UNIVERSIDADE ESTADUAL PAULISTA "JÚLIO DE MESQUITA FILHO"
FACULDADE DE CIÊNCIAS HUMANAS E SOCIAIS

CÍNTHIA BACCARIN

LIMITAÇÕES AOS SISTEMAS DE RECONHECIMENTO FACIAL NO SETOR PRIVADO:

boas práticas em proteção de dados biométricos faciais

FRANCA
2023

CÍNTHIA BACCARIN

LIMITAÇÕES AOS SISTEMAS DE RECONHECIMENTO FACIAL NO SETOR PRIVADO:

boas práticas em proteção de dados biométricos faciais

Dissertação apresentada ao Programa de Pós-graduação *stricto sensu* em Direito da Universidade Estadual Paulista "Júlio de Mesquita Filho", Faculdade de Ciências Humanas e Sociais, campus de Franca-SP, como parte das exigências para obtenção do título de Mestre em Direito. Área de concentração: Cidadania Civil e Política e Sistemas Normativos.

Orientação: Profa. Dra. Luciana Lopes Canavez.

FRANCA

2023

B116l

Baccarin, Cínthia
Limitações aos sistemas de reconhecimento facial no setor privado : boas práticas em proteção de dados biométricos faciais / Cínthia Baccarin. -- Franca, 2023
154 p.

Dissertação (mestrado) - Universidade Estadual Paulista (Unesp), Faculdade de Ciências Humanas e Sociais, Franca
Orientadora: Luciana Lopes Canavez

1. reconhecimento facial. 2. privacidade. 3. proteção de dados. 4. tecnologia. 5. setor privado. I. Título.

Sistema de geração automática de fichas catalográficas da Unesp. Biblioteca da Faculdade de Ciências Humanas e Sociais, Franca. Dados fornecidos pelo autor(a).

Essa ficha não pode ser modificada.

IMPACTO POTENCIAL DESTA PESQUISA

A importância desta pesquisa está atrelada à promoção do equilíbrio entre a inovação tecnológica e os direitos e liberdades fundamentais, como a privacidade, a proteção de dados pessoais, a não discriminação e a liberdade de locomoção, à luz dos Objetivos de Desenvolvimento Sustentável nº 9 e nº 10 elaborados pela Agenda 2030 da Organização das Nações Unidas. A pesquisa tem como pressuposto os riscos para os direitos e liberdades fundamentais causados pelo uso indiscriminado de tecnologias de reconhecimento facial, que envolve o tratamento de massiva quantidade de dados, dentre os quais dados pessoais sensíveis de biometria da face. Nesse sentido, propõe-se a ampliação de valores em privacidade e proteção de dados levando em consideração as necessidades de todas as partes interessadas e da sociedade em geral, ajudando a equilibrar os interesses das pessoas em sua individualidade e das organizações. A adoção de medidas lícitas e transparentes no tratamento de dados pessoais, não protege somente o indivíduo relacionado aos dados, mas também seu grupo social, interesses coletivos e as gerações futuras. Por fim, a pesquisa busca promover o setor empresarial em reputação, competitividade e posicionamento no mercado nacional e internacional, o que se mostra benéfico para dinamizar e ampliar inovação e renda.

POTENTIAL IMPACT OF THIS RESEARCH

The importance of this research is linked to promoting a balance between technological innovation and fundamental rights and freedoms, such as privacy, personal data protection, non-discrimination, and freedom of movement, in light of Sustainable Development Goals No. 9 and No. 10 developed by the United Nations Agenda 2030. The research is based on the risks to fundamental rights and freedoms caused by the indiscriminate use of facial recognition technologies, which involves processing massive amounts of data, including sensitive biometric facial data. Therefore, it proposes the expansion of values in privacy and data protection, taking into account the needs of all stakeholders and society as a whole, helping to balance the interests of individuals and organizations. The adoption of lawful and transparent measures in the processing of personal data not only protects the individual related to the data, but also their social group, collective interests, and future generations. Finally, the research aims to promote the business sector in reputation, competitiveness, and positioning in the national and international market, which proves to be beneficial for dynamizing and expanding innovation and income.

CÍNTHIA BACCARIN

LIMITAÇÕES AOS SISTEMAS DE RECONHECIMENTO FACIAL NO SETOR PRIVADO:
boas práticas em proteção de dados biométricos faciais

Dissertação apresentada ao Programa de Pós-graduação *stricto sensu* em Direito da Universidade Estadual Paulista "Júlio de Mesquita Filho", Faculdade de Ciências Humanas e Sociais, campus de Franca-SP, como parte das exigências para obtenção do título de Mestre em Direito. Área de concentração: Cidadania Civil e Política e Sistemas Normativos.

BANCA EXAMINADORA

Presidente: _____

Prof. Dra. Luciana Lopes Canavez

1º Examinador/a: _____

Prof. Dr. Victor Hugo de Almeida

2º Examinador/a: _____

Prof. Dr. Eduardo Tomasevicius Filho

Franca, 31 de maio de 2023.

Dedico essa dissertação de mestrado à minha mãe, Carmen L. P., que instiga minhas maiores virtudes.

AGRADECIMENTOS

Agradeço a Deus, que me acompanha na jornada da vida e é minha fonte de energia.

Agradeço à minha família, sem os quais eu não conseguiria estar concluindo mais essa etapa da minha carreira. Em especial à minha mãe, Carmen, luz na minha vida, e ao meu irmão, Neto, fonte de apoio e alegria.

Agradeço ao meu amor, Cleber, por ter me acompanhado nessa fase turbulenta. Obrigada por nossos momentos juntos e por todo amor, companheirismo e cuidado. Amo muito você.

Agradeço à Bruna, que tem me ajudado tanto a enfrentar minhas próprias sombras.

Agradeço à minha orientadora, Profa. Luciana Lopes Canavez, que me abriu as portas e depositou sua confiança em mim. Sou grata por ter me incentivado até o fim, mesmo enfrentando as adversidades de uma pandemia.

Agradeço à UNESP Franca pelas lembranças dos quase dez anos de casa, que vão ficar na saudosa memória. Estendo os meus agradecimentos aos professores e colaboradores.

Agradeço ao meu querido Team Privacy do BFBM, André, Fer, Malu, Ber, Gabs, Lari e Bruno, amigos que me ajudam a evoluir diariamente. Obrigada por estarem na minha vida e por terem me ajudado a conciliar o trabalho com essa dissertação.

Agradeço às minhas amigas por ouvirem tantos desabafos e por serem compreensíveis, já me desculpando pelas ausências.

Gratidão aos anos de mestrado que me enriqueceram como profissional e a todos que fizeram parte na minha trajetória por esses anos.

BACCARIN, Cínthia. **Limitações aos sistemas de reconhecimento facial no setor privado:** boas práticas em proteção de dados biométricos faciais. 2023. 154 f. Dissertação (Mestrado em Direito) - Faculdade de Ciências Humanas e Sociais, Universidade Estadual Paulista "Júlio de Mesquita Filho", Franca, 2023.

RESUMO

O uso descontrolado de dados pessoais biométricos da face por sistemas de reconhecimento facial causa vulnerabilidades aos indivíduos, como consequências prejudiciais para a tutela dos direitos e liberdade fundamentais. Contudo, o ordenamento jurídico brasileiro, atualmente, dispõe de normas que regulam até certa medida as tecnologias de reconhecimento facial. Assim, o interesse da pesquisa permeia a consideração de disposições legais sobre proteção de dados, bem como a investigação de Projetos de Lei que possam complementar essa regulamentação, além de legislações internacionais da UE e dos EUA que possam ser modelos de orientação e inspiração. Nesse sentido, buscou-se analisar as regulamentações jurídicas em matéria de reconhecimento facial, dados biométricos e inteligência artificial a fim de se compreender quais são as regras e boas práticas a serem seguidas para que a tecnologia possa ser implementada pelo setor privado, protegendo dados biométricos faciais e os direitos e liberdades fundamentais. No tocante à metodologia, trata-se de uma investigação de natureza básica, fundamentalmente qualitativa e de objetivo exploratório. Como método de procedimento, optou-se pela coleta de dados majoritariamente bibliográfica e pela consulta a textos normativos nacionais e internacionais. Para análise dos dados, adotou-se o método de abordagem dedutivo, partindo de aspectos mais gerais para chegar a interpretações mais específicas. Concluiu-se pela ampla movimentação de iniciativas para a regulamentação específica em matéria de reconhecimento facial, dados biométricos e inteligência artificial; ademais, foram encontradas regulamentações específicas para o reconhecimento facial em cidades dos EUA, mas que são destinadas a restringir o uso da tecnologia pelo setor público; por fim, a pesquisa constatou que a adequação de uma empresa às melhores práticas em proteção de dados biométricos não é uma tarefa trivial, já que demanda atenção às diferentes possibilidades de técnicas e contextos de emprego da tecnologia e às medidas impostas para o tratamento de dados sensíveis, como adequação a princípios, definição de base legal, garantia aos direitos dos titulares de dados e condução e atualização constante de relatórios, documentos e políticas.

Palavras-chave: reconhecimento facial. privacidade. proteção de dados. tecnologia. setor privado.

BACCARIN, Cínthia. **Limitations to facial recognition systems in the private sector:** best practices in facial biometric data protection. 2023. 154 p. Dissertation (Master's in Law) - Faculty of Humanities and Social Sciences, São Paulo State University "Júlio de Mesquita Filho", Franca, 2023.

ABSTRACT

Uncontrolled use of facial biometric personal data by facial recognition systems poses vulnerabilities to individuals, leading to harmful consequences for the protection of fundamental rights and freedoms. However, Brazilian legislation currently provides regulations that control facial recognition technologies to a certain extent. Thus, this research aims to consider legal provisions on data protection, investigate Bills that could complement this regulation, and examine EU and US international regulations that could serve as guidance and inspiration. In this regard, regulations on facial recognition, biometric data, and artificial intelligence were analyzed to understand the rules and best practices that must be followed to implement the technology in the private sector while protecting facial biometric data and fundamental rights and freedoms. The methodology used in this research is primarily qualitative and exploratory, with a deductive approach to data analysis. Data collection was conducted mainly through bibliographical research and consultation of national and international normative texts. The research found a wide range of initiatives aimed at regulating facial recognition, biometric data, and artificial intelligence, as well as specific regulations on facial recognition in US cities that restrict the technology's use by the public sector. Furthermore, the study concluded that companies' compliance with best practices in protecting biometric data is not an easy task and requires attention to different techniques and contexts of technology deployment, and measures imposed for sensitive data treatment, such as adherence to principles, definition of legal bases, guaranteeing data subject rights, and conducting and constantly updating reports, documents and policies.

Keywords: facial recognition. privacy. data protection. technology. private sector.

