INSTITUTO BRASILEIRO DE ENSINO DESENVOLVIMENTO E PESQUISA - IDP
ESCOLA DE DIREITO DE BRASÍLIA – EDB
CURSO DE GRADUAÇÃO EM DIREITO

PEDRO RAPHAEL VIEIRA MELO

RECONHECIMENTO FACIAL AUTOMATIZADO PARA FINS DE SEGURANÇA PÚBLICA E SEUS RISCOS AOS TITULARES DOS DADOS BIOMÉTRICOS

BRASÍLIA
NOVEMBRO DE 2020

PEDRO RAPHAEL VIEIRA MELO

RECONHECIMENTO FACIAL AUTOMATIZADO PARA FINS DE SEGURANÇA PÚBLICA E SEUS RISCOS AOS TITULARES DOS DADOS BIOMÉTRICOS

Trabalho de Conclusão de Curso apresentado como requisito para a conclusão da graduação em Direito do Instituto Brasileiro de Ensino Desenvolvimento e Pesquisa - IDP

Orientador: Prof. Dr. Guilherme Pereira Pinheiro

BRASÍLIA/DF
NOVEMBRO 2020

PEDRO RAPHAEL VIEIRA MELO

RECONHECIMENTO FACIAL AUTOMATIZADO PARA FINS DE SEGURANÇA PÚBLICA E SEUS RISCOS AOS TITULARES DOS DADOS BIOMÉTRICOS

Trabalho de Conclusão de Curso apresentado como requisito para a conclusão da graduação em Direito do Instituto Brasileiro de Ensino Desenvolvimento e Pesquisa - IDP

Orientador: Prof. Guilherme Pereira Pinheiro

Professor Dr. Guilherme Pereira Pinheiro
Professor Orientador

Professora Dra. Miriam Wimmer
Banca Examinadora

Professor Dr. Márcio Camargo Cunha Filho
Banca Examinadora

RECONHECIMENTO FACIAL AUTOMATIZADO PARA FINS DE SEGURANÇA PÚBLICA E SEUS RISCOS AOS TITULARES DOS DADOS BIOMÉTRICOS

Pedro Raphael Vieira Melo

SUMÁRIO. Introdução. 1 Segurança, dados e vigilância. 2. Sistemas de biometria facial como realidade na segurança pública. 3. O funcionamento de sistemas de reconhecimento de faces. 4. Os riscos do reconhecimento facial automatizado. 4.1. Os riscos envolvidos no tratamento de dados sensíveis-biométricos. 4.2. Os riscos da imprecisão tecnológica no reconhecimento de faces. 4.3. Os riscos de vieses discriminatórios de algoritmos e inteligência artificial. 5. O reconhecimento facial automatizado para fins exclusivo de segurança pública. 5.1. O Anteprojeto de Lei de Proteção de Dados para Segurança Pública e Persecução Penal – LGPD Penal e o reconhecimento facial. Considerações finais.

RESUMO

O artigo discorre sobre o emprego de tecnologias de reconhecimento facial como ferramenta destinada à segurança pública nas cidades. Para tanto, é descrita a sociedade da vigilância, conforme sugerem alguns autores, decorrente do desenvolvimento tecnológico e tratamento de dados dos indivíduos. Em seguida, considerando a crescente mobilização de centros urbanos na instalação de leitores faciais autônomos, embasados inteligência artificial e *machine learning*, é descrita a dinâmica e funcionamento da tecnologia para, enfim, adentrarmos nos riscos envolvidos de tal atividade. Para tanto, são destacados três espécies de riscos, os quais impactam direitos e garantias fundamentais. Por fim, são tecidos comentários acerca da Lei Geral de Proteção de Dados – LGPD e seu papel nessa realidade, bem como o Anteprojeto da Lei Geral de Proteção de Dados para Segurança Pública e Persecução Penal – LGPD Penal e o que se aguarda desse documento no âmbito de tratamento de dados biométricos pelas autoridades de segurança pública.

Palavras-chave: Reconhecimento facial; inteligência artificial, *machine learning*; algoritmos; privacidade e não-discriminação.

INTRODUÇÃO

O Direito não está apartado dos acontecimentos do mundo e das transformações sociais. Muito pelo contrário. O delinear da humanidade a todo momento concebe novas formas de pensar, implicando novos fatos e consubstanciando novas relações jurídicas. Dessa forma, cada momento histórico perpassa seus desafios, bem como a busca de soluções às suas questões.

Atualmente, a disciplina jurídica se debruça cada vez mais em entender o fenômeno tecnológico e suas implicações às relações humanas. Para tanto, é dito o caráter ubíquo da tecnologia informacional no cotidiano contemporâneo[1], de maneira que, a todo o momento, os indivíduos se encontram envoltos pelo processamento de dados e informações pessoais[2]. Compreender esse novo fenômeno e suas implicações jurídicas é tarefa necessária, configurando o tratamento de dados pessoais insumos de transformação para o mundo de hoje.

Com isso, para além do modelo mercadológico-econômico digital em afirmação, âmbito no qual é sustentado a preeminência dos dados pessoais como insumo econômico[3], observa-se ainda implicações decorrentes dessa nova realidade em outros setores do cotidiano humano, a exemplo do tratamento de dados pessoais pela Administração Pública com a finalidade de prestação de serviços e políticas públicas. Nessa linha, importante fim a que destina o Poder Público cinge na prestação de segurança pública, compreendida como dever do Estado e direito e responsabilidade de todos - Art. 144, CF/88.

---

1 Sobre o caráter ubíquo das tecnologias informacionais, conforme lecionado por Laura Scheter Mendes, observa-se que "Trata-se do processamento onipresente de dados, que designa o fenômeno segundo o qual a tecnologia da informação e o processamento de dados perpassam todas as áreas da vida de um indivíduo". MENDES, Laura Schertel. **Privacidade, proteção de dados e defesa do consumidor: linhas gerais de um novo direito fundamental**. São Paulo: Saraiva, 2014, livro digital, p. 79.

2 Quanto a diferenciação técnica dos termos "dado" e "informação", Danilo Doneda logo leciona o "dado" como "informação" em potencial. Nesse sentido, "o dado, assim, estaria associado a uma espécie de "pré-informação", anterior à interpretação e a um processo de elaboração. A informação, por sua vez, alude a algo além da representação contida no dado, chegando ao limiar da cognição". DONEDA, Danilo. **Da privacidade à proteção de dados: fundamentos da Lei geral de proteção de dados** – 2ª ed. São Paulo: Thomson Reuters Brasil, 2019, p. 136.

3 Nesse sentido, conforme exposto por Bruno Bioni, observa-se que "com a inteligência gerada pela ciência mercadológica, especialmente quanto à segmentação dos bens de consumo (marketing) e sua promoção (publicidade), os dados pessoais dos cidadãos converteram-se em um fato vital para a engrenagem da economia da informação. E, com a possibilidade de organizar tais dados de maneira mais escalável (e.g., Big Data), criou-se um (novo) mercado cuja base de sustentação é a sua extração e comodificação. Há uma 'economia de vigilância' que tende a posicionar o cidadão como um mero expectador das suas informações". BIONI, Bruno Ricardo. **Proteção de dados pessoais: a função e os limites do consentimento.** Rio de Janeiro: Forense, 2019. p. 12-13.

Atinente a isso, na esperança de otimizar a prestação de segurança pública frente a um contexto de violência, altos índices de criminalidade e generalizado sentimento de insegurança, observa-se a apreensão das autoridades públicas na instalação de sistemas autônomos de reconhecimento facial, valendo-se o Estado do desenvolvimento tecnológico para concretizar deveres a si impostos.

Nessa linha, o presente trabalho se atém aos desafios que acompanham o desenvolvimento tecnológico, em específico sobre sistemas autônomos de reconhecimento de faces, o qual traz consigo preocupações quanto os limites de emprego de novas ferramentas tecnológicas. Logo, o desafio jurídico é posto em balancear o interesse público à segurança em contrapartida a valores fundamentais, tais como privacidade e a não discriminação.

Portanto, sem qualquer pretensão de esgotar a matéria, o presente trabalho visa explorar o emprego do reconhecimento facial para fins de segurança pública, temática a qual perpassa o tratamento de dados pessoais sensíveis, bem como os riscos próprios dessa atividade e eventual necessidade de regulamentação.

Como problema, temos a ausência de legislação específica que permita o Estado a empregar leitores faciais automatizados em locais públicos para fins de segurança da população, prática essa amplamente difundida em diversas cidades brasileiras e que requer maiores debates quantos os riscos envolvidos.

A hipótese levantada é que, assim como apresentado pela própria Lei Geral de Proteção de Dados - LGPD, tal prática não se encontra em vácuo absoluto, vez que, não obstante a recente legislação excetuara sua incidência na hipótese de tratamento de dados para fins segurança, há que se observar os princípios gerais de proteção de dados e os direitos do titular. Ademais, visualiza-se ainda discussões no âmbito do legislativo que visa preencher tal lacuna.

Acerca do corte metodológico, portanto, o artigo se debruça sobre a tecnologia problematizada, descrevendo-a e expondo os seus riscos, conforme levantamento bibliográfico acerca da matéria.

1. SEGURANÇA, DADOS E VIGILÂNCIA

É incontroverso que muitos centros urbanos padecem de segurança pública, constituindo tal fenômeno social enorme preocupação e desafio ao bem estar das cidades. Para tanto, são correlacionados fatores como violência urbana e criminalidade social, o que requer políticas públicas do Estado para reordenar o sentimento de proteção por parte dos indivíduos[4].

