IBDC), representando os consumidores do transporte público, em face da ViaQuatro.

Nos fundamentos, o IBDC arguiu por “graves violações aos direitos à intimidade (art. 5º, X da Constituição Federal de 1988), privacidade e à informação dos usuários do serviço público de mobilidade urbana e relaciona a coleta compulsória e utilização de dados pessoais sensíveis”. Ademais, apontaram pela ausência de consentimento e violações a outros dispositivos legais e marcos normativos, como “marco Civil da Internet e ao Código de Defesa dos Direitos do Usuário dos Serviços Públicos de Mobilidade” (COSTA, 2020, p. 21).

Outrossim, pediu para serem cessados “imediatamente a coleta de dados e o desligamento do sistema, pois além de violar os direitos já citados, também capta a imagem de crianças e adolescentes que transitam no sistema de metrô” (COSTA, 2020, p. 21).

Em sede de decisão, a empresa foi multada em R$ 100 mil reais, além de ter sido impedida de continuar com o uso da tecnologia. Um dos fundamentos da sentença, proferida pela Juíza Patrícia Martins Conceição, se pautou na ausência de consentimento dos usuários que tinham seus dados coletados pela empresa, pois não apresentou essa possibilidade.

No mesmo ano. João Dória, Governador do Estado de São Paulo, vetou o projeto de lei que estabelecia como obrigatória a inserção de tecnologias de reconhecimento facial em todas as estações do Metrô do estado, bem como na companhia Paulista de Trens Metropolitanos (CPTM), e, inclusive, nos vagões (AGÊNCIA BRASIL, 2021; COSTA, 2020, p. 19; PORTO; ROLIM, 2022, p. 14).

Todavia, em oposição à medida da decisão judicial apresentada e do veto pelo Governador do Estado de São Paulo, o ministro da segurança pública assinou a Portaria n.º 793/2019, a qual regulamenta o incentivo financeiro das ações do Eixo Enfrentamento à Criminalidade Violenta, no âmbito da Política Nacional de Segurança Pública e Defesa Social e do Sistema Único de Segurança Pública, com os recursos do Fundo Nacional de Segurança Pública (ARAÚJO; CARDOSO; PAULA, 2021, p. 9; BRASIL, 2020).

A Portaria mira a biometria facial como medida para o combate à criminalidade violenta. Ela, que já é utilizada nos Estados do “Ceará, Rio de Janeiro, Bahia e Distrito Federal” (PORTO; ROLIM, 2022, p. 14), conforme está disposto na alínea b), da portaria visa a implantação de sistemas de videomonitoramento com soluções de reconhecimento facial, por *Optical Character Recognition* - OCR, uso de inteligência artificial ou outros(BRASIL, 2020), “sem referência a qualquer contramedida de limitação no uso dessa tecnologia” (PORTO; ROLIM, 2022, p. 14).

Diante desses avanços na implementação desta IA, mediante as controvérsias que ela possui, reafirma-se aqui, a necessidade de que medidas de proteção sejam criadas, a fim de proteger o direito à privacidade, bem como outros direitos, "pois já há registos de sua implementação e até mesmo de prisões realizadas através dele" (ARAÚJO; CARDOSO; PAULA, 2021, p. 9).

O enviesamento racial nestas destas tecnologias, importadas de países que já apresentaram diversos inconvenientes, não pode ser olvidado, ainda mais pelo contexto racial que o Brasil está inserido (ARAÚJO; CARDOSO; PAULA, 2021, p. 9).

Conforme foi apresentado nos capítulos anteriores, diversos estudos apontam pela ausência de neutralidade que as IAs possuem, implementando os vieses daqueles que programam a máquina afetando "pessoas negras de modo desproporcional" (PORTO; ROLIM, 2022, p. 15), inclusive sob riscos fatais, no caso do estudo dos carros automáticos que tinham mais dificuldade de identificar pessoas negras durante o percurso.

Em razão de tais circunstância, a regulação emerge como um caminho para, ao menos, mitigar estes riscos, tendo em vista que, hoje, o Estado implementa esta tecnologia nas cidades brasileiras sem qualquer regulação que proteja os dados sensíveis da população (SILVA; FRANQUEIRA; HARTMANN, 2021, p. 10), tornado a população mais vulnerável ao controle, sem limites, do Estado.

4.1. A Legislação brasileira sobre o tema e perspectivas regulatórias

As tecnologias de reconhecimento facial coletam dados únicos da projeção da face dos indivíduos. Este dado coletado, de acordo com a Lei Geral de Proteção de Dados (LGPD — Lei 13.709/18), é denominado biométrico, portanto, sensível (PORTO; ROLIM, 2022, p. 19).

Ademais, sob perspectiva histórica, normas "como o Marco Civil da Internet (12.965/2014), as Leis do Cadastro Positivo (Lei 12.414/2011) e Habeas Data (Lei 9.507/1997) e os decretos 6.135/2007, 6.425/2008 e 6.523/2008" (COSTA, 2020, p. 20) já tornavam possível o debate acerca da proteção à exposição indevida, como no caso dos usuários da ViaQuatro, concessionária do metrô de São Paulo, citada no tópico anterior.

Em relação à LGPD, embora seja uma legislação mais recente, já havia algumas leis e decisões que tratavam sobre a matéria da proteção de dados biométricos e da imagem, pois ela,

também se “baseou-se na Constituição brasileira de 1988, no que diz respeito à privacidade e ao direito à imagem” (COSTA, 2020, p. 19).

Conforme foi introduzido nos tópicos anteriores, um meio para regular a atuação estatal na utilização dos dados pessoais foi proposto pela Lei Geral de Proteção de Dados a qual dispõe sobre o tratamento dos dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público, ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural (BRASIL, 2018).