LISTA DE FIGURAS

LISTA DE QUADROS

LISTA DE SIGLAS

AIPD	Avaliação de Impacto sobre a Proteção de Dados
ANPD	Autoridade Nacional de Proteção de Dados
BIPA	*Biometric Information Privacy Act*
BUS&COM	*Texas Business and Commerce Code*
CCPA	*California Consumer Privacy Act*
CEO	*Chief Executive Officer*
CFR	*Charter of Fundamental Rights*
CFTV	Circuito Fechado de Televisão
CNIL	*Commission Nationale de l'Informatique et des Libertés*
CNN	*Convolutional Neural Network*
COIT	Comitê de Tecnologia da Informação
COPPA	Children's Online Privacy Protection Rule
CPA	*California Consumer Privacy Act*
DPIA	*Data Protection Impact Assessment*
DPO	*Data Protection Officer*
DUDH	Declaração Universal dos Direitos Humanos
EDPB	*European Data Protection Board*
EDPS	*European Data Protection Supervisor*
ERPS	Estudos do Parlamento Europeu
ESHB	*Engrossed Substitute House Bill No 1493*
ESSB	*Engrossed Substitute Senate Bill No 6280*
EUA	Estados Unidos
FER	*Face Emotion Recognition*
FERET	*Face Recognition Technology*
FTC	*Federal Trade Commission*
GDPR	*General Data Protection Regulation*
GEPAN IA	Grupo de Peritos de Alto Nível em Inteligência Artificial
HB	*House Bill*
IA	Inteligência artificial
IAPP	*International Association of Privacy Professionals*
ICO	*Information Commissioner's Office*
IDEC	Instituto Brasileiro de Defesa do Consumidor

LED	Diretiva de *Law Enforcement*
LFW	*Labeled Faces in the Wild*
LGPD	Lei Geral de Proteção de Dados
NIST	Instituto Nacional de Padrões e Tecnologia
ONU	Organização das Nações Unidas
RCW	*Revised Code of Washington*
RGPD	Regulamento Geral de Proteção de Dados
RIPD	Relatório de Impacto a Proteção de Dados
TICs	Tecnologia da informação e comunicação
UE	União Europeia

SUMÁRIO

INTRODUÇÃO

O uso das tecnologias de reconhecimento facial vem crescendo no mercado em diversas áreas das atividades humanas. Essa tecnologia pode ser entendida como uma aplicação de inteligência artificial que se utiliza da técnica de coleta de biometria baseada em traços do rosto humano e pode ser utilizada para fins de autenticação, identificação ou classificação de pessoas, conforme será melhor explorado no primeiro tópico.

Além do tratamento de dados biométricos faciais, as programações de inteligência artificial dependem de gigantesca proporção de dados para que atendam aos comandos de processamento, discernimento, aprendizagem e tomada de decisão, que envolvem diferentes técnicas e aplicações na sua engenharia. Em vista disso, o crescimento dessa tecnologia impõe desafios para o Direito, de modo que já demanda atenção para o descompasso existente entre a técnica e a regulação jurídica, cujo propósito é a garantia da privacidade, da proteção de dados pessoais e outros direitos e liberdades fundamentais.

A proteção conferida aos dados pessoais por normas jurídicas gerou a necessidade de se estabelecer de forma sistemática e objetiva diretrizes que devem reger a implementação desses sistemas de reconhecimento facial, para que os riscos de violação à privacidade e a proteção de dados, decorrentes do uso indiscriminado dessa tecnologia, sejam evitados ou minimizados. Contudo, essa tecnologia suscita violações a outros direitos e liberdades fundamentais que as disposições legais de proteção de dados pessoais não são suficientes para regular, causando incertezas ao uso de aplicações de reconhecimento facial pelo setor privado.

O avanço na implementação da tecnologia e os contextos de irregularidades têm levado a movimentos por parte de organizações civis pela regulação do reconhecimento facial e, em alguns casos, pelo seu banimento parcial ou completo. As preocupações não são apenas por parte da sociedade civil organizada, mas também de grandes empresas do setor de tecnologia, que não negam os potenciais problemas advindos do emprego do reconhecimento facial, mas, ao mesmo tempo, não endossam o discurso de banimento, acreditando nos potenciais de uma tecnologia regulada.

Portanto, questiona-se quais seriam as regras e boas práticas a serem seguidas para que o reconhecimento facial possa ser implementado pelo setor privado de forma a proteger os dados biométricos faciais e a respeitar os direitos e liberdades fundamentais.

Nesse sentido, a pesquisa será debruçada na consideração de disposições legais que possam limitar a utilização dos sistemas de reconhecimento facial, como as leis de proteção de dados pessoais, que regulam os dados biométricos. Além disso, também serão empenhados

esforços para a investigação de Projetos de Lei que possam complementar essa regulamentação e para conferir as legislações internacionais dos EUA e em nível da UE, que possam ser modelos de orientação e inspiração. Assim, serão analisadas regulamentações jurídicas em matéria de reconhecimento facial, dados biométricos e inteligência artificial com o objetivo geral de compreender quais são as regras e boas práticas a serem seguidas para que a tecnologia possa ser implementada pelo setor privado, protegendo dados biométricos faciais, a privacidade e outros os direitos e liberdades fundamentais.

O primeiro tópico trata brevemente sobre alguns aspectos característicos da sociedade que são importantes para a compreensão de fatores que possibilitaram o desenvolvimento da tecnologia de reconhecimento facial, bem como aborda sobre como os computadores passaram a ser capazes de detectar, analisar e reconhecer rostos. Adiante, faz uma introdução sobre a dimensão técnica de sistemas de reconhecimento facial e, então, dá um mergulho mais profundo para considerar as implicações dessa tecnologia em relação a dados pessoais, premissas essenciais para a condução e desenrolar de todo o trabalho. Por último e tão importante quanto os pontos anteriores, apresenta os riscos originados pelo uso indiscriminado de tecnologias de reconhecimento facial, que levarão, nos próximos tópicos, ao estudo de responsabilidades legais e boas práticas direcionadas à iniciativa privada para governança e desenvolvimento seguro dessas tecnologias, com o fim na proteção dos dados pessoais sensíveis biométricos da face.

O segundo tópico, por sua vez, é dividido em duas partes. A primeira parte considera as legislações da UE que possam conferir regulamentação jurídica às tecnologias de reconhecimento facial, enquanto a segunda parte destina-se ao mesmo objeto de investigação nas legislações dos EUA. No caso da UE, explora-se o GDPR, que regulamenta as decisões tomadas com base em decisões automatizadas e o tratamento de categorias especiais de dados. Além disso, explora-se os primeiros passos no sentido de regulamentação das inteligências artificiais na UE. Com relação aos EUA, investiga-se leis estaduais da Califórnia, Illinois, Washington e Texas, que possuem regulamentação para tratamento de dados biométricos, bem como legislações locais de São Francisco, Boston e Minnesota, que, por sua vez, possuem regulamentação para tecnologias de vigilância, vigilância facial e reconhecimento facial, respectivamente.

Por último, o terceiro tópico destina-se ao estudo da regulamentação jurídica das tecnologias de reconhecimento facial no Brasil. Assim, a pesquisa faz uma abordagem das disposições legais sobre proteção de dados biométricos da LGPD, bem como faz uma investigação de Projetos de Lei que possam complementar essa regulamentação. O último

subtópico enfrenta a questão principal e mostra as principais regras e boas práticas para a proteção dos dados biométricos faciais no contexto das tecnologias de reconhecimento facial.

O presente trabalho se trata de uma pesquisa de natureza básica, pois visou a produção de informações, conhecimentos e reflexões sobre a efetiva tutela do direito fundamental à proteção de dados pessoais diante das inovações tecnológicas.

A pesquisa também apresenta característica fundamentalmente qualitativa, realizada a partir de análises, percepções e entendimentos do objeto de estudo. Quanto aos objetivos, tratou-se de uma pesquisa exploratória e descritiva do contexto.

A coleta de dados foi realizada por meio do método de procedimento bibliográfico, utilizando materiais doutrinários, artigos científicos, dissertações e, majoritariamente, fontes imediatas jurídico-formais de pesquisa, como a legislação da União Europeia, dos Estados Unidos e do Brasil. Para se extrair conclusões, utilizou-se o método de abordagem dedutivo, partindo de aspectos mais gerais para chegar a interpretações mais específicas.

1. OS SISTEMAS DE RECONHECIMENTO FACIAL

A capacidade de reconhecer rostos é uma atividade natural do cérebro humano e trivial para as relações sociais, mas o exercício dessa função por instrumentos tecnológicos construídos pelo ser humano não era comum até pouco tempo. Os avanços tecnológicos que se iniciaram no século passado ocasionaram uma mudança paradigmática da sociedade centrada nas novas tecnologias de informação e comunicação[1], que foram moldando a experiência humana - e ao mesmo tempo moldadas pela busca incessante do homem pelo novo - até que fosse possível que sistemas de reconhecimento facial estivessem presentes na vida contemporânea pelo mundo todo.

Percebe-se que, ao longo das últimas décadas, houve o aperfeiçoamento da técnica dos *softwares*, a melhora da resolução das imagens capturadas por câmeras, bem como o crescimento exponencial da disponibilidade de dados e da capacidade de seu armazenamento. Esses fatores em conjunto foram responsáveis pela viabilidade e disseminação do uso de tecnologias avançadas como o reconhecimento facial. Se atualmente é possível que o celular seja desbloqueado apenas mostrando o rosto, que uma loja identifique as emoções dos seus clientes e que um indivíduo procurado pela polícia seja identificado por câmeras públicas, é inegável que sistemas de análise facial estejam presentes, tanto no setor público quanto no setor privado.

Tecnologias como essa estão cada vez mais moldando as nossas vidas e se tornando algo integrado de uma sociedade conectada, o que, consequentemente, talvez traga a percepção de que a inserção desses sistemas de reconhecimento facial seja inevitável. Esse estado de aparente inevitabilidade implica em algumas problemáticas que precisam ser expostas e posteriormente enfrentadas, ao menos aquelas que dizem respeito às preocupações do recorte deste trabalho, conforme será visto ao longo da dissertação.

Este tópico passará a tratar (i) brevemente sobre alguns aspectos característicos da sociedade que são importantes para a compreensão de fatores que possibilitaram o desenvolvimento da tecnologia de reconhecimento facial, bem como abordará (ii) um pouco sobre como os computadores passaram a ser capazes de detectar, analisar e reconhecer rostos. Adiante, a pesquisa fornecerá uma (iii) introdução sobre a dimensão técnica de sistemas de reconhecimento facial e, então, dará um mergulho mais profundo para considerar (iv) implicações dessa tecnologia em relação a dados pessoais, que serão premissas para se chegar

[1] CASTELLS, Manuel. **A sociedade em rede.** v. 1, 8. ed. São Paulo: Paz e Terra, 2005. n.p.

ao objetivo central do trabalho. Por último e tão importante quanto os pontos anteriores, serão apresentados (v) os riscos originados pelo uso indiscriminado de tecnologias de reconhecimento facial, que levarão, nos próximos tópicos, ao estudo de responsabilidades legais e boas práticas direcionadas à iniciativa privada para governança e desenvolvimento seguro dessas tecnologias, com o fim na proteção dos dados pessoais sensíveis biométricos da face.