De imediato, observa-se que a Constituição Federal logo garante o direito social à segurança[5] - Art. 6º, de modo a demandar do Poder Público a prestação de condições que possibilitam a percepção de ordem social e preservação do indivíduo e seus bens. Ainda, o texto constitucional é explícito ao definir a segurança pública como "dever do Estado e direito e responsabilidade de todos" [6] - Art. 144, ficando ponto de partida quanto a pretensão dos indivíduos em não se verem intimidados ou tolhidos de suas liberdades.

Nesse sentido, conforme abordado por Robson Sávio Reis Souza,

> Definir segurança pública é uma tarefa bastante complexa. Mais que uma definição conceitual, trata-se de compreensão do que vem a ser a efetivação de políticas associadas a direitos e deveres, cidadania, uso legítimo da força, limites do poder estatal, lei e ordem, entre outros.[7]

Segundo dados do Anuário Brasileiro de Segurança Pública, formulado pelo Fórum Brasileiro de Segurança Pública – FBSP, o Brasil se destaca por elevados números absolutos de crimes praticados contra a vida e contra o patrimônio, o que transmite às populações a sensação de medo e insegurança. Segundo os número da pesquisa, no ano de 2019 foram contabilizados 57.358 mortes por homicídios[8], enquanto que, referente à tutela do patrimônio

---

[4] O tema da segurança pública no Brasil é assunto complexo e afeto à políticas públicas de Estado. Nesse sentido, segundo Robson Sávio Reis Souza, "A ação do Estado na garantia da segurança pública é fundamento das sociedades democráticas. Para tanto, o Estado deve agir de modo isonômico, prevenindo os crimes e punindo, proporcionalmente e dentro dos limites da lei, os infratores". Souza, Robson Sávio Reis. **Quem comanda a segurança pública no Brasil? Atores, crenças e coalizões que dominam a política nacional de segurança pública**. Editora Letramento. Belo Horizonte, 2015, p. 22.

[5] BRASIL. Constituição da República Federativa do Brasil. Art. 6º. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicaocompilado.htm.

[6] BRASIL. Constituição da República Federativa do Brasil. Art. 144. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicaocompilado.htm.

[7] Souza, Robson Sávio Reis. **Quem comanda a segurança pública no Brasi?: atores, crenças e coalizões que dominam a política nacional de segurança pública**. Editora Letramento. Belo Horizonte, 2015, p. 52.

[8] 14º Anuário Brasileiro de Segurança Pública, Disponível em https://forumseguranca.org.br/publicacoes_posts/atlas-da-violencia-2020/ <acesso em 21.10.2020>.

dos particulares, foram registrados 490.956 furtos ou roubos de veículos e 22.334 registros de roubos de cargas[9].

Diante desse contexto de anomalia e medo, opção em voga à disposição Poder Público, como estratégia de segurança pública, cinge na instalação de câmeras e sistemas de vigilância em cidades, sobre os quais são depositadas esperanças para contribuir na repressão, por meio da identificação de indivíduos suspeitos, ou mesmo prevenção de ocorrência de crimes. Para tanto, valendo-se de tecnologias de reconhecimento de faces, embasadas em análises biométricas na identificação de pessoas, pretende-se a vigilância da população como método de promoção de segurança[10].

A proposta, apesar de polêmica, demonstra ser promissora nos centros urbanos, conforme exposto mais adiante. Porém, ao mesmo tempo, é vista por alguns juristas como controversa, vez que implementa sistemas de vigilância ao redor de cidades que, ao final, podem vulnerar direitos fundamentais, tais como a liberdade, privacidade e não-discriminação. Nesse sentido, como manifestado por Ricardo Lewandowski:

> o maior perigo para a Democracia nos dias atuais não é mais representado por golpes de Estado tradicionais, perpetrados com fuzis, tanques ou canhões, mas pelo progressivo controle da vida privada dos cidadãos, levado a efeito por governos de distintos matizes ideológicos, mediante a coleta maciça e indiscriminada de informações pessoais, incluindo, de maneira crescente, o reconhecimento facial. E esses dados são submetidos ao novo instrumental da tecnologia de informações denominado *big data*, que consegue armazenar, interligar e manipular uma enorme quantidade de dados, para o bem ou para o mal. [11]

Para alguns autores, a exemplo de David Lyon, o panorama acima é intitulado como *surveillance*, termo o qual está relacionado à "vigilância concentrada, sistematizada e rotineira em relação aos dados pessoais dos indivíduos, cujo objetivo é influenciar, gerenciar, proteger ou dirigir" pessoas. A propósito dessa vigilância digital:

---

9 *Idem.*

10 Acerca do emprego de tecnologias de reconhecimento facial pelo Poder Público, "A aproximação e normalização dessas tecnologias como coadjuvantes do dia a dia da governança da segurança pública, dos meios de transportes, das cidades, de redes sociais, e de dispositivos inteligentes estabelece um sistema de vigilância baseado em práticas de ordenamento e ordem social". Hurel, Louise Marie. Reconhecimento facial – regular, banir ou punir? Revista Insight Inteligência, Jan/Fev/Mar - edição 84. Disponível em: https://insightinteligencia.com.br/reconhecimento-facial-regular-banir-ou-punir-2/. Acesso em 15.11.2020.

11 Manifestação do Ministro Ricardo Lewandowski no âmbito do julgamento do Referendo da Medida Cautelar na ADI 6.387. BRASIL. Supremo Tribunal Federal (STF). **Ação Direta de Inconstitucionalidade n. 6.387/DF MC-Ref**. Autor: Conselho Federal da Ordem dos Advogados do Brasil. Relator(a): Min. Rosa Weber. Brasília. Julgado em 07/05/2020, divulgado11.11.2020.

> Um dos processos-chave para caracterizar a *surveillance* é o atual uso de bancos de dados indexáveis no processamento de dados para diversas finalidades. Entende-se, portanto, que as novas infraestruturas da tecnologia da informação, ao permitirem o processamento em tempo real e o armazenamento ilimitado de dados, não apenas "qualificam" a vigilância, mas introduzem mudanças qualitativas que permitem um "salto" em direção ao conceito de *surveillance*. [12]

Como se vê, as tecnologias de reconhecimento facial, imersas no contexto de tratamento de dados de terceiros, mostram-se como ferramentas à disposição da vigilância e auxílio na segurança pública. Para tanto, é noticiado que "as câmeras são um exemplo claro de como o investimento em inteligência policial pode ajudar a reduzir a violência", ou ainda exemplos concretos do tipo "a Secretaria de Segurança Pública da Bahia relaciona o uso da tecnologia [de reconhecimento de faces] à queda de 18% nos roubos e de 5% nos furtos de veículo no primeiro semestre de 2019" em comparação com o mesmo período no ano anterior[13].

Portanto, atualmente, os debates acerca segurança pública e vigilância da sociedade também perpassam as tratativas de proteção de dados pessoais, em especial com o advento de tecnologias de vigilância, contexto esse que deve ser lido com cautela e atenção.

2. SISTEMAS DE BIOMETRIA FACIAL COMO REALIDADE NA SEGURANÇA PÚBLICA

A dar concretude ao contexto de *surveillance* acima referido, observa-se que as cidades cada vez mais se mobilizam na instalação de tecnologias de reconhecimento de faces em suas respectivas extensões. Em preliminar contagem realizada pelo Instituto Igarapé[14], observou-se pelo menos trinta e sete cidades brasileira que já dispõem de sistemas biométricos faciais em locais públicos destinados à segurança pública, número esse crescente a cada ano. Para tanto, verifica-se a experiência de alguns locais, como o Distrito Federal, Salvador, Rio de Janeiro, Campinas e Teresina, descritos a seguir.

Primeiramente no Distrito Federal, observa-se a movimentação das autoridades públicas para, em breve, instalar leitores faciais de forma definitiva em regiões de grande movimentação,

---

[12] BAUMAN, Zygmunt; LYON, David. **Vigilância líquida**. Rio de Janeiro: Zahar, 2014. E-book. (1 recurso online). ISBN 9788537811771. Disponível em: https://integrada.minhabiblioteca.com.br/books/9788537811771. Acesso em: 20.11. 2020.

[13] Disponível em <https://exame.com/revista-exame/nao-ha-onde-se-esconder/>. Acesso em 21.10.2020.

[14] Disponível em: <https://igarape.org.br/infografico-reconhecimento-facial-no-brasil/>. Acesso em 10.11.2020.

a exemplo da Rodoviária Central do Plano Piloto e demais pontos centrais da cidade[15]. Inclusive, a tecnologia já foi empregada em caráter de testes durante as festas de carnaval deste ano, tendo como finalidade o reconhecimento de pessoas suspeitas ou foragidas dos órgãos de segurança em meio às multidões[16]. Para tanto, insta salientar a recente sanção da Lei Distrital nº 6.712/2020, a qual disciplina o uso de tecnologias de reconhecimento facial na segurança pública da cidade.

Alguns outros episódios igualmente merecem destaque por demonstrar a disseminação da tecnologia, a exemplo da utilização de leitores faciais no Rio de Janeiro e em Salvador, também durante os festejos de carnaval de 2019 e 2020. Em específico à capital carioca, as autoridades públicas noticiaram que o auxílio da ferramenta resultou em quatro prisões de indivíduos tidos como foragidos do sistema prisional[17]. Por sua vez, na capital baiana, o uso da ferramenta auxiliou a identificação de 42 pessoas foragidas[18].

Ademais, em Campinas, destaca-se a recente ampliação dos sistemas de monitoramento por meio de câmaras e sistemas inteligentes. Após acordo com a empresa *Huawei*, o prefeito comemorou o programa "Campinas Bem Segura", o qual conta com aproximadamente 500 câmeras espalhadas em locais públicos da cidade[19].