Importa destacar que a lei adverte que a administração pública deverá atuar prezando pelo interesse público e na melhor forma de aplicar as políticas públicas no âmbito do gerenciamento no tratamento e armazenamento dos dados. No artigo 3.º da lei, esta atribuição é ratificada, a qual dispõe que a LGPD é aplicável “a qualquer operação de tratamento realizada por pessoa natural ou por pessoa jurídica de direito público ou privado, independentemente do meio, do país de sua sede ou do país onde estejam localizados os dados” (BRASIL, 2018).

Todavia, a lei também prevê algumas exceções, conforme introduzido nos tópicos anteriores, de forma taxativa, no artigo 4.º:

> Art. 4º Esta Lei não se aplica ao tratamento de dados pessoais: I - realizado por pessoa natural para fins exclusivamente particulares e não econômicos; II - realizado para fins exclusivamente: a) jornalístico e artísticos; ou b) acadêmicos, aplicando-se a esta hipótese os arts. 7º e 11 desta Lei; III - realizado para fins exclusivos de: a) segurança pública; b) defesa nacional; **c) segurança do Estado**; ou **d) atividades de investigação e repressão de infrações penais**; ou IV - provenientes de fora do território nacional e que não sejam objeto de comunicação, uso compartilhado de dados com agentes de tratamento brasileiros ou objeto de transferência internacional de dados com outro país que não o de proveniência, desde que o país de proveniência proporcione grau de proteção de dados pessoais adequado ao previsto nesta Lei (BRASIL, 2018).

No que tange as situações previstas no inciso III, em especial as alíneas c) e d) do artigo, a lei não deixa as exceções num limbo. Assim, ela estabelece no § 1º do artigo 4º, que estas exceções, deverão ser regidas por regulação própria, atendendo ao interesse público, o devido processo legal e as garantias de proteção aos dados previstas na LGDP:

> 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 (BRASIL, 2018).

Portanto, na utilização de tecnologias de reconhecimento para aplicação na segurança pública brasileira, pelo Estado, estas deveriam ser aplicadas seguindo uma regulação específica, no entanto, ainda não há regulação que trate sobre esta matéria, embora tais tecnologias estejam presentes com esta finalidade em diversas cidades e municípios brasileiros. Além disso, os processos de licitações para aquisição destas ferramentas, seguem crescentes em todo território nacional[34].

A liberdade para transitar em espaços públicos, assim como os seus usos, devem ser vistos inteiramente vinculados ao princípio da dignidade humana, previsto no artigo 1º, inciso III, da Constituição Federal, pois, é um princípio baseado no respeito não somente entre os indivíduos e o corpo social, mas também em relação Estado:

> Cuida-se, a um só tempo, de uma garantia de posições contra tratamento inadequado e de fonte de obrigação de tratamento adequado. É dizer: deve-se garantir aos indivíduos a possibilidade de pleno e livre desenvolvimento de sua personalidade a partir de um sistema recíproco de respeito por todos que se encontram inseridos em uma dada realidade (PORTO; ROLIM, 2022, p. 16).

Desse modo, tendo em mente o direito como instrumento que viabiliza a dignidade do ser humano, esta, não pode ser ignorada, tendo em vista esse "relevante papel da jurisdição constitucional que, a partir do diálogo entre código e constituição, pode conduzir a soluções juridicamente racionais e aceitáveis para complexos problemas da vida humana" (PORTO; ROLIM, 2022, p. 16).

Logo, devido à sensibilidade do tema e seus impactos discriminatórios sobre as minorias defendidos por diversos estudos, Porto e Rolim (2022, p. 19) sustentam a necessidade da criação de leis, em paralelo com um amplo debate de diversos setores da sociedade, que tratem especificamente do uso destas tecnologias sem inviabilizar sua existência, mas também protegendo o direito dos cidadãos, em esfera nacional:

> Portanto, diante do volume e da sensibilidade dos dados coletados e processados e dos potenciais reflexos no direito ambulatorial dos cidadãos, ressoa inequívoca a necessidade de elaboração de lei específica uniforme, de alcance nacional, a qual estabeleça balizas normativas que viabilizem o uso da tecnologia e, ao mesmo tempo, preserve direitos e garantias fundamentais, não sendo suficiente a edição de normas locais (...) Deve-se promover discussões amplas com a participação de diferentes setores da sociedade, similarmente ao que aconteceu durante aproximadamente oito anos em relação à LGPD e vem ocorrendo em relação à 'LGPD penal (PORTO; ROLIM, 2022, p. 19).

[34]Ver em: https://agenciabrasil.ebc.com.br/geral/noticia/2019-09/tecnologias-de-reconhecimento-facial-sao-usadas-em-37-cidades-no-pais

Como já exposto, a LGPD, embora trate sobre a proteção de dados, ela trata como excludente da lei, no artigo 4º, inciso III, alínea a), os casos em que a finalidade for exclusivamente da matéria de segurança pública, prevendo a necessidade de criação de lei específica para regular essa matéria, sem deixar de observar os princípios gerais de proteção de dados, os direitos do titular e o devido processo legal (ALMEIDA, 2022, p. 265), considerando o interesse público na atuação pelo Estado.

Em razão da "opacidade dos algoritmos utilizados" em conjunto com a "falta de transparência" dos entes públicos acerca de seus processos, não possibilitam à população que se tenha ciência de como são "tratados os dados que lhe digam respeito" (PORTO; ROLIM, 2022, p. 19) e, ainda, traz empecilhos para a limitação do poder do Estado em relação às condutas abusivas que podem sobrevir sob o pretexto de "enfraquecimento da conduta criminosa" (PORTO; ROLIM, 2022, p. 19).