1.1 PARADIGMA INFORMACIONAL DA SOCIEDADE CONTEMPORÂNEA

Com base no surgimento da *Internet* e de outras tecnologias que a precederam e a sucederam, Manuel Castells[2] entende que a humanidade se encontra em um intervalo da história da vida cuja característica é "a transformação de nossa "cultura material" pelos mecanismos de um novo paradigma tecnológico que se organiza em torno da tecnologia da informação"[3] e comunicação (TICs), que seriam, para ele, a microeletrônica, a computação (*softwares* e *hardwares*), as telecomunicações/radiodifusão, a optoeletrônica (fibra óptica e laser) e a engenharia genética, que foram responsáveis pelo grande marco inicial das mudanças experimentadas pela sociedade nas últimas décadas[4].

Nota-se que, com o passar dos anos, as tecnologias[5] utilizadas pela humanidade são gradualmente aprimoradas ou trocadas. Ao mesmo tempo, as inovações tecnológicas, muitas vezes, foram responsáveis por mudanças na sociedade em razão de determinarem questões de trabalho, poder, produção e distribuição do tempo e do espaço. Nesse sentido de interação entre tecnologia e sociedade, o cenário da vida humana vem sofrendo uma transformação acelerada desde o final do século XX até os dias atuais. O celular, o computador e a *Internet*, por exemplo,

---

[2] Sociólogo espanhol e pesquisador, busca contribuir para a compreensão do novo mundo que se apresenta para todos em suas esferas política, econômica, social e cultural. Apesar de ter nascido na Espanha, o autor se mudou para o Vale do Silício, na Califórnia, Estados Unidos, exatamente na época em que surgiam as novas tecnologias de informação e comunicação que proporcionam toda a mudança paradigmática na estrutura social, motivo de seu grande interesse de estudo. Fruto de seus estudos, o autor escreveu a trilogia "A Era da Informação", composta pelos livros "A Sociedade em Rede" (1996), "O Poder da Identidade" (1997) e "Fim do milênio" (1998), referência na discussão das transformações a partir do final do século XX (Wikipédia).

[3] CASTELLS, op. cit., p. 67.

[4] "O homem vem se relacionando com tecnologias cada vez mais sofisticadas nos últimos 20 mil anos de sua história. Mas foi a partir do século XVIII que diversas máquinas foram introduzidas no cotidiano das pessoas." MACHADO FILHO, Francisco. As tecnologias da informação e as novas estruturas sociais e econômicas. **Ciência Geográfica**, v. 16, n. 2, p. 155-167, 2012. Disponível em: http://hdl.handle.net/11449/134969. Acesso em: 14 jan. 2023. p. 156.

[5] Tecnologia, para Castells, é "o uso de conhecimentos científicos para especificar as vias de se fazerem as coisas de uma maneira reproduzível". CASTELLS, *op. cit.*, p. 67. Portanto, não são apenas os computadores modernos, tablets e celulares de última geração que são exemplos de tecnologia, mas qualquer instrumento, técnica, processo, método, que tenha sido dominado para se reproduzirem coisas. Como os tipos móveis de Gutenberg, por exemplo, que representam uma tecnologia, mas não tão inovadora quanto foi um dia, quando do desenvolvimento da imprensa.

são ferramentas tecnológicas marcantes desta sociedade contemporânea, responsáveis por novos comportamentos, novas formas de comunicação, dentre outras modificações.[6]

Alvin Toffler[7] expressou, em seu livro "A terceira onda", o embate que vem acontecendo entre uma organização social que durou por cerca de trezentos anos e a nova era que está mudando hábitos e conceitos há muito definidos[8]. Esse choque seria a passagem da Era Industrial para a Era Informacional.[9] As tecnologias de informação e comunicação utilizadas desde os séculos passados, como a fotografia, o cinema, o rádio e a televisão, foram aprimoradas, ao ponto do ser humano vivenciar, hoje, a revolucionária interação entre texto, som e imagem, simultaneamente, a qualquer tempo e lugar, permitida pela tecnologia em rede, a *Internet.*

A sociedade atual vive em um mundo progressivamente digitalizado e tecnológico, de modo que a maior parcela das atividades humanas acontece com base nas novas tecnologias de informação e comunicação. Isso porque os avanços tecnológicos, nas últimas décadas, possibilitaram o armazenamento, processamento e transmissão de grande quantidade de conjuntos de dados no universo digital. Em razão da penetrabilidade dessas tecnologias em todas as esferas da atividade humana, a sociedade tem cada vez mais aumentado o seu grau de complexidade[10].

---

[6] "É claro que a tecnologia não determina a sociedade. Nem a sociedade escreve o curso da transformação tecnológica, uma vez que muitos fatores, inclusive criatividade e iniciativa empreendedora, intervêm no processo de descoberta científica, inovação tecnológica e aplicações sociais, de forma que o resultado final depende de um complexo padrão interativo. Na verdade, o dilema do determinismo tecnológico é, provavelmente, um problema infundado, dado que a tecnologia é a sociedade, e a sociedade não pode ser entendida ou representada sem suas ferramentas tecnológicas." CASTELLS, op. cit., p. 43.

[7] Alvin Toffler (1928 - 2016) foi um escritor norte-americano, com doutorado em Letras, Leis e Ciência, conhecido pelos seus escritos sobre a revolução digital, a revolução das comunicações e a singularidade tecnológica (Wikipédia).

[8] "Uma nova civilização está emergindo em nossas vidas e por toda a parte há cegos tentando suprimi-la. Esta nova civilização traz consigo novos estilos de família, modos de trabalhar, amar e viver diferentes; uma nova economia; novos conflitos políticos; e além de tudo isto, igualmente uma consciência alterada. Fragmentos desta civilização já existem. Milhões de pessoas já estão sintonizando suas vidas com o ritmo de amanhã. Outros, aterrados diante do futuro, estão empenhados numa fuga inútil para o passado e tentam restaurar o mundo moribundo que lhes deu o ser". TOFFLER, Alvin. **A terceira onda.** Tradução João Távora. 29 ed. Rio de Janeiro: Record, 2007. n.p.

[9] MACHADO FILHO, op. cit., p. 156.

[10] "A Internet que conhecemos hoje atravessa uma de suas maiores e mais desafiantes revolução tecnológica, na qual teremos cada vez mais objetos e dispositivos inteligentes interconectados, trocando dados a todo instante através da sua interconexão. Este conceito é conhecido como a Internet das Coisas (Internet of Things – IoT, em inglês). Esta denominação foi cunhada por Kevin Ashton do MIT (Massachusetts Institute of Technology) em uma de suas apresentações em 2009 e acabou sendo adotado mundialmente para representar essas mudanças" ASHTON, 2009. *Apud*. FERRASI, Faberson Augusto. **O uso de mídias locativas no universo da internet das coisas:** construindo uma prova de conceito. 53f. Dissertação (Mestrado) - Faculdade de Arquitetura, Artes e Comunicação, Universidade Estadual Paulista, Bauru, 2017. Disponível em: http://hdl.handle.net/11449/150785. Acesso em: 14 jan. 2023. p. 16.

De acordo com o Glossário de Ciência dos Dados e Inteligência Artificial (*Data science and AI glossary*), publicado pelo Instituto Alan Turing[11], a definição de conjunto de dados (*Dataset*) está relacionada a uma coleção de números ou palavras que podem ser analisadas para obter informações, sendo que os dados podem vir de observações e medições da vida real ou podem ser gerados artificialmente ao reter as propriedades estatísticas dos dados originais.[12] Ainda de acordo com o Glossário, os dados sintéticos podem ser usados para aumentar um conjunto de dados com pontos de dados adicionais, muitas vezes para ajudar um sistema de inteligência artificial (IA)[13] a aprender alguma propriedade desejável ou para treinar algoritmos[14] em situações em que é perigoso obter os dados reais, como ensinar um carro autônomo a lidar com pedestres na estrada[15].

Em outra publicação, o Instituto Alan Turing informou que embora seja possível pensar nos dados como números em uma tabela, o que geralmente acontece, na realidade os dados estão em toda parte, o que significa que quase tudo o que é possível sentir pode ser capturado de alguma forma e analisado usando métodos de ciência de dados[16], como imagens e vídeos, fala e som, palavras e símbolos. Com todas estas formas de dados, seus formatos e estruturas

---

[11] O Alan Turing Institute (The Turing) é o instituto nacional do Reino Unido para ciência de dados e inteligência artificial.

[12] No original: "Dataset: A collection of numbers or words that can be analysed to obtain information. Datasets are often collected and stored in a tabular format, with each column corresponding to a different variable (e.g. height, weight, age) and each row corresponding to a different entry or 'record' (e.g. a different person). The data might come from real-life observations and measurements, or it can be generated artificially (see 'synthetic data')." DATA science and AI glossary. **The Alan Turing Institute**, London. Disponível em: https://www.turing.ac.uk/news/data-science-and-ai-glossary. Acesso em: 14 jan. 2023.

[13] De modo geral, as inteligências artificiais (IAs) são vistas como sistemas de aprendizagem, ou seja, são máquinas capazes de se aprimorarem em determinada tarefa, seja sob pouca ou nenhuma intervenção humana. Esses sistemas de aprendizagem podem ser montados por diversas técnicas e aplicações, agrupando as inteligências artificiais em diferentes categorias de tecnologia que vão depender de dados como matéria-prima. De acordo com o Glossário do Instituto Alan Turing, "a IA é um campo amplo que incorpora muitos aspectos diferentes da inteligência, como raciocínio, tomada de decisões, aprendizado com erros, comunicação, resolução de problemas e movimentação no mundo físico. A IA foi fundada como uma disciplina acadêmica em meados da década de 1950 e agora é encontrada em inúmeras aplicações cotidianas, incluindo assistentes virtuais, mecanismos de pesquisa, aplicativos de navegação e serviços bancários online." (tradução nossa). Ibidem.

[14] Algoritmo é, de acordo com o Glossário do Instituto Alan Turing: "Uma sequência de regras que um computador usa para concluir uma tarefa. Um algoritmo recebe uma entrada (por exemplo, um conjunto de dados) e gera uma saída (por exemplo, um padrão encontrado nos dados). Os algoritmos sustentam a tecnologia que faz nossas vidas funcionarem, de smartphones e mídias sociais a navegação por satélite e namoro online, e estão sendo cada vez mais usados para fazer previsões e apoiar decisões em áreas tão diversas quanto saúde, emprego, seguros e direito. (tradução autoral). Ibidem.

[15] No original: "Synthetic data: Data that is generated artificially, rather than by real-world events. It is especially useful for research in areas where privacy is key, such as healthcare and finance, as the generated data can retain the original data's statistical properties, but with any identifying information removed. Synthetic data can also be used to augment a dataset with additional data points, often to help an artificial intelligence system to learn some desirable property; or to train algorithms in situations where it is dangerous to get hold of the real data, such as teaching a self-driving car how to deal with pedestrians in the road". Ibidem.

[16] "Data science: An umbrella term for any field of research that involves the processing of large amounts of data in order to provide insights into real-world problems. Data scientists are a diverse tribe, ranging from engineers, medics and climatologists to ethicists, economists and linguists". Ibidem.

podem ser divididas em suas partes constituintes para encontrar padrões que podem ser usados para todos os tipos de aplicações, como para (i) recomendações e escolhas com base em gostos, desgostos, amigos e localização; (ii) reconhecimento facial para segurança e para outros serviços; (iii) verdades que os humanos talvez nunca vejam, simplesmente devido ao grande volume de exemplos que seria preciso digerir. As possibilidades são infinitas[17].