Já em Teresina, o Banco Nacional de Desenvolvimento Econômico e Social - BNDES projetou investimentos em sistemas autônomos de inteligência e reconhecimento facial, os quais seriam destinados à segurança pública da capital piauiense. Logo, o banco informou o aporte de R$ 29,9 milhões, estimando que, após o implemento da tecnologia, 45% das ocorrências serão identificadas com o auxílio do videomonitoramento até o ano de 2023[20].

As cidades brasileiras não estão isoladas nesse contexto, sendo dignas de passagem algumas experiências internacionais. À distância, assistimos aos intensos debates quanto o

---

15 Disponível em https://www.correiobraziliense.com.br/cidades-df/2020/11/4888246-rodoviaria-do-plano-e-um-dos-locais-que-deve-ter-o-reconhecimento-facial.html <acesso em 20.11.2020>.

16 Disponível em <https://www.correiobraziliense.com.br/app/noticia/cidades/2020/02/21/interna_cidadesdf,829615/reconhecimento-facial-sera-utilizado-pela-primeira-vez-no-carnaval.shtml>. Acesso em 20.11.2020.

17 Disponível em: <https://agenciabrasil.ebc.com.br/geral/noticia/2019-03/cameras-de-reconhecimento-facial-levam-4-prisoes-no-carnaval-do-rio>. Acesso em 17.10.2020.

18 http://www.ssp.ba.gov.br/2020/02/7296/Reconhecimento-Facial-captura-42-foragidos-na-folia.html <acesso em 17.10.2020.

19 Disponível em <https://www.huawei.com/br/news/br/2018/dezembro/campinas-reforca-parceria-com-a-huawei>. Acesso em 20.11.2020.

20 Disponível em <https://www.bndes.gov.br/wps/portal/site/home/imprensa/noticias/conteudo/bndes-apoia-investimento-em-tecnologia-e-inteligencia-para-seguranca-publica-em-teresina>. Acesso em 20.11.2020.

emprego de Reconhecimento Facial Automatizado - RFA em cidades como São Francisco, Oakland, Somerville, nos EUA. Nessas, por ora, as autoridades públicas decidiram por suspender a utilização da ferramenta[21], posto o entendimento de que os benefícios não superam os riscos em seu emprego[22].

Ademais, no continente europeu, destacam-se as experiências do Reino Unido e da França. No primeiro, em síntese, recente decisão do Tribunal de Apelação de Londres considerou a ilegalidade do uso de reconhecimento facial pelos agentes de segurança no País de Gales, tendo em vista a insuficiência de supervisão da tecnologia. Conforme noticiado:

> Segundo a decisão do Tribunal, não existem critérios claros sobre quem pode ser colocado na lista de vigilância ou onde as câmeras de reconhecimento facial podem ser instaladas. Ademais, os juízes apontaram ainda que "muitas coisas são deixadas ao critério de cada policial". A Corte não proíbe o uso de reconhecimento facial no Reino Unido, no entanto limita o escopo de sua aplicação e prevê que as agências que implementarem a tecnologia devem estar em conformidade com as leis de proteção aos direitos humanos. [23]

Por seu turno na França, em específico na cidade de Nice, cada vez mais a temática também ganha corpo, precipuamente após a realização de testes na região da Riviera, a qual contou com a participação de voluntários para aferir a relevância e confiabilidade de leitores faciais em locais públicos. Ao final, contudo, revelou-se a necessidade de mais discussões quanto os impactos na implementação da tecnologia, em especial o desenvolvimento de instrumentos normativos para futuras regulamentações[24].

Ao passo em que é crescente o emprego de RFA em centros urbanos, também aumentam as discussões a respeito dos riscos e efeitos indesejáveis decorrentes de sua utilização. Primeiramente porque a tecnologia lança mão do tratamento e armazenamento de dados pessoais biométricos e, posteriormente, em razão dos algoritmos e sistemas autônomos de

---

[21] Disponível em https://olhardigital.com.br/noticia/san-francisco-pode-ser-a-primeira-cidade-dos-eua-a-banir-o-reconhecimento-facial/85767. Acesso em 17.10.2020.

[22] Disponível em < https://genjuridico.jusbrasil.com.br/artigos/730930166/regulacao-de-reconhecimento-facial-em-sao-francisco>. Acesso em 15.10.2020.

[23] Disponível em: https://www.internetlab.org.br/pt/itens-semanario/reino-unido-uso-de-reconhecimento-facial-pela-policia-galesa-e-considerada-ilegal-por-corte-britanica/. Acesso em 15.10.2020.

[24] Disponível em :<https://www.lemonde.fr/pixels/article/2019/08/28/reconnaissance-faciale-la-cnil-tique-sur-le-bilan-de-l-experience-nicoise_5503769_4408996.html>. Acesso em 16.10.2020.

Inteligência Artificial - IA padecerem de desconfianças decorrentes de possíveis vieses discriminatórios[25] e consideráveis margens de erro em contextos de massa[26].

Logo, não constitui exagero afirmar que tal ferramenta estará cada vez mais presente nas cidades no futuro, as quais se valerão de maciças transferências de dados pessoais, inclusive os biométricos, em sua dinâmica diária. Portanto, o Brasil igualmente está inscrito nesse desafiador contexto de regulamentação das inovações tecnológicas, como é o caso de sistemas autônomos de reconhecimento facial, não devendo se eximir do debate e responsabilidades advindas pela instalação de sistemas de vigilância em locais públicos.

3. O FUNCIONAMENTO DE SISTEMAS DE RECONHECIMENTO DE FACES

Antes de encararmos o debate que se destina o presente trabalho, insta esclarecer a tecnologia ora problematizada. Posto o potencial dos sistemas de vigilância que envolvem biometria facial e o seu respectivo empregado nas cidades para diversas finalidades, exsurge aclarar em que consiste tal ferramenta, sua dinâmica e como a sua utilização implica riscos aos indivíduos.

Inicialmente, destaca-se que a biometria facial versa em espécie do gênero de análise biométrica, dentre o qual também estão contidos outros tipos de identificação do indivíduo, a exemplo daqueles se valem de impressões digitais, leitura da íris ocular, reconhecimento de voz[27] e, inclusive, o andar das pessoas[28]. Nesse sentido, conforme exposto por Juliano Kazienko, verifica-se que a "Biometria é o ramo da ciência que estuda a mensuração dos seres vivos. Em especial, entende-se por biometria a medida de características únicas do indivíduo que podem

---

[25] Nesse sentido, Carlos Nelson Konder expõe que "A segurança sobre o acesso a esses dados e as formas de sua utilização torna-se, então, objeto de necessárias atenção ao direito, uma vez que o tratamento de dados pessoais, em particular por processos automatizados, é uma atividade de risco". KONDER, Carlos Nelson. **O tratamento de dados pessoais sensíveis à luz da lei 13.709/2018**. In Tepedino, Gustavo; Frazão, Ana; Oliva, Milena Donato (Coord.). **Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito brasileiro** – 1ª ed. São Paulo: Thomson Reuters, 2019.

[26] Para além da própria dificuldade e limitação tecnológica, observa-se ainda preocupações quanto a preconceitos e parcialidade dos algoritmos de reconhecimento. Nesse sentido, "muitas situações reais e recentes ilustram esta discussão, como o algoritmo de reconhecimento de imagens do Google que categorizou dois amigos negros como "gorilas" ou quando uma câmera da Nikon, projetada para detectar quando alguém pisca, insistiu que os olhos de uma mulher asiática estavam fechados" Disponível em https://www.jota.info/paywall?redirect_to=//www.jota.info/opiniao-e-analise/artigos/a-tecnologia-de-reconhecimento-facial-aplicada-a-seguranca-publica-23072019. Acesso em 25.10.2020.

[27] Disponível em: https://www.uol.com.br/tilt/noticias/redacao/2020/03/12/fale-e-eu-te-escuto-como-funciona-o-reconhecimento-por-voz.htm. Acesso em 25.09.2020.

[28] Por mais que inusitado que seja, mas a forma de andar de cada pessoa também é passível coleta e identificação de indivíduos. Nesse sentido https://exame.com/tecnologia/china-usa-tecnologia-que-reconhece-pessoas-pelo-jeito-de-andar/. Acesso em 25.09.2020.

ser utilizadas para reconhecer sua identidade. Tais características podem ser tanto físicas como comportamentais"[29].

Para a sua efetiva dinâmica, tal ramo do conhecimento lança mão de métodos estatísticos, biológicos e tecnológicos ao determinar seres vivos, vez que se destina a mensurar cada indivíduo a partir de características que, quando cotejadas às demais individualidades de outros seres, permite a distinção de alguém. Por assim dizer, a biometria se vale de *discrímens* exclusivos para precisar quem é quem.

A propósito, verificam-se duas formas básicas de reconhecimento biométrico, quais sejam, a) biometria de autenticação e b) biometria de identificação. Em síntese,

> Na biometria de autenticação, o processo consiste em comparar o conjunto de dados do indivíduo com o "modelo" biométrico armazenado para determinar a semelhança. Nessa aplicação, a pergunta a ser respondida é: Você é de fato quem diz ser? Na biometria de identificação, por sua vez, o objetivo é capturar um item de dado biométrico e compará-lo aos dados biométricos de vários outros indivíduos mantidos em um banco. Nesse modelo, a questão é simples: Quem é você. [30]

Quanto à primeira forma, embasada na pergunta "você é de fato quem diz ser?", essa é tida como biometria de certificação, motivo pelo qual a sua dinâmica cinge na comparação de determinado dado biométrico a outros previamente agrupados em bancos de dados. Mera utilidade desse modelo se refere às catracas digitais ou senhas biométricas em instituições financeiras, as quais se valem, por exemplo, de impressões digitais para permitir o ingresso de pessoas em determinados locais ou certificar a identidade de titulares para operações financeiras.