Dando importância às preocupações apontadas por organizações da sociedade civil em relação à privacidade e acurácia do sistema no processo de detecção e identificação de faces do sistema, algumas movimentações do governo brasileiro para a regulamentação desta tecnologia têm surgido. A audiência pública na Comissão de Ciência e Tecnologia, Comunicação e Informática, organizada pela Câmara dos Deputados, com participação de diversos setores da sociedade para discutir a aplicação de reconhecimento facial para manutenção da segurança pública, em 2019, é um destes exemplos (ALMEIDA, 2022, p. 265).

Em diversos países e cidades ao redor mundo, a tecnologia de reconhecimento facial em sido proibida devido as suas controvérsias, no entanto, no Brasil, o cenário é diferente. Cada vez mais, as cidades brasileiras, como Minas Gerais, Rio de Janeiro, Espírito Santo, Distrito Federal, dentre outras, têm aberto processos licitatórios e parcerias para aquisição desta IA para fins de segurança pública[35]. Contudo, a LGPD, de acordo com o vimos neste tópico, não é suficiente para regular matéria de segurança pública, cabendo, portanto, a criação de lei específica para tratar e dispor desta matéria.

[35] (DE 2019; 11H50, [s.d.])

4.2. Casos concretos

Não são novos os problemas trazidos pelo racismo no contexto da sociedade brasileira, até mesmo, porque o racismo permeia a história do Brasil desde seu início como nação. Como alguns de seus reflexos sobre a população negra, há as maiores taxa de mortes violentas, minorias em posições de nível hierárquico superior no mercado de trabalho e possuem menores salários em uma mesma função; são maioria em situação de pobreza e vulnerabilidade social; maioria no sistema carcerário; minoria no ensino superior e nas taxas de alfabetização (ARAÚJO; CARDOSO; PAULA, 2021, p. 7; UOL, [s.d.]; VALOR, 2019).

Sobre o cenário citado, recomenda-se que ele seja pensado como base quando ao tratar da implementação as tecnologias de inteligência artificial no Brasil, pois, como já foi exposto repetidamente ao longo deste trabalho, os algoritmos não neutros, mas são dotados de vieses daqueles que as programam e alimentam as suas bases de informação.

Embora haja este contexto que pode resultar em diversas violações aos direitos constitucionais como à privacidade, liberdade e igualdade, bem como a proteção de dados como um direito da personalidade, ainda assim, se expandido ao redor do Brasil sem amplo debate da população sobre seus riscos, frente ao seu largo crescimento.

A acurácia prejudicada destes sistemas, principalmente no que tange as pessoas pretas e pardas, população que já maioria em prisões equivocadas por reconhecimento fotográfico, pode piorar o quadro atual de prisões injustas e de encarceramento em massa. Por conseguinte, a vigilância e o controle sobre a população negra "já ocorre atualmente sem o uso indiscriminado de novas tecnologias auxiliares de repressão policial" (PORTO; ROLIM, 2022, p. 15). As implementações das câmeras de reconhecimento ainda crescem nas cidades brasileiras, mas, apenas no ano em que começou, em 2019, graves erros aconteceram, conforme será visto a seguir.

No estado do Rio de Janeiro, no ano de sua implementação, em 2019 durante o Carnaval, em apenas de 3 meses de uso da tecnologia, mais de 50 pessoas foram presas. As câmeras foram instaladas no bairro de Copacabana, área nobre localizada na Zona Sul do Estado e no entorno do estádio Maracanã, na Zona Norte.

Foram instaladas 34 câmeras de reconhecimento facial e o projeto foi feito em parceria com a empresa Oi (parceira da empresa Huawei, chinesa, da qual importa a tecnologia), de forma gratuita, sem onerar os cofres públicos. "O sistema atua de forma integrada ao Centro Integrado de Comando e Controle (CICC) da PMERJ, que recebe as imagens em tempo real".

A base de dados utilizada para identificar foragidos da Justiça, veículos roubados e até torcedores proibidos de frequentar estádios, são oriundas do banco de dados da Polícia Civil (DIA, 2021; G1 RIO, 2019).

No mesmo ano, em julho, exatamente no mês em que quantidade de câmeras instaladas saltou de 34 para 140, houve duas pessoas identificadas pelo sistema como foragidas injustamente (SILVA; FRANQUEIRA; HARTMANN, 2021).

Nesse período, uma mulher foi presa injustamente, identificada como foragida da justiça, sob acusação do delito de homicídio e de ocultação de cadáver, o que motivou a sua prisão, no entanto, ao chegar na delegacia, constatou-se que não se tratava da mesma pessoa e o Porta-Voz da Policia Militar do Estado informou que foi feito o pedido de desculpas e a parte foi liberada (SBT NEWS, 2019).

Além disso, após alguns dias, os agentes identificaram que a pessoa que estava como procurada no sistema já estava cumprindo pena, há 4 anos (ARAÚJO; CARDOSO; PAULA, 2021, p. 9) e é com esta base de dados comprovadamente desatualizada que este projeto de segurança pública tem sido implementado. Como se o erro já não fosse o bastante, após alguns dias mais uma pessoa foi presa por engano.

No ano seguinte, uma audiência pública na Assembleia Legislativa do Estado do Rio de Janeiro (ALERJ), foi realizada para debater as prisões por falhas no reconhecimento facial. De acordo com o relatório da Defensoria Pública do Estado em conjunto com o Conselho Nacional das Defensoras e Defensores Públicos-Gerais (CONDEGE), pelo menos 90 pessoas haviam sido presas injustamente com base em reconhecimento fotográfico, no período de 2012 a 2020 (DIA, 2021).

Outro caso emblemático, ocorreu no Estado do Piauí, onde o pedreiro José Domingos Leitão, de 52 anos, foi preso injustamente após ser reconhecido equivocadamente pela tecnologia de reconhecimento facial do Estado de Brasília. Ele relatou que os policiais civis do Distrito Federal acordaram ele e sua família com chutes nas portas de casa, aos gritos e ordens para calar a boca. Ele foi preso às 5h da manhã, no dia 7 de outubro de 2020.