Retoma-se, então, a ideia de que há muito mais informações disponíveis hoje em dia do que nunca. Desde o surgimento das TICs, houve aumentos colossais no volume de dados produzidos todos os dias no meio digital, superando as quantidades de informações que antes eram gravadas e transmitidas somente por meios físicos, como o papel. Informações tornaram-se codificações de alfabeto binário e foram introduzidas em *softwares* em formatos de digitação, áudio e vídeo, possibilitando o acúmulo e a transmissão de informações de maneira inimaginavelmente maior e em tempo imediato.

De acordo com Bruno Bioni[18], "a revolução binária não somente comprimiu tangivelmente o armazenamento da informação, mas, igualmente, permitiu a ela um acesso mais facilitado. Houve, portanto, um progresso quantitativo e qualitativo do processamento informacional". Esses dois fatores facilitaram para que os dados fossem convertidos em conhecimento para fins produtivos e estratégicos da atividade empresarial, sendo destinados para as mais diversas e novas utilidades. Nesse sentido:

> Todo mundo sabe que a Internet mudou como as empresas operam, os governos funcionam e as pessoas vivem. Mas uma nova tendência tecnológica menos visível é igualmente transformadora: "big data". Big data começa com o fato de que há muito mais informações flutuando hoje em dia do que nunca, e estão sendo colocadas em novos usos extraordinários. Big data é diferente da Internet, embora a Web facilite muito a coleta e o compartilhamento de dados. Big data é sobre mais do que apenas comunicação: a ideia é que podemos aprender com um grande corpo de informações coisas que não conseguiriamos compreender usando apenas quantidades menores (tradução nossa).[19]

---

[17] THE ALAN TURING INSTITUTE. **Could AI solve your data problems?**. Disponível em: https://www.turing.ac.uk/events/could-ai-solve-your-data-problems. Acesso em: 14 jan. 2023.

[18] BIONI, Bruno Ricardo. **Proteção de dados pessoais:** a função e os limites do consentimento. 2. ed. Rio de Janeiro: Forense, 2020. p. 31.

[19] No original: "Everyone knows that the Internet has changed how businesses operate, governments function, and people live. But a new, less visible technological trend is just as transformative: "big data." Big data starts with the fact that there is a lot more information floating around these days than ever before, and it is being put to extraordinary new uses. Big data is distinct from the Internet, although the Web makes it much easier to collect and share data. Big data is about more than just communication: the idea is that we can learn from a large body of information things that we could not comprehend when we used only smaller amounts". CUKIER, Kenneth; MAYER-SCHOENBERGER, Victor. The Rise of Big Data: how it's changing the way we think about the world. **Foreign Affairs,** [*S.l*], n. 3, v. 92, may/june 2013. Disponível em: https://www.foreignaffairs.com/articles/2013-04-03/rise-big-data. Acesso em: 9 fev. 2021. p. 28.

A partir da grande disponibilidade de dados após as TICs, houve o desenvolvimento de uma economia global que despertou para o valor da análise de dados[20]. A magnitude das informações circulantes fez com que fosse cada vez mais instigante e urgente a aquisição de ferramentas necessárias para a absorção, avaliação e utilização dessas informações. Então, empresas especializadas em tecnologia desenvolveram ferramentas e *softwares* inteligentes com capacidade de analisar dados, desde o *software* mais simples até os mais elaborados - de tradução de texto, como o Google Tradutor, e de recomendações de livros e filmes, como o App Skoob e o Netflix, até reconhecimento facial e diagnóstico médico a partir de imagens.

Assim, os dados ganharam contornos de mercadoria no sistema capitalista, de forma que, deter a informação e o conhecimento tornou-se interessante para a competitividade de mercado. Agora, o que agrega valor é a informação associada ao acúmulo de conhecimentos e ao maior nível de complexidade do processamento da informação. Não é por acaso que, em 2014, a Meta (na época, apenas Facebook), comprou o WhatsApp[21], um dos aplicativos de mensagens instantâneas mais populares do mundo, por cerca de US$ 16 bilhões (R$ 86 bilhões) e que, apenas dois anos antes, havia comprado a rede social Instagram por US$ 1 bilhão (R$ 5,3 bilhões). Mais recente, em 2022, Elon Musk, CEO (*Chief Executive Officer*) da Tesla e da SpaceX, comprou por US$ 44 bilhões (R$ 233 bilhões) a rede social Twitter[22], o que representou uma das maiores aquisições das companhias de tecnologia.

Nesse contexto, cresceu assustadoramente a coleta e a comercialização de um tipo em especial de informações: as que dizem respeito à vida das pessoas. A *Internet* desempenha, nesse momento, o meio mais propício, uma vez que coloca o mundo todo no mesmo espaço: o virtual.

Um filósofo italiano, Lévy Pierre, refletiu sobre a temática da "virtualização" em sua obra "O que é o virtual?"[23]. Pesquisador em ciência da informação e da comunicação, estuda o impacto da *Internet* na sociedade, as humanidades digitais e o virtual. Em seu livro, Lévy revela que, no senso comum, o virtual seria caracterizado pela falta de materialidade ou a ausência de

[20] THE ECONOMIST. The world's most valuable resource is no longer oil, but data. **The Economist**, 2017. Disponível em: https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data. Acesso em: 16 jan. 2023.
[21] MÜLLER, Leonardo. Aquisição do WhatsApp pelo Facebook foi finalmente concretizada. **Tecmundo**, 2014. Disponível em: https://www.tecmundo.com.br/whatsapp/64054-aquisicao-whatsapp-facebook-finalmente-concretizada.htm. Acesso em: 16 jan. 2023.
[22] CNN BRASIL. Elon Musk compra Twitter por US $44 bilhões. **CNN Brasil**, 2022. Disponível em: https://www.cnnbrasil.com.br/business/elon-musk-compra-twitter-por-us-44-bilhoes/. Acesso em 16 jan. 2023.
[23] LÉVY, Pierre. **O que é o virtual?** Tradução de Paulo Neves do original "Qu'est-ce le virtuel?". São Paulo: Editora 34, 2003. p. 1-30.

existência de algo concreto. Contudo, o autor desmistifica o virtual como algo inexistente e defende que é tão existente quanto o real.

Da obra de Lévy, retira-se que a palavra latina "virtual" é derivada da definição de força e potência, portanto, ele considera o virtual como uma potência no sentido de processo, de tornar-se, vir a ser, e não um ato, algo constituído. Para o autor, "o virtual é um processo de transformação de um modo de ser num outro"[24], de modo que o virtual é tão existente quanto o real, como uma árvore está presente em uma semente, a exemplo dado pelo filósofo.

De modo geral, tem ocorrido uma virtualização da vida, pois o virtual está em todas as estruturas da sociedade, desde a criação de um perfil pessoal até as relações sociais, de trabalho e de consumo. No espaço virtual, a interação com os websites e aplicativos de provedores de conteúdo, seja por meio de imagens, áudios, check-ins, pesquisas, curtidas ou compartilhamentos, permite que tudo seja identificado, registrado, computado, lido e interpretado.[25] Dessa forma, pode-se dizer que houve uma virtualização das formas de exposição e de vigilância, que agora são exercidas de outras maneiras e que alimentam a economia informacional com cada vez mais dados.

A exemplo disso, Bernard Harcourt[26], em seu livro "Exposed" (2015)[27], analisa a construção de uma nova sociedade, que ele chama de expositiva, e que se configura como uma plataforma de níveis de exibição, vigilância e influência jamais vistos, cuja consequência é a reformulação das relações políticas e a modificação da racionalidade humana e seu significado de ser um indivíduo. Harcourt expõe a ideia de que essa vigilância é alimentada pelos próprios indivíduos que constantemente divulgam e atualizam seus dados na *Internet*, isto é, as pessoas estão normalizando a superexposição causada pelas novas tecnologias, de forma que não se escandalizam com isso, pelo contrário, a superexposição vem justamente pela própria vontade dos indivíduos de se expor e renunciar a privacidade e o anonimato, seja para acessar as redes sociais ou para fazer compras virtualmente. Seu livro traz a reflexão de que o ser humano começa a se importar com a privacidade quando sua perda é sentida por uma afronta à liberdade

---

[24] LÉVY, Pierre. **O que é o virtual?** Tradução de Paulo Neves do original "Qu'est-ce le virtuel?". São Paulo: Editora 34, 2003. p. 12.

[25] PÉREZ, Montse Hidalgo. Quantas mensagens de WhatsApp são necessárias para nos identificar? Não muitas. **El País**, Madri, 2021. Disponível em: https://brasil.elpais.com/tecnologia/2021-08-31/quantas-mensagens-de-whatsapp-sao-necessarias-para-nos-identificar-nao-muitas.html?rel=buscador_noticias. Acesso em: 16 jan. 2023.

[26] Bernard Harcourt, nascido em 1963, é um teórico crítico americano com especialização na área de punição, vigilância, teoria jurídica e política e economia política. Ele é professor na Columbia University Law School, em Nova York, e na École des Hautes Études en Sciences Sociales (EHESS), em Paris. Ele recebeu um diploma de bacharelado em teoria política pela Princeton University, em 1984, um diploma de Juris Doctor (Doutor em Direito) pela Harvard Law School, em 1989, e um Ph.D. em ciência política pela Harvard, em 2000 (Wikipédia).

[27] HARCOURT, Bernard E. The expository society. In: HARCOURT, Bernard E. **Exposed**: Desire and Disobedience in the Digital Age. Cambridge: Harvard University Press, 2015.

física, quando na verdade, a liberdade e a privacidade já foram perdidas pela exposição e vigilância no espaço virtual.

Para além da autoexposição, o desenvolvimento tecnológico tem feito com que as informações inseridas na *internet* não sejam feitas apenas por pessoas, mas também por coisas e algoritmos que possuem inteligência artificial e que trocam dados entre si. Assim, a exposição e vigilância não é somente exercida pela ação voluntária dos indivíduos, mas também é exercida por terceiros, seja por governos ou pela iniciativa privada, de forma mais tecnologicamente avançada que um dia já existiu. Assim, a vigilância coleta expressiva quantidade de informações e dados pessoais para diferentes interesses.

Consequência disso, a proteção dos dados pessoais se tornou um dos assuntos mais relevantes atualmente, enquanto que legisladores do mundo todo tem respondido a isso criando novas leis e regulamentações sobre o tema, definindo o que pode ser feito com esses dados e quais os direitos garantidos aos seus titulares, não só no espaço virtual, mas principalmente nele.

Yuval Noah Harari, em seu livro "21 lições para o século 21", afirmou que a questão mais importante na atual Era seria a regulamentação da propriedade dos dados, considerando que a humanidade não tem muita experiência no assunto tanto quanto possui com a propriedade da terra e a propriedade da indústria, isso porque regular os dados é uma tarefa mais difícil em razão de estarem "em toda parte e em parte alguma ao mesmo tempo"[28].