Já na segunda forma, compreendida na pergunta "quem é você?", verifica-se que essa se destina a constatar a identidade de indivíduos de maneira difusa, perfilando quem quer que seja em determinados ambientes. Disso decorrem algumas preocupações, conforme problematizado mais à frente. A respeito de sua utilidade, observa-se que os sistemas

---

[29] Belanda, Douglas. **Biometria como mecanismo de formação e prova contratual: um olhar para as transações eletrônicas bancárias na sociedade da informação.** Revista dos Tribunais: São Paulo, vol. 1016/2020, jun.2020, p. 43-62.

[30] Disponível em https://www.jota.info/paywall?redirect_to=//www.jota.info/opiniao-e-analise/artigos/a-tecnologia-de-reconhecimento-facial-aplicada-a-seguranca-publica-23072019. Acesso em 25.10.2020.

autônomos de reconhecimento de faces se valem desse modelo para distinguir indivíduos em meio a multidões.

De tal contexto decorre o reconhecimento biométrico facial, o qual, a grosso modo, pode ser considerado como ferramenta que permite a identificação de pessoas a partir de características próprias em cada rosto humano. Para tanto, por intermédio de avançada engenharia de computação, são coletadas métricas faciais, comumente decorrentes de formatos de rostos, bocas e narizes, assim como distâncias de pontos nodais na face humana. Logo, tal qual a capacidade humana na diferenciação de rostos, a máquina espelha a lógica e cognição do ser humano para também distinguir indivíduos.

Nesse sentido, tem-se que "um sistema de reconhecimento facial opera mediante o uso de biometria para mapear características faciais de uma pessoa presente em uma fotografia ou vídeo, comparando as informações obtidas com um banco de dados de rostos conhecidos para encontrar uma correspondência"[31]. Mais ainda sobre a dinâmica de reconhecimento facial por máquinas, observa-se que:

> "Primeiramente, uma foto do rosto da pessoa é capturada a partir de uma foto ou vídeo; em seguida, o software de conhecimento facial analisa a 'geometria' do rosto, identificando fatores como a distância entre os olhos e a distância da testa ao queixo e elaborando uma 'assinatura facial' a partir da identificação dos pontos de referência faciais. O terceiro passo consiste na comparação da assinatura facial – que nada mais é que uma fórmula matemática – a um banco de dados de rostos conhecidos, pré-coletados e armazenados. Finalmente, realiza-se a etapa de determinação em que pode ocorrer a verificação (quando se analisa uma determinada assinatura digital em comparação a uma única outra, já definida) ou identificação (quando se compara determinada assinatura digital a diversas outras constantes do banco de dados) do rosto analisado". [32]

Ponto merecedor de destaque diz respeito ao desenvolvimento de sistemas tidos como "autônomos", os quais desnecessitam de constante controle externo. Por assim dizer "autonomia", entende-se "aquilo que não está sujeito a potência ou influência estranha; que se governa por leis próprias"[33] Tais sistemas independentes estão fundadas em sofisticados

---

[31] NEGRI, Sergio Marcos Carvalho de Ávila; DE OLIVEIRA, Samuel Rodrigues; COSTA, Ramon Silva. O uso de tecnologias de reconhecimento facial baseadas em inteligência artificial e o direito à proteção de dados. **Direito Público**, [S.l.], v. 17, n. 93, jul. 2020. ISSN 2236-1766. Disponível em: <https://www.portaldeperiodicos.idp.edu.br/direitopublico/article/view/3740>. Acesso em: 10.11.2020.

[32] *Idem.*

[33] Conceito extraído do Dicionário Michaelis, disponível em http://michaelis.uol.com.br/busca?r=0&f=0&t=0&palavra=aut%C3%B4nomo. Acesso em: 20.11.2020.

algoritmos tidos como "inteligentes" e auto programáveis, ambos respectivamente denominados inteligência artificial – IA e *machine learning*.

Logo, o desenvolvimento de plataformas autônomas visa espelhar modelos de cognição humana a partir de proposições lógicas, possibilitando o sistema algorítmico a tirar lições próprias de determinados dados e, por conseguinte, retroalimentar sua dinâmica. Com isso, "quanto mais dados forem inseridos no sistema, mais ele (o sistema) aprende"[34].

Nesse sentido, verifica-se que:

> "o aprendizado de máquina (*Machine Learning*) é uma forma de se alcançar ou conseguir essa tal inteligência artificial. É um ramo da inteligência artificial que envolve a criação de algoritmos que podem aprender automaticamente a partir de dados inseridos. Ao invés de os desenvolvedores de software elaborarem enormes códigos e rotinas com instruções específicas para que a máquina possa realizar determinadas tarefas e conseguir resultados (e com isso limitar drasticamente o seu campo de atuação e resultados), no aprendizado de máquina treina-se o algoritmo para que ele possa aprender por conta própria, e até mesmo conseguir resultados que os desenvolvedores dos algoritmos nem mesmo poderiam imaginar anteriormente. Neste treinamento, há o envolvimento de grandes quantidades de dados que precisam ser alimentadas para o algoritmo (ou aos algoritmos envolvidos), permitindo que o algoritmo se ajuste e melhore cada vez mais os seus resultados". [35]

Por fim, evidente que o desenvolvimento desses sistemas está inserido na temática de proteção de dados, mormente a coleta, armazenamento e tratamento de vultuosas quantidade de dados biométricos para compor bancos de dados faciais. Disso decorre diversos riscos pelo manejo de dados pessoais de terceiros, o que conclama a supervisão de leis de proteção de dados e respectivos instrumentos de controle a fim de evitar prejuízos à privacidade, liberdade dos indivíduos ou mesmo desvios de finalidade das informações. Nesse sentido:

> Até pouco tempo, diferentemente das máquinas, apenas os seres humanos poderiam marcar imagens que contém um cachorro, um poste ou placas de trânsito frente àquelas que não os possuem. O algoritmo de aprendizagem constrói um modelo que pode marcar com precisão uma imagem como contendo um cachorro ou não, assim como um ser humano. Uma vez que o nível de precisão é alto o suficiente, a máquina "aprende" como é um cachorro, como ele se parece e a identificá-lo em problemas futuros e semelhantes. Tal tecnologia está presente no algoritmo do *Facebook*, e em tantos outros aplicativos, que já reconhecem muitos dos rostos de amigos do

---

[34] Engelmann, Wilson; Werner, Deivid Augusto. Inteligência artificial e Direito, 159. In Frazão, Ana; Mulholland, Caitlin (coord.). Inteligência artificial e direito: ética, regulação e responsabilidade. São Paulo: Thomson Reuters, 2019.

[35] Reis, Paulo Victor Alfeo. **Algoritmo e o direito**. São Paulo: Almedina, 2020, p. 136.

> usuário em fotos postadas por ele, habilitando a marcação de seus perfis com seus nomes, quer você entenda isso como invasão de privacidade ou não. [36]

Portanto, pelos riscos envolvidos, "a manipulação de dados pessoais digitalizados, por agentes públicos e privados, consiste em um dos maiores desafios contemporâneos do direito à privacidade"[37].

4. OS RISCOS DO RECONHECIMENTO FACIAL AUTOMATIZADO

Dos tópicos anteriores, após demonstrada a contemporaneidade do tema e descrita a dinâmica de sistemas automatizados de reconhecimento facial, emergem duas conclusões parciais: A) a disponibilidade de vultuosas quantidade de dados biométricos é condição necessária para o desenvolvimento de sistemas de reconhecimento de faces, quer seja para compor bancos de dados e viabilizar a identificação de indivíduos, quer seja na calibragem de sistemas autônomos. Logo, sendo esses dados considerados sensíveis, os seus titulares, inevitavelmente, estão sujeitos a riscos discriminatórios sobremaneira. Ainda, B) quanto mais difundidas tecnologias de vigilância sem prévia análise de impacto e riscos, mais vulneráveis e expostos se tornam os indivíduos e, por conseguinte, seus direitos.

A seguir, são expostos alguns dos riscos que envolve a tecnologia de reconhecimento de faces e os respectivos debates que circundam essas questões.

4.1. Os riscos envolvidos no tratamento de dados sensíveis-biométricos

Assente o RFA como espécie de análise biométrica, é eloquente dizer que a identificação de faces se escora no tratamento de dados biométricos, compreendidos esses como dados pessoais sensíveis (Art. 5º, II, LGPD). Quanto a justificação dessa qualidade especial de dado pessoal, conforme lições de Danilo Doneda, observa-se que "a criação de uma categoria de dados sensíveis foi fruto da observação pragmática sobre a diferença dos efeitos do tratamento desta categoria de dados em relação aos demais", de modo que "a própria seleção de quais seriam estes dados considerados sensíveis provém da constatação de que a circulação de

---

[36] *Idem*, p. 138.

[37] Brasil. Supremo Tribunal Federal (STF). Ação Direta de Inconstitucionalidade n. 6.387/DF MC-Ref. Autor: Conselho Federal da Ordem dos Advogados do Brasil. Relator(a): Min. Rosa Weber. Brasília. Julgado em 07/05/2020, divulgado11.11.2020.

determinadas espécies de informação apresentariam um elevado potencial lesivo aos seus titulares, em uma determinada configuração social"[38].