Por conta do ocorrido, ele relatou que perdeu diversos trabalhos, porque ficou estigmatizado perante a vizinhança. Ele relata que quando foi algemado, pensou que ou seria preso para o resto da vida ou que seria executado no meio do caminho, sem saber o que fizera, pois, até isso lhe fora negado.

Esses casos também demonstram a dificuldade da responsabilização do Estado nestes erros. Inclusive, a Procuradoria do Distrito Federal declarou que não houve culpa dos agentes da Polícia Civil, porque eles estavam agindo sob ordem de decisão judicial, constante nos registros oficiais (R7 BRASÍLIA, 2021, 2021; RECORD TV BRASÍLIA, 2021).

Conforme apontamento de Rede de Observatórios de Segurança que monitorou a utilização das tecnologias de reconhecimento em 5 estados, identificou que desde março de 2019, nos casos em que foi possível colher informações, cerca de 90,5% dos presos por "monitoramento facial" eram negros. De acordo com o relatório "A Bahia liderou o número de abordagens e prisões com a nova técnica: 51,7% das prisões, seguida do Rio, com 37,1%, Santa Catarina, com 7,3%, Paraíba, com 3,3% e o Ceará, com 0,7%", em sua maioria relacionadas ao tráfico de entorpecentes" (THE INTERCEPT, 2019).

É inarredável a necessidade de se questionar a suposta neutralidade dos algoritmos. Os sistemas de controle social são, como regra, frutos de uma decisão política anterior. Assim, a seletividade do sistema penal, ainda que de forma indireta, acaba por reforçar a repressão sobre categorias de indivíduos que já seriam destinatários naturais do sistema repressivo (PORTO; ROLIM, 2022, p. 16).

Assim, para a população negra, a tecnologia de reconhecimento, do jeito que se apresenta hoje, tem surgido como uma certeza de que ela continuará a ser abordada de forma preferencial, em nome da guerra às drogas e à criminalidade. Desse modo, esta ferramenta tem se mostrado como um novo meio "para o velho e conhecido racismo na base do sistema de justiça criminal e guia o trabalho policial há décadas"[36] (THE INTERCEPT, 2019).

Em casos como os citados, a Porto e Rolim trazem questionamentos importantes:

> A conduta do policial que procedeu à prisão sem verificar se o alvo da diligência era, de fato, quem deveria ser preso, seria penalmente punível? E, na hipótese de inserção de informações dolosas que podem levar à prisão de um indivíduo, haveria responsabilização penal? A constatação de uma falha pelo gestor do tratamento dos dados e a omissão quanto à tomada de providências para sua correção é uma conduta penalmente relevante? (PORTO; ROLIM, 2022, p. 3).

[36] No estudo apresentado pela Intecept uma comparação apresentada sobre o sistema elucida a compensação do sistema: "Se compararmos a técnica com o envio de uma ambulância para socorrer uma vítima, vemos o quanto ela é ineficiente. Se em nove de cada dez chamadas ao Samu não houver uma emergência real, teremos o desperdício de dinheiro público e a alocação inútil de tempo e pessoal. É exatamente o que tem ocorrido na aplicação da tecnologia de reconhecimento facial. Por exemplo, durante o carnaval, nos quatro dias da Micareta de Feira de Santana, na Bahia, o sistema de videomonitoramento capturou os rostos de mais de 1,3 milhões de pessoas, gerando 903 alertas, o que resultou no cumprimento de 18 mandados e na prisão de 15 pessoas, ou seja, de todos os alertas emitidos, mais de 96% não resultaram em nada".

Perguntas como as acima devem ser respondidas de forma esclarecida para a população mediante à implementação destas tecnologias no âmbito da segurança pública e persecução penal nas cidades brasileiras. A população está sendo exposta a um experimento social de controle e vigilância que tenham ciência de tal fato. Com o cruzamento de dados individualizados e populacionais contidos na administração pública, em conjunto com os dados fornecidos pelas “big techs”, podendo ser identificados em tempo real a cada passo dado, revelam uma cultura de vigilância e disciplina dos corpos que não deve ser ignorada.

CONSIDERAÇÕES FINAIS

Mediante a tudo que foi exposto ao longo deste trabalho, conclui-se que ainda existem muitas perguntas que devem ser respondidas pela administração pública e pelas empresas que constroem esta tecnologia antes de sua implementação massiva sobre a população.

Ademais, questiona-se a necessidade desta vigilância ininterrupta do comportamento humano sob o pretexto de proteção à segurança nacional e combate ao crime organizado pelo Estado, às custas do direito à privacidade.

Considerando os enviesamentos, preocupantes, identificados nos algoritmos das tecnologias de reconhecimento facial, e tendo em vista o contexto nacional em que a maioria da população brasileira é composta por pessoas negras e pardas, sem regulação sobre esta matéria, quais garantias essa população têm perante o monitoramento pelo Estado?

Recentemente, foi publicada a notícia de que a Polícia Militar do Estado do Rio de Janeiro (PMERJ) está realizando cotações pata a aquisição de câmeras de reconhecimento facial para serem inseridas no programa Cidade Integrada, nas ruas do Jacarezinho, área pobre, marcada pela ausência da atuação do poder público, detentora de um dos menores índices de desenvolvimento humano (IDH) do município do RJ. Sob a alegação de que “muitas ações policiais são ‘levianamente acusadas de serem eivadas de ilegalidades, excessos e arbitrariedades’, controla-se mais ostensivamente uma população que já é excluída (de garantias básicas como, acesso à educação, saneamento básico, segurança e saúde) e, em simultâneo, perseguida pelo Estado debaixo do pretexto de guerra à criminalidade.

Ainda, no contexto brasileiro, qual é o intuito de promovermos a inserção das tecnologias de reconhecimento facial em território nacional, quando as principais empresas detentoras desta tecnologia, juntamente com algumas cidades e Estados em outros países, estão suspendendo a sua utilização?