Consequentemente, as novas tecnologias desencadearam novos desafios para a ciência jurídica na proteção dos direitos fundamentais. A vulnerabilidade das pessoas cresceu na mesma proporção da inovação tecnológica, principalmente em relação a inseguranças e riscos para os dados pessoais sensíveis biométricos, recorte que será dado a esta pesquisa. A sociedade informacional necessita agora de meios eficazes de proteção dos dados que fornece e produz no mundo digital. Numa sociedade em que a quantidade de dados gerada por pessoas singulares será cada vez maior, o seu modo de coleta e de utilização deve dar primazia ao equilíbrio entre a inovação tecnológica e aos interesses individuais das pessoas, em consonância com os valores, as regras e os direitos fundamentais. Os cidadãos só irão confiar nas inovações baseadas em dados se estiverem seguros de que qualquer operação feita com seus dados pessoais estará sujeita à plena observância das regras e boas práticas em matéria de proteção de dados, por isso mostra-se tão relevante que o setor empresarial cumpra com essas diretrizes.

---

[28] HARARI, Yuval Noah. **21 lições para o século 21**. Tradução Paulo Geiger. 1. ed. São Paulo: Companhia das Letras, 2018. p. 110-111.

1.2 COMO A TECNOLOGIA PASSOU A RECONHECER ROSTOS?

O Doutor David Leslie[29], do Instituto Alan Turing, no guia explicativo de sua autoria "Entendendo o Viés nas Tecnologias de Reconhecimento Facial" (*Understanding bias in facial recognition technologies: an explainer*)[30], ensina um pouco sobre a história de como os computadores tornaram-se capazes de detectar, analisar e reconhecer rostos. Segundo ele, tudo começou na década de 1990, quando as câmeras digitais foram desenvolvidas e disponibilizadas no comércio em substituição àquelas câmeras fotográficas antigas que funcionavam com bobinas de filmes. Antes, as fotos eram produzidas a partir de filmes com produtos químicos sensíveis à luz e foram substituídas por imagens capturadas por fotossensores que convertem ondas de luz em grades de valores de pixels[31] registrando padrões de brilho e cor dessas ondas:

> Enquanto as câmeras tradicionais produziam fotos usando filme de celulóide revestido com produtos químicos sensíveis à luz, as câmeras digitais usavam fotossensores para capturar imagens convertendo ondas de luz em grades de valores de pixel que registravam os padrões de brilho e cor gerados por essas ondas recebidas. (tradução nossa)[32].

Essa conversão de ondas de luz em valores numéricos, conforme expressou o Doutor Leslie, foi revolucionária, porque tornou possível que computadores automaticamente compreendessem essa linguagem com padrões de números. Isso quer dizer que, a partir desse momento, as fotografias passaram a ser armazenadas e recuperadas como dados.

Com esse novo método, somado à expansão rápida da *Internet*, cada vez mais pessoas passaram a utilizar a *Web* para compartilhar e armazenar informações e mais e mais imagens digitais preencheram as páginas da *Web*, como nos sites de notícias e nas redes sociais, por exemplo, o Facebook. O Doutor Leslie destacou em seu guia explicativo que esse aumento exponencial de compartilhamento de conteúdo não só introduziu a revolução do *Big Data*, como também o crescente reservatório de imagens digitais online formou uma base para o

---

[29] Diretor de Ética e Pesquisa de Inovação Responsável no Alan Turing Institute e Professor de Ética, Tecnologia e Sociedade, Queen Mary University of London.

[30] LESLIE, David. **Understanding bias in facial recognition technologies:** an explainer. The Alan Turing Institute, 2020. Disponível em: https://doi.org/10.5281/zenodo.4050457. Acesso em: 16 jan. 2023.

[31] "Pixel é o menor elemento em um dispositivo de exibição, ao qual é possível atribuir-se uma cor. De uma forma mais simples, um pixel é o menor ponto que forma uma imagem digital, sendo que um conjunto de pixels com várias cores formam a imagem inteira." (Wikipédia)

[32] No original: "Whereas traditional cameras produced photos using celluloid film coated with light-sensitive chemicals, digital cameras used photosensors to capture images by converting light waves into grids of pixel values that recorded the patterns of brightness and colour generated by these incoming waves." LESLIE, op.cit.

desenvolvimento das tecnologias de visão computacional orientadas por dados, que evoluíram para as tecnologias de reconhecimento facial atuais[33].

A respeito do Big Data, o Instituto Alan Turing, em seu Glossário de Ciência dos Dados e Inteligência Artificial (*Data science and AI glossary*), definiu-o como um amplo campo de pesquisa que utiliza grandes conjuntos de dados e que possui como grande desafio a descoberta de como gerar, a partir dos dados, informações úteis que não comprometam a privacidade das pessoas a quem os dados se referem:

> Um amplo campo de pesquisa que lida com grandes conjuntos de dados. O campo cresceu rapidamente nas últimas duas décadas, à medida que os sistemas de computador se tornaram capazes de armazenar e analisar as grandes quantidades de dados cada vez mais coletados sobre nossas vidas e nosso planeta. Um dos principais desafios em big data é descobrir como gerar informações úteis a partir dos dados sem comprometer de forma inadequada a privacidade das pessoas a quem os dados se relacionam. (tradução nossa)[34].

Por sua vez, o *Information Commissioner's Office* (ico.)[35], autoridade responsável por supervisionar a proteção de dados no Reino Unido, publicou um documento sobre análise das implicações do Big Data, inteligência artificial e aprendizado de máquina (*machine learning*)[36], em que trouxe a definição popular de Big Data fornecido pelo Gartner[37] Information Technology Glossary: "Big Data é o alto volume, alta velocidade e alta variedade de ativos de informações que exigem formas inovadoras e econômicas de processamento de informações que permitem ideias aprimorados, tomada de decisão e automação de processos" (tradução nossa)[38]. A autoridade informou que, embora não haja uma definição única de Big Data,

---

[33] No original: "Not only did this exponential increase in content-sharing usher in the big data revolution, the growing online reservoir of digital images provided a basis for the development of the data-driven computer vision technologies that have evolved into today's FDRTs (...)." LESLIE, op. cit.

[34] No original: "A wide-ranging field of research that deals with large datasets. The field has grown rapidly over the past couple of decades as computer systems became capable of storing and analysing the vast amounts of data increasingly being collected about our lives and our planet. A key challenge in big data is working out how to generate useful insights from the data without inappropriately compromising the privacy of the people to whom the data relates." DATA science and AI glossary. **The Alan Turing Institute**, op. cit.

[35] Information Commissioner's Office (ico.). Disponível em: https://ico.org.uk/. Acesso em 16 jan. 2023.

[36] INFORMATION COMMISSIONER'S OFFICE (ico.). Big data, artificial intelligence, machine learning and data protection. v. 2.2. **Information Commissioner's Office (ico.)**, [s/d]. Disponível em: https://ico.org.uk/media/for-organisations/documents/2013559/big-data-ai-ml-and-data-protection.pdf. Acesso em: 16 jan. 2023.

[37] "Gartner é uma empresa de consultoria fundada em 1979 por Gideon Gartner. A Gartner desenvolve tecnologias relacionadas a introspecção necessária para seus clientes tomarem suas decisões todos os dias". (Wikipédia).

[38] No original: "Big data is high-volume, high-velocity and/or high-variety information assets that demand cost-effective, innovative forms of information processing that enable enhanced insight, decision making, and process automation" GARTNER. **Information Technology Glossary.** Disponível em: https://www.gartner.com/en/information-technology/glossary/big-data. Acesso em: 16 jan. 2023.

consideram-na como dados que, devido a muitas características variáveis, são difíceis de analisar usando métodos tradicionais de análise de dados[39].

A partir dessa incalculável quantidade de informações, os sistemas de reconhecimento facial foram desenvolvidos conforme a evolução de quatro períodos ao longo dos anos com base no lançamento de três bases de dados que continham imagens de faces humanas[40]. No primeiro período, considerado entre 1964 a 1995, o reconhecimento facial através do computador foi devido a Woodrow Bledsoe que, em 1964, usou um conjunto de dados de fotografias de faces frontais e de lado e um algoritmo que usava um vetor (conjunto ordenado de números) de distâncias entre pontos faciais. Esse primeiro estágio foi um sucesso e, junto com o aperfeiçoamento das câmeras e do computador, novos algoritmos de processamento de imagens e novas técnicas de aprendizado de máquina foram desenvolvidos[41].

Por sua vez, o segundo período, compreendido entre 1996 a 2006, foi marcado pelo investimento do governo norte americano na criação de uma base de dados destinado aos estudos em tecnologia de reconhecimento facial, que inaugurou o "*Face Recognition Technology*" (FERET), um conjunto de dados maior e mais abrangente. Assim, foi possível a utilização de novos métodos de aprendizado de máquina para visão computacional, porém os resultados ainda eram limitados a esse banco de dados e restritos a fotografias de faces frontais e de lado, bem como estavam sujeitos a falhas quando pequenas mudanças ocorriam, como alteração na luminosidade ou adição de algum adereço no rosto[42].

Como consequência das limitações anteriores, o terceiro período, de 2007 a 2013, consagrou os esforços para melhorias e, a partir de um banco de dados já existente, chamado "*Faces in the Wild*", em conjunto com fotos do sítio eletrônico de notícias do "*Yahoo News*", que continham faces em poses variadas e em diferentes iluminações, foi lançado o "*Labeled Faces in the Wild*" (LFW). Os métodos continuaram os mesmos, na esperança de que os resultados melhorariam com novos conjuntos de dados, o que não foi suficiente[43].

---

[39] No original: "While there is no unassailable single definition of big data, we think it is useful to regard it as data which, due to several varying characteristics, is difficult to analyse using traditional data analysis methods." INFORMATION COMMISSIONER'S OFFICE (ico.), op. cit.

[40] Parecer produzido pelo InternetLab para a Ação Civil Pública contra reconhecimento facial para fins de segurança pública no Metrô de São Paulo. ABELLO, Antonio A.; ARAÚJO, Rafael Will Macêdo de.; HIRATA JR., R. **Parecer InternetLab.** Mar, 2021. Disponível em: https://internetlab.org.br/wp-content/uploads/2022/03/Parecer-Metro-de-Sao-Paulo.-Reconhecimento-facial.pdf. Acesso em: 17 jan. 2023.

[41] Ibidem, p. 13-14.

[42] Ibidem, p. 14-15.

[43] Ibidem, p. 15-16.

Por fim, de 2014 até os dias de hoje, destaca-se o quarto período de desenvolvimento do reconhecimento facial, em que foi criado um modelo neural profundo chamado "*DeepFace*", desenvolvido por pesquisadores do Facebook que usaram fotos dos perfis dos usuários:

> O conjunto relatado é de 4,4 milhões de imagens de faces pertencentes a 4.030 pessoas diferentes (de 800 a 1.200 imagens de faces por pessoas). O maior impacto deste avanço é, sem dúvida, o aumento da quantidade de acertos em quase 27% do estado da arte anterior (ou, 97,35% de acurácia)[44].