Logo, para informações sobremaneira íntimas e potencialmente discriminatórias, a temática de proteção de dados despertou maior atenção em especificar e tutelar a sua existência. Conforme exposto por Laura Schertel, tal entendimento não é inédito, seja no Brasil e muito menos em outros países, expondo a autora que "o debate acerca dos dados sensíveis acompanha a história da proteção de dados e esteve presente desde o início das discussões acadêmicas e iniciativas legislativas sobre o tema[39]".

Algumas legislações europeias já previam a titulação especial dos dados dos indivíduos desde décadas passadas, a exemplo do disciplinado na Lei Nacional de Dados Pessoais da Suécia, em 1973, seguida por países como a França, Dinamarca e Noruega, em 1978, e Luxemburgo, em 1979[40].

Posteriormente, e de modo comunitário, sobreveio no Continente Europeu a Convenção de Estrasburgo, ou Convenção 108, em 1981, a qual disciplinou que "os dados pessoais relativos a origem racial, saúde, vida sexual e condenações penais somente poderiam ser objeto de tratamento caso o direito interno previsse as garantias adequadas para o seu processamento"[41]. Mesmo que isso não viesse a constar em seu texto, a referida Convenção ainda destoaria sua importância por vincular a temática de proteção de dados à matéria de direitos humanos e liberdades fundamentais[42], assim como veio a refletir na formação da legislação[43], e jurisprudência brasileira[44].

---

38 DONEDA, Danilo. **Da privacidade à proteção de dados: fundamentos da Lei geral de proteção de dados** – 2ª ed. São Paulo: Thomson Reuters Brasil, 2019, p. 143

39 MENDES, Laura Schertel. **Privacidade, proteção de dados e defesa do consumidor: linhas gerais de um novo direito fundamental**. São Paulo: Saraiva, 2014, p. 72.

40 *Idem*

41 *Idem*

42 DONEDA, Danilo. **Da privacidade à proteção de dados: fundamentos da Lei geral de proteção de dados** – 2ª ed. São Paulo: Thomson Reuters Brasil, 2019, p. 194.

43 Nesse sentido, o Art. 2º, VII, da LGPD, expõe que: "A disciplina da proteção de dados pessoais tem como fundamentos: (...) VII - os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais". BRASIL. Lei n. 13.709, de 14 de agosto de 2018. Dispõe sobre a proteção de dados pessoais e altera a Lei n. 12.965, de 23 de abril de 2014 (Marco Civil da Internet). **Diário Oficial [da] República Federativa do Brasil**. Brasília, DF, 14 ago.2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm

44 BRASIL. Supremo Tribunal Federal (STF). **Ação Direta de Inconstitucionalidade n. 6.387/DF MC-Ref**. Autor: Conselho Federal da Ordem dos Advogados do Brasil. Relator(a): Min. Rosa Weber. Brasília. Julgado em 07/05/2020, divulgado em 11.11.2020.

A partir da Diretiva Europeia 95/46/CE o conceito de dados sensíveis ganhou maior uniformidade, a ponto de permitir a proibição de tratamento desses tipos de dados, assim como se deu nas legislações da França, Noruega, Finlândia e Dinamarca. Outros países, por sua vez, adotaram posturas restritivas, a exemplo da Alemanha e Suíça[45], os quais condicionaram o tratamento de dados pessoais sensíveis quando atendidos determinados requisitos expressos em lei.

Atualmente restam vigentes na União Europeia, dentre outros, dois importantes instrumentos normativos sobre a temática de proteção de dados, quais sejam o Regulamento Geral sobre Proteção de Dados 2016/679 – RGPD (ou em inglês, *General Data Protection Regulation* – GDPR) e a Diretiva 2016/680[46], os quais são reconhecidos como marcos ao tratamento de dados na Europa, bem como sobre os dados sensíveis e biométricos[47].

No que tange o RGPD, tal documento, dotado de força normativa no âmbito da União Europeia, corroborou a existência de excessivos riscos a direitos e liberdades fundamentais quando do tratamento de dados que envolvam práticas potencialmente discriminatórias. Nessa linha, conforme exposto em sua Consideração 51, "Merece proteção específica os dados pessoais que sejam, pela sua natureza, especialmente sensíveis do ponto de vista dos direitos e liberdades fundamentais, dado que o contexto do tratamento desses dados poderá implicar riscos significativos para os direitos e liberdades fundamentais"[48].

Por conseguinte, tanto o Regulamento quanto a Diretiva vigentes se ocuparam de idêntico conceito para "dados biométricos", expondo esses como "resultantes de um tratamento técnico específico relativo às características físicas, fisiológicas ou comportamentais de uma pessoa que permitam ou confirmem a identificação única dessa pessoa, notadamente imagens faciais ou dados dactiloscópicos"[49]. Portanto, não à toa as normativas optaram por tutelar tais

---

45 MENDES, Laura Schertel. **Privacidade, proteção de dados e defesa do consumidor: linhas gerais de um novo direito fundamental**. São Paulo: Saraiva, 2014, p. 73.

46 Em relação ao previsto na Diretiva (UE) 2016/680, essa se destina "à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas autoridades competentes para efeitos de prevenção, investigação, detecção ou repressão de infrações penais ou execução de sanções penais, e à livre circulação desses dados".

47 DONEDA, Danilo. **Da privacidade à proteção de dados: fundamentos da Lei geral de proteção de dados** – 2ª ed. São Paulo: Thomson Reuters Brasil, 2019, p. 191

48 EUROPA. General Data Protection Regulation (GDPR). Regulamento Geral sobre a Proteção de Dados. Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016. Disponível versao portugues em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016R0679&from=EN

49 *Idem.*

espécies de dados pessoais, de modo a conceder relevância jurídica quando de seu tratamento por fundado temor na malversações em seu tratamento e riscos discriminatórios.

A propósito da sensibilidade dos dados pessoais no contexto brasileiro[50], Bruno Bioni expõe a perspicácia da legislação brasileira na adoção de um regime próprio para determinadas informações pessoais, referindo-se à seção II, do 2º Capítulo, da LGPD[51]. Para tanto, a lei geral brasileira, à luz das longínquas discussões sobre o tema e normativas do Continente Europeu, precisou os dados pessoais sensíveis como aqueles referentes à "origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural" [52], bem como fixou estreitos requisitos para o seu tratamento, assim como previsto entre os artigos 7° a 9°.

Logo, se se diz que um dado pessoal é sensível, inevitavelmente, isso implica no potencial discriminatório que tal dado carrega em si. Acerca disso, na esteira de Gustavo Tepedino e Chiara S. de Teffé, "essa categoria integra o 'núcleo duro' da privacidade, tendo em vista que, pelo tipo e natureza de informação que traz, ela apresenta dados cujos tratamento pode ensejar a discriminação de seu titular, devendo, por conseguinte, ser protegido de forma mais rígida"[53].

A sistemática de proteção de dados reage à malversação de tratamento de dados sensíveis precipuamente a partir de dois princípios, quais seja, a) princípio da não discriminação e b) princípio da finalidade. Em síntese quanto o primeiro, verifica-se que a não descriminação é objetivo basilar do Estado Brasileiro[54]. Nesse sentido, "a não discriminação é um princípio

---

50 Para além da LGPD, observa-se também o previsto na Lei nº 12.414/2011, em seu art. 3º, §3º, II, a qual proíbe, para os fins de concessão de crédito, a anotação de informações sensíveis, essas compreendidas como "pertinentes à origem social e étnica, à saúde, à informação genética, à orientação sexual e às convicções políticas, religiosas e filosóficas" BRASIL. Lei n. 12.414, de 9 de Junho de 2011. Disciplina a formação e consulta a bancos de dados com informações de adimplemento, de pessoas naturais ou de pessoas jurídicas, para formação de histórico de crédito. **Diário Oficial [da] República Federativa do Brasil**. Brasília, DF, 9 jun.2011. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2011/Lei/L12414.htm.

51 BIONI, Bruno Ricardo. **Proteção de dados pessoais: a função e os limites do consentimento.** Rio de Janeiro: Forense, 2019. p. 86.

52 Não apenas a LGPD prevê o caráter sensível de dados ou informações na legislação brasileira, motivo pelo qual a Lei de Cadastro Positivo – Lei 12.414/2011, ao proibir as anotações de informações sensíveis para fins de concessão de crédito, considera informações sensíveis como "(...) aquelas pertinentes à origem social e étnica, à saúde, à informação genética, à orientação sexual e às convicções políticas, religiosas e filosóficas" (Art. 3º, §3º, II).

53 Tepedino, Gustavo; Teffé, Chiara Spadaccini. Consentimento e proteção de dados pessoais na LGPD.

54 BRASIL. Constituição da República Federativa do Brasil. Art. 3º, inciso IV. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicaocompilado.htm

que há tempos já tinha conquistado espaços nas legislações internacionais, com a identificação e o tratamento diferenciado da categoria dos dados sensíveis"[55], visto que estão relacionados a informações de caráter personalíssimo do indivíduo[56].