A tecnologia não deve ser mais um meio para a segregação de pessoas, reafirmando as discriminações e desigualdades. A inteligência artificial pode sim, ser uma ferramenta importante nas atividades do nosso dia a dia, bem como a sua ramificação na forma de biometria facial, mas não nos moldes que ocorre atualmente, dotada de vieses racistas, obscura e de forma compulsória sem qualquer informação ou notificação as partes interessadas.

A ausência de regulação agrava o problema, pois como poderá haver contraditório e ampla defesa quando a outra parte que imputa o resultado é considerada neutra e dotada de respostas isentas de subjetividades, quase que como um ser "mítico superior", capaz de realizar julgamentos melhores que os humanos, como nos filmes de Hollywood.

Mais uma vez, destaca-se que mais questionamentos foram originados da questão principal que precisam ser esclarecidas: será mesmo que a consolidação de uma sociedade vigilante traz a reposta que irá sanar os impasses relacionados à violência, ou irá agravá-la sob a forma de totalitarismo estatal e, até mesmo, privado? Quem serão os protegidos do controle e quem são os impedidos de ter o seu direito de estar só e ser deixado em paz garantidos? Qual será o custo para se obter privacidade? Pois, conforme exposto no decorrer deste trabalho, áreas e populações mais pobres e marginalizadas costumam ser o cenário principal para experimentos de controle, leia-se o Projeto de Cidade Integrada em implementação nas comunidades do Estado do Rio de Janeiro. Além disso, a quem interessa o controle massivo sobre a população?

No que tange a pesquisa, embora, incialmente, a intenção consistia em verificar se a tecnologia de reconhecimento facial, utilizada pela segurança pública brasileira, seria capaz de colocar o direito à privacidade da população em risco, no decorrer da investigação, identificou-se que, mais que o direito à privacidade, direitos como à liberdade, a autodeterminação, à igualdade, dentre outros, são postos em risco.

Para mais, também se observou que não apenas a biometria facial, mas como as outras tecnologias de inteligência artificial, por meio da sua possível habilidade de modificar comportamentos, pode colocar a democracia em risco, influenciando, inclusive, em nossa capacidade de autodeterminação, livre escolha. Assim, quem tem o poder de influenciar coletivamente, teria, também, o poder de decidir o futuro de uma nação, como em uma eleição presidencial.

Outrossim, foi possível identificar que fenômenos sociais que acontecem no "mundo real", podem ser potencializados através das máquinas, como o racismo e as exclusões que dele decorrem, pois, conforme já fora exposto, não há neutralidade, não há ausência de vieses, quando nos referimos a qualquer processo, inclusive, o tecnológico.

Adicionalmente, o papel das empresas privadas, em que pese não fossem o objeto central da pesquisa, mostraram ter alta relevância, pois, são elas que produzem os sistemas de mineração de dados que são adquiridos pelos entes estatais. E, inclusive, são as propulsoras deste novo capitalismo e modelo de sociedade vigilante que estamos inseridos.

Portanto, ainda há muito para ser explorado acerca das novas tecnologias e as transformações que elas podem causar na sociedade. Aliás, ainda há espaço para muitas discussões no campo da regulação, no que tange aos processos por detrás destas tecnologias e sua implementação no cotidiano, não somente das atividades desempenhadas por instituições públicas, mas também por instituições privadas. Afinal, direitos muito caros estão sendo mitigados constantemente, sem que nem tenhamos dimensão disso. Talvez se não houver intervenção em tempo, poderá ser tarde demais.

REFERÊNCIAS BIBLIOGRÁFICAS

AGÊNCIA BRASIL. **Tecnologias de reconhecimento facial são usadas em 37 cidades no país**. Disponível em: <https://agenciabrasil.ebc.com.br/geral/noticia/2019-09/tecnologias-de-reconhecimento-facial-sao-usadas-em-37-cidades-no-pais>. Acesso em: 13 jan. 2022.

AGÊNCIA BRASIL. **Doria veta projeto para instalação de reconhecimento facial no Metrô**. Disponível em: <https://agenciabrasil.ebc.com.br/politica/noticia/2021-03/doria-veta-projeto-para-instalacao-de-reconhecimento-facial-no-metro>. Acesso em: 13 jun. 2022.

ALMEIDA, E. C. Os grandes irmãos: o uso de tecnologias de reconhecimento facial para persecução penal. **Revista Brasileira de Segurança Pública**, v. 16, n. 2, p. 264–283, 23 mar. 2022.

ARAÚJO, R. DE A.; CARDOSO, N. D.; PAULA, A. M. DE. Regulação e uso do reconhecimento facial na segurança pública do Brasil. **Revista de Doutrina Jurídica**, v. 112, p. e021009–e021009, 30 set. 2021.

BALKO, R. **Condenações injustas roubaram 20 mil anos de inocentes nos EUA**. Disponível em: <https://www.gazetadopovo.com.br/justica/condenacoes-injustas-roubaram-20-mil-anos-de-inocentes-nos-eua-bsb3rajnag8sg1jmcshxsdmvi/>. Acesso em: 8 jun. 2022.

BARROS, J. N. Big Data, Proteção de Dados e Transparência: desafios para a Consolidação da Confiança e Garantia dos Direitos do Cidadão. **Revista Culturas Jurídicas**, v. 7, n. 17, 2020.

BASTOS, E. A. V.; PANTOJA, T. L. S.; SANTOS, S. H. C. S. DOS. Os impactos das novas tecnologias da informação e comunicação no direito fundamental à privacidade / The impacts of new information and communication technologies in the fundamental right to privacy. **Brazilian Journal of Development**, v. 7, n. 3, p. 29247–29267, 23 mar. 2021.

BATISTA, M. G. C. O direito à imagem nas redes sociais. p. 133, 18 out. 2017b.