Pelo exposto até aqui, pode-se notar que os enormes conjuntos de imagens digitais inseridas no astronômico montante de dados disponíveis no universo virtual alimentaram o treinamento de muitos modelos de detecção e reconhecimento facial que se originaram no nascimento da era da *Internet*. Além disso, foi possível compreender a evolução histórica das características dos campos de amostragem utilizados para os treinamentos de máquina. Entretanto, ainda permanece a dúvida de como realmente uma tecnologia é capaz de "ver" um rosto em uma imagem.

A construção de sistemas artificiais que obtêm informações de imagens ou vídeos digitais, tentando dar ao computador um pouco da extraordinária capacidade do conjunto olho-cérebro humano, é tarefa desenvolvida por uma ciência chamada Visão Computacional, uma subárea da Ciência da Computação. Assim, essa área científica dedica-se à construção de algoritmos de visão computacional que são capazes de "ler" dados e tomar decisões sem interferência humana. Esses algoritmos são, conforme definição do Glossário do Instituto Alan Turing, "uma sequência de regras que um computador usa para concluir uma tarefa. Um algoritmo recebe uma entrada (por exemplo, um conjunto de dados) e gera uma saída (por exemplo, um padrão encontrado nos dados)"[45]. Portanto, entende-se que uma tecnologia consegue "ver" algo com base em uma sequência de regras (comandos) preestabelecidas para executar uma atividade e alcançar o objetivo de extrair informações úteis e relevantes desejadas.

O que os algoritmos de visão computacional, de fato, "veem" em uma imagem digital são valores numéricos, isto é, apenas uma matriz de números (linhas e colunas de números

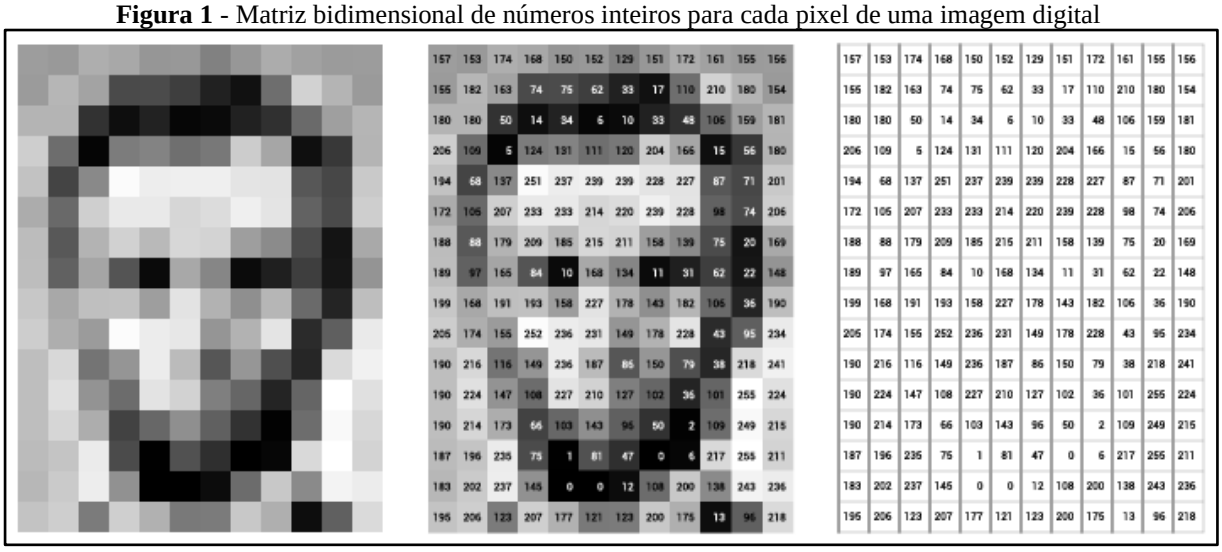
---

[44] Ibidem, p. 16.

[45] No original: "A sequence of rules that a computer uses to complete a task. An algorithm takes an input (e.g. a dataset) and generates an output (e.g. a pattern that it has found in the data). Algorithms underpin the technology that makes our lives tick, from smartphones and social media to sat nav and online dating, and they are increasingly being used to make predictions and support decisions in areas as diverse as healthcare, employment, insurance and law." DATA science and AI glossary. **The Alan Turing Institute**, op. cit.

indicando intensidades de cor e brilho) correspondentes aos menores elementos da imagem, os pixels (*picture elements*)[46], conforme demonstrado na Figura 1 abaixo:

Figura 1 - Matriz bidimensional de números inteiros para cada pixel de uma imagem digital



Fonte: Google Imagens.

Portanto, a detecção do rosto de um ser humano em uma imagem por um algoritmo de visão computacional requer que ele leia a matriz de números, que representam cores, tons e brilho e identifique padrões nos valores dos pixels que indiquem com segurança que se tratam de características faciais[47].

O Doutor Leslie explica que, para as primeiras técnicas de visão computacional de detecção de faces em imagens digitais, foram feitas regras representando características típicas da fisionomia do rosto humano, por exemplo, "uma face tem dois conjuntos simétricos de olhos e ouvidos". As regras eram codificadas em matrizes numéricas para que o *software* tentasse encontrar esses padrões correspondentes nos valores de intensidade do pixel. Contudo, dois problemas foram notados: (i) a criação de regras que traduzem características do rosto humano para fórmulas matemáticas era desafiador em razão da imprecisão da linguagem e das numerosas formas que as faces humanas podem refletir a mesma regra; (ii) esse método das regras somente funcionava bem em fotos uniformes, isto é, nas quais os objetos estivessem voltados para frente e as condições de iluminação, obstrução, orientação, posição e expressão facial, fossem relativamente parecidas[48].

---

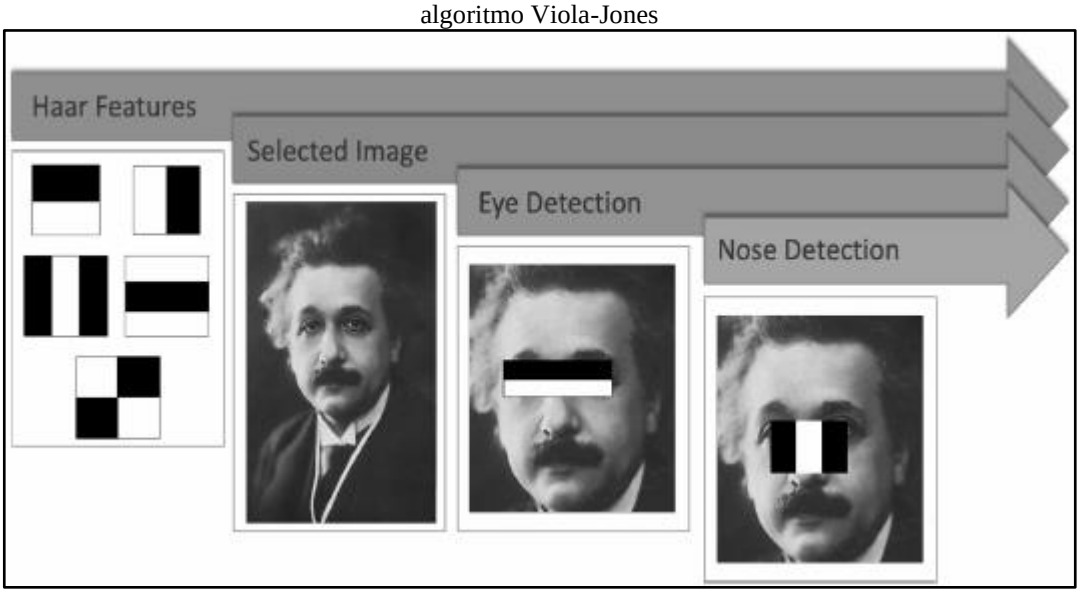
[46] ALBUQUERQUE, Márcio Pontes de; CANER, Eugenio S.; MELLO, Aline Gesualdi; ALBUQUERQUE, Marcelo Pontes de. **Análise de Imagens e Visão Computacional.** Centro Brasileiro de Pesquisas Físicas (CBPF), 2012. Disponível em: https://mesonpi.cat.cbpf.br/e2012/arquivos/g06/CursoE2012-PI.pdf. Acesso em 20 jan. 2023. p. 3.
[47] LESLIE, op.cit., p. 8.
[48] Ibidem, p. 9.

O método de visão computacional começou a mudar para uma abordagem baseada em dados conforme foi crescendo a disponibilidade de imagens digitais no início do século, como visto anteriormente. Nesse segundo momento, os algoritmos foram treinados para que eles mesmos aprendessem e extraíssem características e propriedades faciais a partir de grandes conjuntos de dados, buscando encontrar aspectos invariáveis do rosto entre tantas condições diferentes nas imagens.

Dessa forma, a partir de 2001, começou a ser usado um algoritmo de detecção facial em imagens que utilizava a combinação de classificadores para o treinamento de máquina. Desenvolvido pelos pesquisadores Paul Viola e Michael Jones, o "algoritmo Viola-Jones" passou a fazer a leitura das imagens usando formas retangulares simples pré-classificadas, conhecidas como Recursos de Haar, para identificar padrões comuns que permitiam a detecção facial rápida. Assim, foram criados classificadores em formatos retangulares para representar uma determinada região do rosto conforme as diferentes intensidades de brilho. Por exemplo, "a testa é mais clara que a área dos olhos" ou "as áreas laterais do nariz são mais escuras que a parte central", o que funciona para qualquer tipo de rosto. A combinação de classificadores permitiu identificar nas imagens a existência de regiões que se pareciam com os olhos e com o nariz de acordo com as tonalidades, verificando se havia ou não uma face. Os Recursos de Haar eram expressos em valores numéricos e colocados sobre a grade numérica da imagem para serem deslizados por toda a imagem, de parte em parte, a fim de encontrar as áreas em que as mudanças correspondentes na intensidade do brilho revelassem correspondências com padrões faciais[49]. A Figura 2 abaixo mostra o funcionamento desse mecanismo:

[49] LESLIE, op. cit., p. 10.

Figura 2 - Representação dos Recursos de Haar para detecção de olhos e nariz utilizados pelo algoritmo Viola-Jones



Fonte: Understanding bias in facial recognition technologies: an explainer[50].

Apesar do algoritmo Viola-Jones ser capaz de identificar uma face em uma imagem de forma mais rápida que antes, ainda não era possível a distinção entre um rosto e outro ou mesmo a identificação de rostos iguais entre muitos. Nota-se que, até o momento, não se falava em reconhecimento facial, mas apenas detecção facial, justamente pela limitação que os algoritmos apresentavam em não conseguir comparar, distinguir e identificar rostos. Para que isso fosse possível, era preciso que características faciais fossem extraídas das imagens digitais.