Ou ainda, conforme especificado por Caitlin Sampaio Mulholland, o

> princípio da não discriminação é dos mais relevantes, no que diz respeito ao tratamento de dados sensíveis. É esse o ponto fundamental quando diante do uso de dados sensíveis potencialmente lesivo, em decorrência de sua capacidade discriminatória, seja por entes privados – i.e. fornecedoras de produtos e serviços – seja por entes públicos. [57]

Quanto a finalidade no tratamento de dados pessoais (art. 6º, I), esse diz respeito à "realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades"[58]. Isso é, tal princípio requer a explicitação dos fins a que se destinam os dados e informações coletados, especificando, com clareza, os objetivos pretendidos pelo tratamento realizado e vedando qualquer outra hipótese de tratamento que o titular não tenha conhecimento. Nesse sentido, assim como observado por Doneda:

> Este princípio possui grande relevância prática: com base nele, fundamenta-se a restrição da transferência de dados pessoais a terceiros, além do que pode-se, a partir dele, estruturar-se um critério para valorar a razoabilidade da utilização de determinados dados para uma certa finalidade (fora da qual haveria abusividade). [59]

Compreendida a correlação entre a lei brasileira e as normas europeias, ambas as quais tecem considerações acerca dos dados sensíveis e biométricos, observa-se o interesse comum dos sistemas de proteção de dados pessoais em acautelar violações a valores fundamentais, tais

---

55 Oliveira, Marco Aurélio Bellize; Lopes, Isabela Maria Pereira. **Os princípios norteadores da proteção de dados pessoais no Brasil e sua otimização pela Lei 13.709/2019**, p. 79. In Tepedino, Gustavo; Frazão, Ana; Oliva, Milena Donato (Coord.). **Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito brasileiro** – 1ª ed. São Paulo: Thomson Reuters, 2019.

56 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. Disponível em https://sisbib.emnuvens.com.br/direitosegarantias/article/view/1603.

57 *Idem.*

58 BRASIL. Lei n. 13.709, de 14 de agosto de 2018. Dispõe sobre a proteção de dados pessoais e altera a Lei n. 12.965, de 23 de abril de 2014 (Marco Civil da Internet). **Diário Oficial [da] República Federativa do Brasil.** Brasília, DF, 14 ago.2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm

59 DONEDA, Danilo. **Da privacidade à proteção de dados pessoais: elementos da formação da Lei geral de proteção de dados** - 2ª ed. São Paulo: Thomson Reuters Brasil, 2019, p. 182.

como a não discriminação e o desvirtuamento da finalidade dos dados coletados[60]. Portanto, o temor na malversação na utilização de dados biométricos justifica o rigoroso regime de tutela pelo sistema de proteção de dados pessoais.

4.2. Os riscos da imprecisão tecnológica no reconhecimento facial

Para além dos riscos próprios no tratamento de dados pessoais sensíveis, preocupações outras advêm quando do emprego de sistemas autônomos de reconhecimento de faces em locais públicos. Conforme anteriormente exposto, inserida essa tecnologia em plataformas algorítmicos e embasada por IA, são temíveis práticas discriminatórias que vulneram a privacidade e a liberdade individuais pela vigilância constante a partir de tecnologias pouco confiáveis[61].

Nessa linha, é de se notar que locais como São Francisco e Oakland se opuseram à instalação de câmeras de reconhecimento facial em locais públicos, sob a justificativa de que "a propensão da tecnologia de reconhecimento facial de prejudicar direitos e liberdades civis supera os benefícios pretendidos"[62]. Isso é, com mais dúvidas que certezas, preferiu-se pela parcimônia na instalação de sistemas de reconhecimento de faces ao redor das cidades, bem como foram priorizados debates acerca dos efeitos indesejáveis dessa tecnologia.

De fato, pelo estado da arte dos sistemas autônomos de reconhecimento facial, verifica-se que o seu emprego requer paciência e maior acuidade da tecnologia o quanto for possível. Vide o ocorrido no Reino Unido, onde as autoridades de segurança foram criticadas pela utilização de sistemas de reconhecimento de faces cujo sucesso na identificação cingiu a 92% do indivíduos[63].

A experiência brasileira é ainda mais preocupante, a exemplo de determinado episódio ocorrido no Rio de Janeiro, ocasião na qual "uma mulher foi detida por engano em Copacabana,

---

60 *Idem.*

61 Hurel, Louise Marie. Reconhecimento facial – regular, banir ou punir? Revista Insight Inteligência, Jan/Fev/Mar - edição 84. Disponível em: https://insightinteligencia.com.br/reconhecimento-facial-regular-banir-ou-punir-2/. Acesso em 15.11.2020.

62 Disponível em https://olhardigital.com.br/noticia/san-francisco-pode-ser-a-primeira-cidade-dos-eua-a-banir-o-reconhecimento-facial/85767. Acesso em 17.10.2020.

63 Hurel, Louise Marie. Reconhecimento facial – regular, banir ou punir? Revista Insight Inteligência, Jan/Fev/Mar - edição 84. Disponível em: https://insightinteligencia.com.br/reconhecimento-facial-regular-banir-ou-punir-2/. Acesso em 15.11.2020.

após ter sido confundida pela sistema de reconhecimento facial da Polícia Militar". Para tanto, foi noticiado que:

> "Os policiais acreditavam estar prendendo uma foragida da Justiça, acusada pelos crimes de homicídio e ocultação de cadáver. Um detalhe importante: a verdadeira procurada está presa desde 2015, informação que a Polícia Militar, responsável pela operação do sistema, simplesmente desconhecia. Em nota oficial sobre o ocorrido, a Polícia Militar explicou que as câmeras trabalham com uma estatística de reconhecimento (70% de possibilidade de ser a pessoa procurada) e que 'pelo princípio da presunção da inocência e como em qualquer ação policial, reforçamos o compromisso com o tal respeito às garantias constitucionais de todos os cidadãos'". [64]

Acaso confirmado esse número de 70% de acurácia da tecnologia na capital fluminense, o emprego da tecnologia naquela cidade é motivo de alerde, vez que se vale de precisão muito aquém para o seu emprego em contexto de massa. Em simples aritmética, tratando-se do segundo município mais populoso do país, com aproximadamente 6,72 milhões de habitantes[65], dispor a tecnologia de sucesso de 70% na identificação de indivíduos é expor sobremaneira a coletividade a reiterados erros de identificação.

A guisa de exemplo quanto a importância do debate estatístico, verifica-se sistemas outros de reconhecimento facial que trabalham com a margem 99,7% de acurácia na identificação e que, mesmo nesse patamar, expõem preocupações acaso empregados em contexto de massa[66]. Nesse sentido, conforme descrito por Alessandro Faria, ciente que a tecnologia se dirige à identificação de multidões, "mesmo com uma margem de erro de 0,01%, entre 12 milhões de habitantes, ainda estamos falando de 1200 pessoas com possíveis alertas falsos"[67]. Seguindo esse raciocínio, o que dizer de margem de erro em aproximadamente 30% em uma cidade com pouco mais de meia dúzia de milhões de habitantes?

Ao que parece, as autoridades públicas estão cientes de que a tecnologia de reconhecimento automatizada não está isenta de falhas na identificação, motivo pelo qual devem ser aplicados protocolos de revisão quando da identificação de indivíduos suspeitos.

---

[64] Disponível em https://www.jota.info/paywall?redirect_to=//www.jota.info/opiniao-e-analise/artigos/a-tecnologia-de-reconhecimento-facial-aplicada-a-seguranca-publica-23072019. Acesso em 25.10.2020.

[65] Dados do IBGE disponível em https://agenciadenoticias.ibge.gov.br/agencia-sala-de-imprensa/2013-agencia-de-noticias/releases/25278-ibge-divulga-as-estimativas-da-populacao-dos-municipios-para-2019#:~:text=O%20munic%C3%ADpio%20de%20S%C3%A3o%20Paulo,(2%2C9%20milh%C3%B5es). Acesso em 15.11.2020.

[66] Disponível em :https://epocanegocios.globo.com/colunas/IAgora/noticia/2019/10/alerta-tecnologias-de-reconhecimento-facial-estao-nos-ameacando.html. Acesso em 15.11.2020.

[67] Disponível em <https://exame.com/revista-exame/nao-ha-onde-se-esconder/>. Acesso em 21.10.2020.

Nesse ponto, a LGPD oferece luz a partir do art. 20, o qual confere o direito de revisão ao titular dos dados em casos de decisões automatizadas. *In verbis*:

> "Art. 20. O titular dos dados tem direito a solicitar a revisão de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem seus interesses, incluídas as decisões destinadas a definir o seu perfil pessoal, profissional, de consumo e de crédito ou os aspectos de sua personalidade".

No mesmo sentido, conforme expresso na recente Lei Distrital 6.712/2020, que disciplina a tecnologia de reconhecimento facial na segurança pública da capital federal, em seu art. 5º, consta o dever da autoridade pública de vigilância em revisar a identificação da pessoa, de modo a evitar qualquer acusação errônea ou equivocada pelo sistema automatizado:

> Art. 5º Toda e qualquer sinalização de identificação positiva gerada por sistema de reconhecimento facial deve ser revisada por um agente público antes de qualquer ação decorrentes.
> Parágrafo único: A identificação positiva gerada pelo sistema deve ser validada em campo próprio pelo agente público responsável

Portanto, conforme exposto por Louise Marie Hurel acerca da acurácia da tecnologia de reconhecimento em locais públicos, "sua capacidade de precisão e potenciais benefícios setoriais não se sobrepõem ao debate sobre direitos e proporcionalidade do uso", razão pela qual é necessária compreensão sobre os percentuais e riscos de falsas identificações antes mesmo do emprego da tecnologia[68].

4.3. Os riscos de vieses discriminatórios de algoritmos e inteligência artificial

Atrelado à automatização dos sistemas de reconhecimento, existem fundados receios de vieses discriminatórios embutidos em algoritmos, os quais podem "naturalizar preconceitos, a depender de quais sejam seus *inputs* e como [os sistemas] os processarão"[69].