BBC MUNDO. **O plano chinês para monitorar – e premiar – o comportamento de seus cidadãos**. Disponível em: <https://www.bbc.com/portuguese/internacional-42033007>. Acesso em: 14 jan. 2022.

BBC NEWS BRASIL. **Coronavírus: como a China usa seu sistema de vigilância para conter a covid-19**. , 4 abr. 2020. Disponível em: <https://www.youtube.com/watch?v=bluQdsLiOMU>. Acesso em: 13 abr. 2022

BIG BROTHER WATCH. **Stop Facial Recognition — Big Brother Watch**. Disponível em: <https://bigbrotherwatch.org.uk/campaigns/stop-facial-recognition/>. Acesso em: 11 jun. 2022.

BRASIL. [Constituição (1988)]. **Constituição da República Federativa do Brasil de 1988**. Brasília, DF: Presidência da República, [2020]. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 23 mar. 2022.

Brasil. Lei nº 13.709, de 14 de agosto de 2018. Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet). Brasília, DF: Presidência

da República; 2018. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm>. Acesso em 8 jun. 2022.

BRASIL. 793/2019. Portaria nº 793-2019 - Enfrentamento à Criminalidade Violenta. . 16 jul. 2020.

CANALTECH. **Google vai pagar US$ 100 mi por violação de privacidade em reconhecimento facial**. Disponível em: <https://canaltech.com.br/seguranca/google-vai-pagar-us-100-mi-por-violacao-de-privacidade-em-reconhecimento-facial-218244/>. Acesso em: 9 jun. 2022.

CANCELIER, M. V. DE L. O Direito à Privacidade hoje: perspectiva histórica e o cenário brasileiro. **Sequência (Florianópolis)**, p. 213–239, ago. 2017.

CARVALHO, M. A. Capitalismo de vigilância : a privacidade na sociedade da informação. 27 abr. 2019.

CNN BRASIL. **Na China, há câmeras na porta da casa das pessoas - às vezes, do lado de dentro**. Disponível em: <https://www.cnnbrasil.com.br/internacional/na-china-ha-cameras-na-porta-da-casa-das-pessoas-as-vezes-do-lado-de-dentro/>. Acesso em: 13 jan. 2022.

COSTA, T. K. DA. O uso da tecnologia de reconhecimento facial e a violação a dados biométricos sob a luz da Lei Geral de Proteção de Dados. 6 fev. 2020.

COSTA, R.; DE OLIVEIRA, S. Os Direitos da Personalidade Frente À Sociedade de Vigilância: Privacidade, Proteção de Dados Pessoais e Consentimento nas Redes Sociais (Personality Rights In The Society Of Surveillance: Privacy, Personal Data Protection And Consent On Social Network). 13 fev. 2020.

DIA, O. **“Pensei que minha vida tinha acabado”, diz homem preso por reconhecimento facial em audiência na Alerj | Rio de Janeiro**. Disponível em: <https://odia.ig.com.br/rio-de-janeiro/2021/10/6252323-eu-pensei-que-minha-vida-tinha-acabado-diz-homem-preso-por-reconhecimento-facial-em-audiencia-na-alerj.html>. Acesso em: 14 jun. 2022.

EL PAÍS. **Google conserta seu algoritmo “racista” apagando os gorilas**. Disponível em: <https://brasil.elpais.com/brasil/2018/01/14/tecnologia/1515955554_803955.html>. Acesso em: 8 jun. 2022.

ESTADÃO. **Como uma cidade nos EUA usou inteligência artificial para tentar prevenir crimes**. **Link Estadão**, [s.d.]. Disponível em: <https://link.estadao.com.br/blogs/ligia-aguilhar/policia-usa-inteligencia-artificial-para-prevenir-crimes-eua/>. Acesso em: 8 jun. 2022

ESTADO DE MINAS. **Amazon prorroga suspensão do reconhecimento facial EUA**. Disponível em: <https://www.em.com.br/app/noticia/internacional/2021/05/18/interna_internacional,1267920/amazon-estende-proibicao-de-uso-de-reconhecimento-facial-a-policia.shtml>. Acesso em: 9 jun. 2022.

EXAME. **Número de empresas de tecnologia cresce no Brasil — elas faturam R$ 426 bi**. Disponível em: <https://exame.com/pme/numero-de-empresas-de-tecnologia-no-brasil-cresce/>. Acesso em: 30 maio. 2022.

FALK, M.; RODRIGUES, R. C. O Problema da Vigilância na Sociedade da Informação Tecnológica: Considerações Introdutórias. p. 13, 2015.

FARIAS, R. VIEIRA; FRANCA, R. P. A Tutela Material e Processual no Meio Ambiente Digital. **A Tutela Material e Processual no Meio Ambiente Digital**, v. 20, p. 291–311, set. 2017.

FGV. **Brasil tem dois dispositivos digitais por habitante, revela pesquisa da FGV | Portal FGV**. Disponível em: <https://portal.fgv.br/noticias/brasil-tem-dois-dispositivos-digitais-habitante-revela-pesquisa-fgv>. Acesso em: 27 jul. 2022.

FOLHA DE S.PAULO. **O que é reconhecimento facial e como ele pode afetar sua vida | FOLHA EXPLICA**. , 11 ago. 2021. Disponível em: <https://www.youtube.com/watch?v=7HuUsntdgWk>. Acesso em: 13 abr. 2022

FORBES. **Forbes Global 2000: veja quais são as maiores empresas do mundo em 2022**. Disponível em: <https://forbes.com.br/forbes-money/2022/05/forbes-global-2000-veja-quais-sao-as-maiores-empresas-do-mundo-em-2022/>. Acesso em: 6 jun. 2022.