O rompimento com essas limitações aconteceu por meio das Redes Neurais Convolucionais (*Convolutional Neural Network - CNN*), algoritmos que se tornaram uma ferramenta importante para o reconhecimento de elementos em imagens e que puderam ir além, principalmente na extração de características faciais humanas. De modo geral e sem aprofundar no assunto tão vasto, as CNNs são um tipo de rede neural, ou seja, uma inteligência artificial inspirada no cérebro biológico que utiliza a técnica de aprendizado de máquina chamada de *deep learning* para o reconhecimento de padrões em imagens e o fornecimento de uma resposta. Esses sistemas consistem em um enorme "conjunto de unidades computacionais simples e interconectadas ('neurônios'), com dados passando entre eles como entre neurônios no cérebro. As redes neurais podem ter centenas de camadas desses neurônios, com cada camada desempenhando um papel na solução do problema"[51].

[50] LESLIE, op. cit., p. 9.
[51] No original: "Neural network: An artificial intelligence system inspired by the biological brain, consisting of a large set of simple, interconnected computational units ('neurons'), with data passing between them as between neurons in the brain. Neural networks can have hundreds of layers of these neurons, with each layer playing a role in solving the problem. They perform well in complex tasks such as face and voice recognition. See also 'deep learning'." DATA science and AI glossary. **The Alan Turing Institute**, op. cit.

Segundo o Doutor Leslie, as CNNs

> (...) dividem a matriz bidimensional de valores de pixel de uma imagem digital em partes menores, mas, em vez de deslizar formas retangulares pela imagem em busca de correspondências, elas ampliam trechos específicos da imagem usando grades menores de valores de pixels chamados kernels (...). Esses kernels criam mapas de recursos movendo-se passo a passo por toda a imagem tentando localizar correspondências para o recurso específico que a rede neural treinou cada um deles para procurar. Uma camada convolucional é composta por uma pilha desses mapas de recursos e qualquer modelo CNN pode ter muitas camadas de profundidade. (...) Cada próxima camada é capaz de combinar os recursos das camadas anteriores para extrair padrões que estão em níveis mais altos de complexidade e abstração. (tradução nossa)[52].

O modelo de aprendizado de máquina das CNNs extrai padrões das imagens a partir do que aprendeu de grandes conjuntos de dados anteriormente rotulados. Geralmente a rotulagem dos dados é feita por humanos que os identificam como pertencente ou não a classe de dados em que o algoritmo procura encontrar o resultado. No caso do reconhecimento facial, por exemplo, uma grande quantidade de imagens é classificada em categorias como "contém rostos" e outra em "não contém rostos". Esses conjuntos de dados categorizados em uma ampla variedade de tipos são a base sobre a qual os sistemas de detectar e reconhecer faces atualmente são construídos, bem como são responsáveis por moldar o funcionamento deles. O conhecimento desse mecanismo é peça chave para compreensão de dilemas socialmente relevantes sobre a tecnologia em questão, que serão apontados posteriormente.

Após esse estágio de desenvolvimento da técnica de reconhecimento de rostos humanos em imagens digitais, outros aprimoramentos surgiram a partir das CNNs, mas que não serão exploradas na presente pesquisa em razão de não ser a pretensão. Contudo, algo relevante para este estudo, nota-se que a construção desses sistemas inteligentes requer uma significativa quantidade de dados contidos em conjuntos pré classificados de imagens de feições humanas. Dessa maneira, em conformidade com o que foi visto no tópico anterior, "não é difícil ver como a explosão da disponibilidade de imagens digitais na internet alimentou o desenvolvimento de

[52] No original: "CNNs break down a digital image's two-dimensional array of pixel values into smaller parts, but instead of sliding rectangular shapes across the image looking for matches, they zoom in on particular patches of the image using smaller grids of pixels values called kernels (Figure 3). These kernels create feature maps by moving step-by-step through the entire image trying to locate matches for the particular feature that the neural net has trained each of them to search for. A convolutional layer is composed of a stack of these feature maps, and any given CNN model may be many layers deep. (...) Each next layer is able to combine the features from previous layers to extract patterns that are at higher levels of complexity and abstraction." LESLIE, op. cit., p. 10.

CNNs e outras técnicas de aprendizado profundo relacionadas como os algoritmos dominantes de visão computacional da era do big data"[53].

A título de percepção da quantidade de dados disponíveis e frequentemente usados para treinamento de algoritmos, até 2017, o JFT-300M do Google era o maior conjunto de dados de origem da Internet, que continha 300 milhões de imagens, abarcando mais de 1 bilhão de objetos marcados com algoritmos, extraídos de 18 mil classes.[54] Em relação às tecnologias de reconhecimento facial, em 2007 havia o conjunto de dados LFW, composto por 13 mil imagens de quase 6 mil identidades de indivíduos, o que foi superado, em 2018, pelo VGGFace2 da Universidade de Oxford[55], que continha mais de 3,3 milhões de imagens de cerca de 9 mil identidades de indivíduos[56].

1.3 O QUE É, COMO FUNCIONA E OBJETIVOS DA TECNOLOGIA DE RECONHECIMENTO FACIAL

A tecnologia de reconhecimento facial tem sido empregada tanto pelo setor empresarial quanto por governos para diversas finalidades, por exemplo, para vigilância em locais públicos, controle de acessos e segurança, desbloqueio de celular e aplicativos, abertura de uma conta bancária, pagamentos online, registros de ponto de colaboradores, entre outras funções utilizadas diariamente pelas pessoas e que, portanto, despertam o interesse para o conhecimento da técnica dessas tecnologias[57].

---

[53] No original: "It's not difficult to see how the explosion of the availability of digital images on the internet fuelled the development of CNNs and other related deep learning techniques as the dominant computer vision algorithms of the big data age." LESLIE, op.cit., p. 12.

[54] Mais informações sobre o JFT-300M em: SUN, Chen; SHRIVASTAVA, Abhinav; SINGH, Saurabh; GUPTA, Abhinav. Revisiting Unreasonable Effectiveness of Data in Deep Learning Era. **Cornell University**, arXiv, 2. v., aug. 2017. Disponível em: https://doi.org/10.48550/arXiv.1707.02968. Acesso em: 01 fev. 2023.

[55] Obtenha o dataset VGGFace2 em: https://www.robots.ox.ac.uk/~vgg/data/vgg_face2/. Acesso em: 01 fev. 2023.

[56] No original: "By 2017, the largest of the internet-sourced datasets, Google's JFT-300M, included 300 million images, containing over 1 billion algorithmically labelled objects drawn from 18 thousand classes. Meanwhile, in the more specialised world of FDRTs, the modest "Labelled Faces in the Wild" dataset, released in 2007 and comprised of 13 thousand images of almost 6 thousand individual identities, would be eclipsed by the likes of Oxford University's 2018 VGGFace2 dataset, which contained over 3.3 million images of about 9 thousand individual identities (...)" LESLIE, op.cit., p. 12.

[57] Exemplo de usos do reconhecimento facial na prática: G1. **Latam, Gol e Azul disponibilizam embarque com reconhecimento facial a partir desta terça-feira.** 9 ago. 2022. Disponível em: https://g1.globo.com/turismo-e-viagem/noticia/2022/08/09/gol-disponibiliza-embarque-com-reconhecimento-facial-a-partir-desta-terca-feira.ghtml. Acesso em: 9 jan. 2023.; G1. **A democracia que usa reconhecimento facial para registrar os rostos de seus cidadãos.** 8 ago. 2022. Disponível em: https://g1.globo.com/tecnologia/noticia/2022/08/08/a-democracia-que-usa-reconhecimento-facial-para-registrar-os-rostos-de-seus-cidadaos.ghtml. Acesso em: 9 jan. 2023.; G1. **Metrô de SP adota novo sistema de reconhecimento facial.** 21 nov. 2022. Disponível em: https://g1.globo.com/sp/sao-paulo/sp2/video/metro-de-sp-adota-novo-sistema-de-reconhecimento-facial-11144903.ghtml. Acesso em: 9 jan. 2023.

O reconhecimento facial pode ser entendido como uma aplicação de inteligência artificial[58] que se utiliza da técnica de coleta de biometria baseada em traços do rosto humano. Esse processo é realizado a partir da medição de pontos da face que fazem uma ligação algorítmica de traços e tamanhos, levando em consideração a distância exata entre nariz e orelhas, espaçamento dos olhos, tamanho da testa, contorno dos lábios, entre outras medidas. A partir dessas medições do rosto, extrai-se o dado biométrico, que possibilita a verificação e a autenticação da identidade de uma pessoa ao basear-se nas características exclusivas e específicas desse indivíduo. Essas informações, que se transformam em números, na maioria das situações permanecem armazenadas para eventual necessidade de comparação futura desses dados com outros. No caso do reconhecimento facial, as particularidades da biometria são faciais, diferentemente da impressão digital e da voz, que são outros tipos de dados biométricos.

A legislação brasileira não possui disposição específica para definição de dado biométrico. Contudo, o Glossário Eleitoral[59], disponível no Portal do Tribunal Superior Eleitoral (TSE), dispõe que biometria é a "tecnologia que permite identificar uma pessoa por características biológicas únicas, ou seja, por elementos corporais que tenham diferenças particulares, como a impressão digital, a íris, a retina, a voz e o formato do rosto e o da mão."

De acordo com o Artigo 4º, nº 14, do Regulamento Geral de Proteção de Dados europeu (RGPD) ou, em inglês, *General Data Protection Regulation* (GDPR)[60], dados biométricos são considerados os dados "resultantes de um tratamento técnico específico relativo às características físicas, fisiológicas ou comportamentais de uma pessoa singular que permitam ou confirmem a identificação única dessa pessoa singular, nomeadamente imagens faciais ou dados dactiloscópicos" (impressão digital). Em momento oportuno, este trabalho discorrerá sobre a proteção legal destinada ao dado biométrico e sua implicação no desenvolvimento e na implementação de tecnologias destinadas a reconhecer rostos humanos.

O reconhecimento facial, segundo o Guia de boas práticas desenvolvido pela parceria entre o InternetLab e o Instituto Brasileiro de Defesa do Consumidor (Idec)[61], é um tipo de aplicação de inteligência artificial que utiliza o método *machine learning* para aprender a

---

[58] Ver sobre inteligência artificial em: COMISSÃO EUROPEIA. **Uma Definição de IA:** principais capacidades e disciplinas científicas. Comissão Europeia, 2019. Disponível em: https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai. Acesso em: 27 jan. 2023.

[59] TRIBUNAL SUPERIOR ELEITORAL (TSE). **Glossário Eleitoral.** Disponível em: https://www.tse.jus.br/servicos-eleitorais/glossario/termos-iniciados-com-a-letra-b. Acesso em: 23 jan. 2023.

[60] UNIÃO EUROPEIA. Regulamento (UE) nº 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016. Relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados). **Jornal Oficial da União Europeia**, Bruxelas, 27 abr. 2016. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX: 32016R0679 & from=PT. Acesso em: 23 jan. 2023.

[61] Conheça o Idec em: https://idec.org.br/.

identificar rostos humanos a partir de uma base de dados de fotos pré-classificadas, por exemplo, em “rosto humano” ou “não rosto humano”. Nesse sentido:

> O reconhecimento facial é uma das funcionalidades dos algoritmos classificatórios. Trata-se de uma das aplicações de uma vertente específica da inteligência artificial: o aprendizado de máquina – ou machine learning, como é conhecido em inglês. Grosso modo, para poderem desempenhar essa funcionalidade, tais algoritmos utilizam uma base de treinamento, ou seja, uma base de fotos pré-classificadas por seres humanos como (em seu nível mais simples) “rosto humano” ou “não rosto humano”, gerando um modelo estatístico que irá representar os atributos mais presentes nos rostos apresentados (e.g. a presença de sobrancelhas, nariz, distância entre os olhos etc.) Com base nisso, poderão detectar a presença de um rosto humano na imagem analisada[62].