A presente preocupação é objeto de intenso debate no âmbito da regulamentação de novas tecnologias, precipuamente aqueles embasada por algoritmos e IA. Não à toa, conforme exposto anteriormente, o desenvolvimento e emprego de sistemas automatizados de

---

[68] Hurel, Louise Marie. Reconhecimento facial – regular, banir ou punir? Revista Insight Inteligência, Jan/Fev/Mar - edição 84. Disponível em: https://insightinteligencia.com.br/reconhecimento-facial-regular-banir-ou-punir-2/. Acesso em 15.11.2020.

[69] CALABICH, Bruno Freire de Carvalho. **Discriminação algorítmica e transparência na Lei Geral de Proteção de Dados Pessoais.** Revista de Direito e as Novas Tecnologias, vol. 8/2020, jul-setemb/2020.

reconhecimento de faces foram interrompidos em algumas cidades dos EUA enquanto inexistirem balizas regulatórias sobre a tecnologia, razão pela qual se constatou riscos concretos decorrentes de resultados – *output* – discriminatórios em identificação de indivíduos.

Para tanto, conforme exposto por Joy Buolamwini, no âmbito de pesquisas desenvolvidas pelo *Massachusetts Institute of Technology* – MIT, por mais que algoritmos e sistemas automatizados não carreguem preconceitos em si, os dados dispersos e tratados por tais plataformas podem direcionar a resultados tidos como discriminatórios[70]. A exemplo disso, conforme demonstrado pela pesquisadora, constatou-se a dificuldade de sistemas autônomos em reconhecer faces de grupos minoritários, em especial mulheres negras[71].

Tal fato, a princípio, poderia indicar apenas "erros" ou "imprecisões" da tecnologia. Todavia, o problema não é tão simples como parece, vez que as consequências dessas "falhas" imbricam em práticas discriminatórias e que desembocam em experiências de exclusão de pessoas. Logo, o debate posto cinge na necessidade de diversificação dos dados tratados, bem como a concepção de máquinas que atendam a diversidade humana.

Dessa maneira, a propósito dos limites éticos e a *accountabily* de sistemas de inteligência artificial e *machine learning*, Andriei Gutierrez sintetiza que:

> Decisões passam a ser automatizadas a partir de critérios nem sempre conhecidos de modo a ter influência na vida cotidiana de cidadãos e consumidores. Nesse sentido, perguntas legítimas têm surgido:
> - Como garantir que os sistemas de decisões automatizadas não discriminem (e, assim, respeitem o direito constitucional à não discriminação) ou não firam o direito à privacidade?
> - Quais são os critérios éticos que estão embasando ou podem definir possíveis decisões de sistemas automatizados e que porventura podem ter como efeito a discriminação, ameaça à vida, à democracia ou ao cumprimento das leis vigentes?" [72]

---

[70] Acerca de preconceitos em algoritmos por Joy Boulamwini, https://www.ted.com/talks/joy_buolamwini_how_i_m_fighting_bias_in_algorithms?language=pt. Acesso em 20.11.2020.

[71] Nesse sentido: https://canaltech.com.br/inteligencia-artificial/algoritmos-de-reconhecimento-facial-falham-em-combinar-rostos-de-mulheres-negras-144657/>. Acesso em 20.11.2020

[72] GUTIERREZ, Andriei. **É possível confiar em um sistema de inteligência artificial? Práticas em torno da melhoria da sua confiança, segurança e evidências de accountability**, p. 86/87. In Frazão, Ana; Mulholland, Caitlin (coord.). **Inteligência artificial e direito: ética, regulação e responsabilidade**. São Paulo: Thomson Reuters, 2019.

Portanto, sendo reconhecidamente diversas as vantagens e empregos das novas tecnologias embasadas em algoritmos e inteligência artificial, primeiramente, requer-se a definição dos limites éticos e legais de tais tecnologias, de modo a evitar cisões sociais amplamente tensionadas. Logo, conforme exposto por Suzel Tunes:

> Boa parte dos algoritmos de inteligência artificial (IA) é desenvolvida para identificar padrões de modo a automatizar decisões e facilitar a vida das pessoas. Essas tecnologias pode reconhecer o estilo de música preferida de usuários, o gênero de filmes que lhe interessa ou os assuntos que mais busca no jornal. No entanto, por serem programados para captar modelos de comportamento, os algoritmos também podem replicar comportamentos indesejáveis, como o racismo, a misoginia e a homofobia. Absorvem, reproduzem e, como resultado, robustecem a discriminação e a intolerância vista na sociedade nas mais variadas formas", em Algoritmos Parciais. [73]

Ao encontro disso, é válido de destaque a atuação de importantes empresas tecnológicas, a exemplo da IBM[74] e Amazon[75], as quais, por ora, preferiram por suspender o desenvolvimento e comercialização de *softwares* de reconhecimento faciais e, por conseguinte, pressionar governos e comunidades a debaterem os riscos de seu emprego. O estopim de tal suspensão adveio após os protestos ocorridos nos EUA contra a morte de George Floyd e o debate de delicadas questões raciais naquele país, de modo que as empresas optaram por repensar vieses discriminatórios, mesmo que não intencionais, em tecnologias de vigilância[76].

5. O RECONHECIMENTO FACIAL AUTOMATIZADO PARA FINS EXCLUSIVO DE SEGURANÇA PÚBLICA

Para além das preocupações e fatos expostos, o direito surge como importante elemento de regulamentação dos riscos envolvidas no tratamento de faces por máquinas. Para tanto, de início, seria de se supor que a LGPD regulasse todas a conjectura de tratamento de dados pessoais, inclusive a problemática do reconhecimento facial para os fins coletivos de segurança pública. Contudo, a lei é expressa em excetuar a sua incidência nas hipóteses de tratamento de

---

[73] Tunes, Suzel. Revista Pesquisa FAPESP: São Paulo, edição 287, jan.2020. Disponível em: https://revistapesquisa.fapesp.br/algoritmos-parciais-2/. Acesso em 20.11.2020.

[74] 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 20.11.2020.

[75] Disponível em: https://www.uol.com.br/tilt/noticias/redacao/2020/06/11/apos-ibm-amazon-tambem-proibe-seu-reconhecimento-facial-para-vigilancia.htm. Acesso em 20.11.2020.

[76] Disponível em: https://neofeed.com.br/inovacao/o-reconhecimento-facial-e-racista-uma-questao-para-ibm-microsoft-e-amazon/. Acesso em 20.11.2020.

dados pessoais para fins exclusivos de segurança pública, defesa nacional, segurança do Estado ou atividade de investigação e repressão de infrações penais (art. 4, III, alíneas, da LGPD).

Por conseguinte, no § 1º, o texto legal imediatamente indica a regência de legislação específica, ainda a ser criada, para o tratamento de dados pessoais nos casos previstos no inciso III, a qual deverá se atender à proporcionalidade, respeito ao interesse público, bem como os procedimentos, os princípios gerais de proteção e os direitos do titular descritos da LGPD.

De modo geral, o emprego de reconhecimento facial está amparado na LGPD, em específico na parte do texto que disciplina o tratamento de dados sensíveis. De modo específico, a tecnologia é objeto de debates regulatórios e legislativos, como se percebe do Projeto de Lei 4.612/2019, em tramitação na Câmara dos Deputados, o qual "dispõe sobre o desenvolvimento, aplicação e uso de tecnologias de reconhecimento facial e emocional, bem como outras tecnologias digitais voltadas à identificação de indivíduos e à predição ou análise de comportamentos"[77].

Porém, problema maior advém quando do emprego de reconhecimento facial para fins de segurança pública, aliás âmbito o qual a tecnologia tem maior potencial de difusão, de maneira que a própria Lei Geral excepciona a sua incidência e, por conseguinte, especifica a necessidade de legislação própria ao tema.

A despeito disso, Caitlin Sampaio Mulholland sintetiza a esperança na lei porvir, a qual, agora voltada à esfera penal, toca sobremaneira as liberdades individuais, sendo aguardada em termos ainda mais rígidos que a LGPD. Para a autora:

> Considerando que o tratamento desses dados está relacionado em grande medida aos objetivos de proteção do próprios Estado e dos interesses públicos. Deve-se visar a um tratamento limitado desses dados, para evitar o seu eventual uso para propósito que não atendam aos fundamentos republicanos do Estado Democrático de Direito"[78].

---

[77] BRASIL. Câmara dos Deputados. **Projeto de Lei nº 4.612/2019**. Dispõe sobre o desenvolvimento e isso de tecnologias de reconhecimento facial e emocional, bem como outras tecnologias digitais voltadas à identificação de indivíduos e à predição ou análise de comportamentos. Disponível em <https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2216455>. Acesso em 20.11.2020.

[78] 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. Disponível em https://sisbib.emnuvens.com.br/direitosegarantias/article/view/1603.

5.1. O Anteprojeto de Lei de Proteção de Dados para Segurança Pública e Persecução Penal – LGPD Penal e o reconhecimento facial

Por todo o exposto, verifica-se a existência de considerável lacuna legal desde a sanção da LGPD, ainda em 2018. Por mais que o texto tenha aguardado longo período para viger, transcorridos pouco mais de dois anos e sucessivas tentativas de ampliação da *vacatio legis*, fato é que hoje a lei geral goza de plena vigência, demandando a edição de lei específica quanto o tratamento de dados pessoais destinados à segurança pública.

Atento a isso, o Congresso Nacional mobilizou uma comissão de juristas com foco na elaboração do Anteprojeto de Lei de Proteção de Dados Pessoais para Segurança Pública e Persecução Penal – LGPD Penal[79]. Conforme se percebe de seu esboço, a minuta, em alguns momentos, é consoante à Lei nº 13.709/2019, sendo que em outros se destaca por ser ainda mais rígida e específica aos fins que se destina.