G1. **Amazon proíbe uso de sua tecnologia de reconhecimento facial pela polícia por um ano**. Disponível em: <https://g1.globo.com/economia/tecnologia/noticia/2020/06/10/amazon-proibe-uso-de-sua-tecnologia-de-reconhecimento-facial-pela-policia-por-um-ano.ghtml>. Acesso em: 9 jun. 2022.

G1. **IBM encerra área de pesquisa em reconhecimento facial e pede reforma da polícia**. Disponível em: <https://g1.globo.com/economia/tecnologia/noticia/2020/06/09/ibm-encerra-area-de-pesquisa-em-reconhecimento-facial-e-pede-reforma-da-policia.ghtml>. Acesso em: 9 jun. 2022.

G1; GLOBONEWS. **EUA grampearam Dilma, ex-ministros e avião presidencial, revela WikiLeaks**. Disponível em: <http://g1.globo.com/politica/noticia/2015/07/lista-revela-29-integrantes-do-governo-dilma-espionados-pelos-eua.html>. Acesso em: 9 jun. 2022.

G1 RIO. **Sistema de reconhecimento facial da PM do RJ falha, e mulher é detida por engano**. Disponível em: <https://g1.globo.com/rj/rio-de-janeiro/noticia/2019/07/11/sistema-de-reconhecimento-facial-da-pm-do-rj-falha-e-mulher-e-detida-por-engano.ghtml>. Acesso em: 26 maio. 2022.

HUMAN RIGHTS WATCH. **A ameaça global da China aos direitos humanos**. [s.l: s.n.]. Disponível em: <https://www.hrw.org/pt/world-report/2020/country-chapters/337324>. Acesso em: 15 abr. 2022.

INSTITUTO IGARAPÉ. **Infográfico reconhecimento facial no Brasil**. **Instituto Igarapé**, [s.d.]. Disponível em: <https://igarape.org.br/infografico-reconhecimento-facial-no-brasil/>. Acesso em: 9 jun. 2022a

INSTITUTO IGARAPÉ. **Videomonitoramento Webreport**. **Instituto Igarapé**, [s.d.]. Disponível em: <https://igarape.org.br/videomonitoramento-webreport/>. Acesso em: 15 abr. 2022b

KANTAYYA, S. **Coded Bias**. Netflix, , 2020. Disponível em: <https://www.netflix.com/br/title/81328723>. Acesso em: 11 jun. 2022

KAUFMAN, D.; SANTAELLA, L. O papel dos algoritmos de inteligência artificial nas redes sociais. **Revista FAMECOS**, v. 27, n. 1, p. e34074–e34074, 29 maio 2020.

KOERNER, A. Capitalismo e vigilância digital na sociedade democrática. **Revista Brasileira de Ciências Sociais**, v. 36, 15 jan. 2021.

LUDERMIR, T. B. Inteligência Artificial e Aprendizado de Máquina: estado atual e tendências. **Estudos Avançados**, v. 35, p. 85–94, 19 abr. 2021.

MARTIN, K. E. Ethical Issues in the Big Data Industry. Em: GALLIERS, R. D.; LEIDNER, D. E.; SIMEONOVA, B. (Eds.). **Strategic Information Management**. 5. ed. [s.l.] Routledge, 2020. p. 450–471.

MEIRELES, A. V. Algoritmos e autonomia: relações de poder e resistência no capitalismo de vigilância. **Opinião Pública**, v. 27, p. 28–50, 4 jun. 2021.

MENDES, L. S.; MATTIUZZO, M. Discriminação Algorítmica: Conceito, Fundamento Legal e Tipologia. **Direito Público**, v. 16, n. 90, 3 dez. 2019.

MULHOLLAND, C. S. Dados pessoais sensíveis e a tutela de direitos fundamentais: uma análise à luz da lei geral de proteção de dados (Lei 13.709/18). **Revista de Direitos e Garantias Fundamentais**, v. 19, n. 3, p. 159–180, 29 dez. 2018.

MUNDO NEGRO. **Sua melhor versão? Apps que mudam o rosto revelam o racismo clareando pessoas negras**. **Mundo Negro**, 16 jul. 2019. Disponível em: <https://mundonegro.inf.br/sua-melhor-versao-apps-que-mudam-o-rosto-revelam-o-racismo-clareando-pessoas-negras/>. Acesso em: 11 jun. 2022

OLIVEIRA, S. R. DE; COSTA, R. S. O Uso de Tecnologias de Reconhecimento Facial em Sistemas de Vigilância e suas Implicações no Direito à Privacidade. **Revista de Direito, Governança e Novas Tecnologias**, v. 5, n. 2, p. 1–21, 20 dez. 2019.

OLIVEIRA, L. V. et al. Aspectos ético-jurídicos e tecnológicos do emprego de reconhecimento facial na segurança pública no Brasil. **Revista Tecnologia e Sociedade**, v. 18, n. 50, p. 114–135, 2 jan. 2022.

ORACLE. **O que é Inteligência Artificial (IA)?** Disponível em: <https://www.oracle.com/br/artificial-intelligence/what-is-ai/>. Acesso em: 27 maio. 2022.

PORTO, V. B.; ROLIM, E. C. O reconhecimento facial e o viés algorítmico racista / Facial recognition and racist algorithmic bias. **Brazilian Journal of Development**, v. 8, n. 5, p. 33349–33371, 3 maio 2022.

PROGRAMARIA. **Algoritmos de Inteligência Artificial (IA) e Vieses: uma reflexão sobre ética e justiça**. **PrograMaria**, 8 maio 2020. Disponível em: <https://www.programaria.org/algoritmos-de-inteligencia-artificial-e-vieses-uma-reflexao-sobre-etica-e-justica/>. Acesso em: 8 jun. 2022

R7 BRASÍLIA. **“Disseram que eu era traficante”, diz pedreiro preso injustamente**. Disponível em: <http://noticias.r7.com/brasilia/disseram-que-eu-era-traficante-diz-pedreiro-preso-injustamente-16122021>. Acesso em: 14 jun. 2022.

RECORD TV BRASÍLIA. **Tecnologia de reconhecimento facial pode causar erros em prisões**. , 17 dez. 2021. Disponível em: <https://www.youtube.com/watch?v=w6QNRpuRN08>. Acesso em: 14 jun. 2022

RODOTÁ, S. **A vida na Sociedade de Vigilância - a privacidade hoje**. Rio de Janeiro: Editora Renovar, 2008.

SAMPAIO, J. A. L. et al. Capitalismo de Vigilância e a Ameaça aos Direitos Fundamentais da Privacidade e da Liberdade de Expressão. **Revista Juridica**, v. 1, n. 63, p. 89–113, 31 mar. 2021.

SAMPAIO, J. A. L.; FURBINO, M.; ASSIS BOCCHINO, L. Capitalismo de vigilância e tecnopolítica: os direitos fundamentais de privacidade e liberdade de expressão sob ataque. **Opinión Jurídica**, v. 20, n. 42, p. 509–527, dez. 2021.

SBT NEWS. **Câmeras de reconhecimento facial auxiliam polícia do Rio | SBT Brasil (04/10/19)**. , 4 out. 2019. Disponível em: <https://www.youtube.com/watch?v=KXOlkpC0jbA>. Acesso em: 14 jun. 2022

SENADO FEDERAL. **Governo quer lei para regular vigilância estatal por meio de reconhecimento facial - Notícias**. Disponível em: <https://www.camara.leg.br/noticias/554826-governo-quer-lei-para-regular-vigilancia-estatal-por-meio-de-reconhecimento-facial/>. Acesso em: 13 jan. 2022.

SILVA, A. V. Segurança Humana e os Cidadãos Europeus: O Impacto do PATRIOT Act e do Foreign Intelligence Amendments Act. **OBSERVARE 2nd International Conference - World War and international Relations**, 3 jul. 2014.

SILVA, J. A. S. DA; MAIRINK, C. H. P. Inteligência artificial: **LIBERTAS: Revista de Ciênciais Sociais Aplicadas**, v. 9, n. 2, p. 64–85, 13 dez. 2019.

SILVA, L. A. DA; FRANQUEIRA, B. D.; HARTMANN, I. A. O que os olhos não veem, as câmeras monitoram: reconhecimento facial para segurança pública e regulação na América Latina. **Revista Digital de Direito Administrativo**, v. 8, n. 1, p. 171–204, 29 jan. 2021.

SILVA, T. DA. Visão Computacional e Racismo Algorítmico: Branquitude e Opacidade no Aprendizado de Máquina. **Revista da Associação Brasileira de Pesquisadores/as Negros/as (ABPN)**, v. 12, n. 31, 7 fev. 2020.

SILVA, V. A. DA. **Direito Constitucional Brasileiro**. [s.l.] Editora da Universidadede São Paulo, 2021.

SILVA, M. L. S. As tecnologias de reconhecimento facial para Segurança Pública no Brasil: perspectivas regulatórias e a garantia de Direitos Fundamentais. 4 abr. 2022.

SIQUEIRA, E. **O mundo na Era do Zettabyte**. **Economia Estadão**, 18 maio 2012. Disponível em: <https://economia.estadao.com.br/blogs/ethevaldo-siqueira/o-mundo-na-era-do-zettabyte/>. Acesso em: 30 maio. 2022

STATISTA. **Total data volume worldwide 2010-2025**. Disponível em: <https://www.statista.com/statistics/871513/worldwide-data-created/>. Acesso em: 30 maio. 2022.

TACCA, A.; ROCHA, L. S. Inteligência artificial: reflexos no sistema do direito. jul. 2018.

THE INTERCEPT. Exclusivo: levantamento revela que 90,5% dos presos por monitoramento facial no Brasil são negros. **The Intercept Brasil**, 21 2019.

THE VERGE. **Google Photos settlement in Illinois to pay out $100 million over biometrics privacy - The Verge**. Disponível em: <https://www.theverge.com/2022/6/6/23156198/google-class-action-face-grouping-biometric-information-illinois-privacy-act>. Acesso em: 9 jun. 2022.

UOL. **Negros são 75% entre os mais pobres; brancos, 70% entre os mais ricos**. Disponível em: <https://noticias.uol.com.br/cotidiano/ultimas-noticias/2019/11/13/percentual-de-negros-entre-10-mais-pobre-e-triplo-do-que-entre-mais-ricos.htm>. Acesso em: 14 jun. 2022.

VALOR. **IBGE: Dos 13,5 milhões vivendo em extrema pobreza, 75% são pretos ou pardos**. Disponível em: <https://valor.globo.com/brasil/noticia/2019/11/13/ibge-dos-135-milhoes-vivendo-em-extrema-pobreza-75percent-sao-pretos-ou-pardos.ghtml>. Acesso em: 14 jun. 2022.

VEJA. **Exposto à internet, robô da Microsoft vira racista em 1 dia | VEJA**. Disponível em: <https://veja.abril.com.br/tecnologia/exposto-a-internet-robo-da-microsoft-vira-racista-em-1-dia/>. Acesso em: 11 jun. 2022.

WILSON, B.; HOFFMAN, J.; MORGENSTERN, J. **Predictive Inequity in Object Detection**. [s.l.] arXiv, 21 fev. 2019. Disponível em: <http://arxiv.org/abs/1902.11097>. Acesso em: 11 jun. 2022.

ZUBOFF, S. Big other: Surveillance Capitalism and the Prospects of an Information Civilization. **Journal of Information Technology**, v. 30, n. 1, p. 75–89, mar. 2015.

ZUBOFF, S. **A era do capitalismo de vigilância: a luta por um futuro humano na fornteira do poder**. Rio de Janeiro: Intrínseca, 2021.