Nesse sentido, o anteprojeto inova ao prever, dentre seus fundamentos preliminares, a presunção de inocência (art. 2º, V) e a garantia do devido processo legal, ampla defesa, do contraditório, da motivação e da reserva legal (art. 2º, VII). Ademais, posteriormente em suas considerações, apresentou definições próprias e atinentes ao seu conteúdo, a exemplo de dados sigilosos (art. 5º, III), análise de impacto regulatório (art. 5º, XIX), atividade de segurança pública (art. 5º, XXI), atividade de persecução penal (art. 5º, XXII), tecnologia de monitoramento (art. 5º, XXIII) e registros criminais (art. 5º, XXIV).

Ainda, impende destacar a nova sistemática esboçada pelo anteprojeto, o qual prevê o interesse público e a execução de políticas públicas como requisitos para tratamento de dados pessoais (art. 9º, I, II e III), todos calcados na legalidade. Por sua vez, a hipótese de tratamento de dados sensíveis e sigilosos é tida ainda mais rígida, momento em que é exigida atenção à legalidade estrita face à delicadeza dos dados envolvidos. Nesse aspecto estão contidas as tecnologias de monitoramento facial, tratando-se os dados biométricos como espécie dos dados sensíveis, conforme já exposto.

---

[79] Disponível em: https://www.camara.leg.br/noticias/618483-maia-cria-comissao-de-juristas-para-propor-lei-sobre-uso-de-dados-pessoais-em-investigacoes/. Acesso em 21.11.2020.

Logo, com o advento da LGPD Penal, acaso mantido o presente tópico pelas Casas Legislativas, tal requisição exigirá de todas as autoridades de tratamento a edição de lei própria que vise regulamentar os sistemas de reconhecimento facial.

CONSIDERAÇÕES FINAIS

Portanto, o presente trabalho explanou o emprego, desenvolvimento e risco da tecnologia de reconhecimento facial como ferramenta auxiliadora na segurança pública, bem como os riscos envoltos em tal atividade pelo Estado. Primeiramente, fixou-se o dever constitucional do Poder Público em prestar segurança à toda coletividade. Atinente a isso, exsurge determinado estado de vigilância constante, o qual se vale das novas tecnologias para alcançar seu compromisso público.

Em seguida, para dar concretude ao trabalho, foram apresentadas alguns locais que utilizam sistemas automatizados de reconhecimento de faces em seus cotidianos, a exemplo do Distrito Federal, Rio de Janeiro, Salvador, Campinas e Teresina. Nessas áreas, a tecnologia foi empregada em ambientes com grande circulação de pessoas, tendo por finalidade a identificação de indivíduos, suspeitos ou não.

Por outro lado, verifica-se temor em outras localidades pelo mundo quanto à utilização da tecnologia, a exemplo de São Francisco e Oakland, Nice e Reino Unido, cada qual por suas razões. Exemplo mais contundente se refere às cidades São Francisco e Oakland, as quais decidiram, por ora, suspender a utilização da tecnologia pelas autoridades públicas de segurança, tendo em vista algumas inconsistências nos algoritmos e resultados discriminatórios.

Em seguida, o trabalho focou em descrever os sistemas de reconhecimento de faces, expondo os dados biométricos, categorizados como dados pessoais sensíveis, como combustível ao desenvolvimento desse tipo de tecnologia. Para tanto, além de elementos computacionais como algoritmos, inteligência artificial e *machine learning*, os sistemas de reconhecimento de faces prezam pela coleta, tratamento e armazenamento de dados pessoais, o que convida para o debate a sistemática jurídico-constitucional da privacidade e não discriminação dos indivíduos.

Mais ainda, da atividade de tratamento de dados pessoais exsurgem perigos, os quais podem ser resumidos nos riscos próprios do tratamento de dados sensíveis, os riscos da imprecisão tecnológica e riscos de vieses discriminatórios de algoritmos.

Por último, a correlação entre a temática de proteção de dados e segurança pública serão matérias afins nos debates vindouros, principalmente com a proposta do anteprojeto da LGPD Penal, que visa preencher lacuna criada pela Lei nº 13.709/2018 e, por conseguinte, o uso de reconhecimento facial na segurança pública.

Referências

BAUMAN, Zygmunt; LYON, David. Vigilância líquida. Rio de Janeiro: Zahar, 2014. E-book. (1 recurso online). ISBN 9788537811771. Disponível em: https://integrada.minhabiblioteca.com.br/books/9788537811771.

BELANDA, Douglas. Biometria como mecanismo de formação e prova contratual: um olhar para as transações eletrônicas bancárias na sociedade da informação. Revista dos Tribunais: São Paulo, vol. 1016/2020, jun.2020.

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

BRASIL. Câmara dos Deputados. Projeto de Lei nº 4.612/2019. Dispõe sobre o desenvolvimento e isso de tecnologias de reconhecimento facial e emocional, bem como outras tecnologias digitais voltadas à identificação de indivíduos e à predição ou análise de comportamentos. Disponível em https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2216455

BRASIL. Constituição da República Federativa do Brasil. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicaocompilado.htm Brasil

BRASIL. Lei n. 12.414, de 9 de Junho de 2011. Disciplina a formação e consulta a bancos de dados com informações de adimplemento, de pessoas naturais ou de pessoas jurídicas, para formação de histórico de crédito. Diário Oficial [da] República Federativa do Brasil. Brasília, DF, 9 jun.2011. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2011/Lei/L12414.htm

BRASIL. Lei n. 13.709, de 14 de agosto de 2018. Dispõe sobre a proteção de dados pessoais e altera a Lei n. 12.965, de 23 de abril de 2014 (Marco Civil da Internet). Diário Oficial [da] República Federativa do Brasil. Brasília, DF, 14 ago. 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm

BRASIL, Supremo Tribunal Federal. Ação Direta de Inconstitucionalidade n. 6.387/DF MC-Ref. Autor: Conselho Federal da Ordem dos Advogados do Brasil. Relator(a): Min. Rosa Weber. Brasília. Julgado em 07/05/2020, divulgado 11.11.2020.

CALABICH, Bruno Freire de Carvalho. Discriminação algorítmica e transparência na Lei Geral de Proteção de Dados Pessoais. Revista de Direito e as Novas Tecnologias, vol. 8/2020, jul-setemb/2020.

DONEDA, Danilo. Da privacidade à proteção de dados: fundamentos da Lei geral de proteção de dados – 2ª ed. São Paulo: Thomson Reuters Brasil, 2019.

EUROPA. General Data Protection Regulation (GDPR). Regulamento Geral sobre a Proteção de Dados. Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016. Disponível versao portugues em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016R0679&from=EN

GUTIERREZ, Andriei. É possível confiar em um sistema de inteligência artificial? Práticas em torno da melhoria da sua confiança, segurança e evidências de accountability. In Frazão, Ana; Mulholland, Caitlin (coord.). Inteligência artificial e direito: ética, regulação e responsabilidade. São Paulo: Thomson Reuters, 2019.

HUREL, Louise Marie. Reconhecimento facial – regular, banir ou punir? Revista Insight Inteligência, Jan/Fev/Mar - edição 84. Disponível em: https://insightinteligencia.com.br/reconhecimento-facial-regular-banir-ou-punir-2/.

KONDER, Carlos Nelson. O tratamento de dados pessoais sensíveis à luz da lei 13.709/2018. In Tepedino, Gustavo; Frazão, Ana; Oliva, Milena Donato (Coord.). Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito brasileiro – 1ª ed. São Paulo: Thomson Reuters, 2019.

MENDES, Laura Schertel. Privacidade, proteção de dados e defesa do consumidor: linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014.

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. Disponível em https://sisbib.emnuvens.com.br/direitosegarantias/article/view/1603.

NEGRI, Sergio Marcos Carvalho de Ávila; DE OLIVEIRA, Samuel Rodrigues; COSTA, Ramon Silva. O uso de tecnologias de reconhecimento facial baseadas em inteligência artificial e o direito à proteção de dados. Direito Público, [S.l.], v. 17, n. 93, jul. 2020. ISSN 2236-1766. Disponível em: <https://www.portaldeperiodicos.idp.edu.br/direitopublico/article/view/3740>. Acesso em: 10.11.2020.

OLIVEIRA, Marco Aurélio Bellize; LOPES, Isabela Maria Pereira. Os princípios norteadores da proteção de dados pessoais no Brasil e sua otimização pela Lei 13.709/2019. In Tepedino, Gustavo; Frazão, Ana; Oliva, Milena Donato (Coord.). Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito brasileiro – 1ª ed. São Paulo: Thomson Reuters, 2019.

REIS, Paulo Victor Alfeo. Algoritmo e o direito. São Paulo: Almedina, 2020.

SOUZA, Robson Sávio Reis. Quem comanda a segurança pública no Brasil? Atores, crenças e coalizões que dominam a política nacional de segurança pública. Editora Letramento. Belo Horizonte, 2015.

TEPEDINO, Gustavo; Teffé, CHIARA Spadaccini. Consentimento e proteção de dados pessoais na LGPD. In Tepedino, Gustavo; Frazão, Ana; Oliva, Milena Donato (Coord.). Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito brasileiro – 1ª ed. São Paulo: Thomson Reuters, 2019.

TUNES, Suzel. Revista Pesquisa FAPESP: São Paulo, edição 287, jan.2020. Disponível em: https://revistapesquisa.fapesp.br/algoritmos-parciais-2/. Acesso em 20.11.2020.