Machine learning, segundo o Glossário do Instituto Alan Turing, é um campo de inteligência artificial que envolve algoritmos de computador que podem “aprender” encontrando padrões em dados de amostra, o que permite que os algoritmos normalmente apliquem essas descobertas a novos dados para fazer previsões ou fornecer outros resultados (saídas) úteis, como simplesmente traduzir texto ou até guiar um robô em uma nova configuração[63].

Para ajudar a compreender as tecnologias que reconhecem e identificam rostos, algumas autoridades de proteção de dados internacionais publicaram documentos técnicos sobre o tema que trazem definições e explicações. Nesse sentido, o *Information Commissioner's Office* (ico.)[64], autoridade do Reino Unido, considera que a tecnologia de reconhecimento facial é aquela que identifica ou reconhece uma pessoa a partir de uma imagem facial digital, de modo que isso acontece a partir da junção de câmeras que capturam as imagens, que contém um *software* de reconhecimento facial - incorporando elementos de inteligência artificial (IA), algoritmos e processos de aprendizado de máquina - e são responsáveis pela medição e análise das características do rosto das pessoas nas imagens, com o propósito de produzir um modelo biométrico, o que irá possibilitar a identificação, autenticação ou categorização de indivíduos. Nessa lógica:

> Frequentemente, o software que incorpora elementos de inteligência artificial (IA), algoritmos e processos de aprendizado de máquina estima o grau de semelhança entre

[62] SIMÃO, Bárbara; FRAGOSO, Nathalie; ROBERTO, Enrico. Reconhecimento Facial e o Setor Privado: Guia para a adoção de boas práticas. **InternetLab/IDEC**, São Paulo, 2020. Disponível em: https://idec.org.br/sites/default/files/reconhecimento_facial_diagramacao_digital_2.pdf. Acesso em: 12.01.2023.
[63] DATA science and AI glossary. **The Alan Turing Institute**, op. cit.
[64] INFORMATION COMMISSIONER'S OFFICE. Guidance on video surveillance (including CCTV). **Information Commissioner's Office (ico.)**, 2022. Disponível em: https://ico.org.uk/media/for-organisations/guide-to-data-protection/key-dp-themes/guidance-on-video-surveillance-including-cctv-1-0.pdf. Acesso em: 16 jan. 2023.

> dois modelos faciais para identificar uma correspondência. Por exemplo, para verificar a identidade de alguém ou para colocar um modelo em uma categoria específica (por exemplo, faixa etária)[65] (tradução nossa).

No mesmo sentido foi a definição apresentada pela *Commission Nationale de l'Informatique et des Libertés* (CNIL.)[66], autoridade supervisora em matéria de proteção de dados na França, em seu documento oficial publicado[67]. As suas contribuições sobre o reconhecimento facial e as novas utilizações das câmeras de vídeo levantaram um ponto importante para o debate: os termos devem ser claros a ponto de se saber a abrangência do conceito de reconhecimento facial, para evitar que os diferentes casos de utilização dessa tecnologia, que não levantam as mesmas dificuldades, sejam tratados da mesma forma, ou que o mesmo tratamento também ocorra com tecnologias similares, mas de natureza diferente[68].

Sendo assim, a CNIL. esclarece que o reconhecimento facial ocorre em uma ampla gama de técnicas de processamento de imagens de vídeo, mas que essa condição por si só não quer dizer que todas as câmeras de vídeo permitirão o reconhecimento automático de indivíduos, como não será em uma simples captura de vídeo para monitoramento de um determinado local ou de captura de fotografia. Ou seja, uma câmara não é um sistema de reconhecimento facial, bem como a mera detecção de rostos por câmeras não constitui um dispositivo de reconhecimento facial, porque, para assim o ser, as fotografias das pessoas devem ser objeto de um procedimento específico para extrair dados biométricos[69]. Portanto,

> [...] embora também levantem questões importantes em termos de ética ou eficiência, as técnicas informáticas de detecção de comportamentos anormais ou de eventos violentos, de reconhecimento de emoções em rostos ou mesmo em silhuetas não constituem geralmente sistemas biométricos[70].

---

[65] No original: "Facial recognition technology identifies or otherwise recognises a person from a digital facial image. Cameras are used to capture these images and facial recognition software measures and analyses facial features to produce a biometric template. This typically enables the user to identify, authenticate or verify, or categorise individuals. Often, the software which incorporates elements of artificial intelligence (AI), algorithms and machine learning processes estimates the degree of similarity between two facial templates to identify a match. For example, to verify someone's identity, or to place a template in a particular category (e.g. age group)." INFORMATION COMMISSIONER'S OFFICE. Guidance on video surveillance (including CCTV), op.cit.

[66] Conheça a *Commission Nationale de l'Informatique et des Libertés* (CNIL.) em: https://www.cnil.fr/en/home. Acesso em: 18 jan. 2023.

[67] COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS. Reconnaissance faciale: pour un débat à la hauteur des enjeux. **Commission Nationale de l'Informatique et des Libertés (CNIL.)**, 2019. Disponível em: https://www.cnil.fr/fr/reconnaissance-faciale-pour-un-debat-la-hauteur-des-enjeux. Acesso em: 18 jan. 2023.

[68] Ibidem, p. 2.

[69] Ibidem, p. 4.

[70] No original: "La seule détection de visages par des caméras dites « intelligentes » ne constitue pas davantage un dispositif de reconnaissance faciale. Si elles soulèvent elles aussi d'importantes questions en termes éthiques ou d'efficacité, les techniques informatiques de détection de comportements anormaux ou d'événements violents, de reconnaissance d'émotions sur les visages ou même de silhouettes ne constituent pas généralement pas des systèmes biométriques." Ibidem, p. 4.

Entretanto, a CNIL. faz uma ressalva de que os exemplos citados não estão imunes, uma vez que o reconhecimento facial é um recurso de *software* que pode ser associado a outros sistemas, câmeras, bancos de dados etc., de forma que poderão passar a extrair a biometria.

O Grupo de Trabalho do Artigo 29 (*Article 29 Data Protection Working Party*)[71], que em maio de 2018 foi substituído pelo Conselho Europeu de Proteção de Dados (*European Data Protection Board* - EDPB), no Parecer 02/2012 (*WP 192*)[72] sobre reconhecimento facial em serviços online e de celular, expressou que essa tecnologia é o processamento automático de imagens digitais que contenham rostos de indivíduos com o propósito de identificação, autenticação/verificação ou categorização daqueles indivíduos.

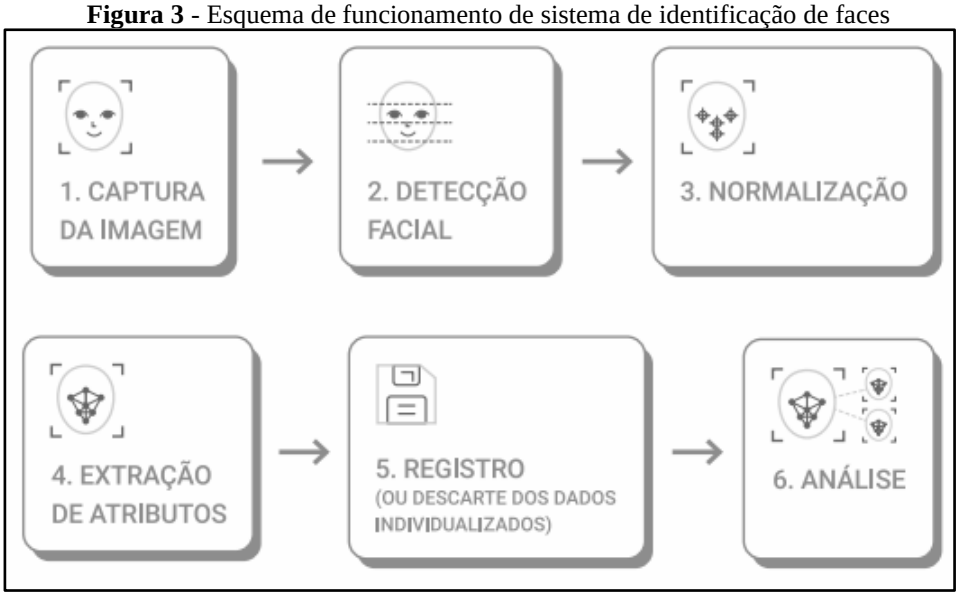
Assim como a ico., o Parecer 02/2012 (*WP 192*) também destacou, na definição de reconhecimento facial, as finalidades dessa tecnologia: identificação, autenticação e categorização. Para atingir esses objetivos, o mecanismo de processamento das imagens, então, passa por alguns subprocessos, como: (i) aquisição de imagem: captura da face através de uma câmera e sua conversão em formato digital; (ii) detecção de rosto: localização de um rosto na imagem capturada e sua demarcação; (iii) normalização: suavização das variações na imagem, como conversão em tamanho padrão, rotação para adequar o ângulo e distribuição de cores; (iv) extração de características atributo: isolamento e extração de leituras repetíveis e distintas, sendo que o conjunto de características chave pode ser armazenado para ser modelo de referência em uma comparação posterior; (v) registro: se for a primeira vez que um indivíduo mostra o rosto em um sistema de reconhecimento, a imagem e/ou modelo de referência pode ser armazenado como um registro para comparação posterior; por fim, (vi) comparação/análise: medição da similaridade entre o conjunto de características extraídas (amostra) com outro conjunto previamente cadastrado. Essa fase de comparação irá variar conforme a finalidade da tecnologia. Na Figura 3 abaixo, é possível visualizar os subprocessos descritos.

---

[71] O "Grupo de Trabalho do Artigo 29" é o nome abreviado do Grupo de Trabalho de Proteção de Dados estabelecido pelo Artigo 29 da Diretiva 95/46/EC (sobre processamento e livre circulação de dados na UE). Forneceu à Comissão Europeia aconselhamento independente sobre questões de proteção de dados e ajudou no desenvolvimento de uma implementação harmonizada das regras de proteção de dados nos Estados-Membros da UE. Após 25 de maio de 2018, o Grupo de Trabalho do Artigo 29 deixou de existir e foi substituído pelo Conselho Europeu de Proteção de Dados (EDPB). O site da EDPB pode ser consultado no seguinte endereço: https://edpb.europa.eu/.

[72] WORKING PARTY. Article 29. **Opinion 02/2012 on facial recognition in online and mobile services** (WP 192). Bruxelas, 2012. Disponível em: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp192_en.pdf. Acesso em: 19 jan. 2023. p. 2.

Figura 3 - Esquema de funcionamento de sistema de identificação de faces



Fonte: Reconhecimento Facial e o Setor Privado: Guia para a adoção de boas práticas. InternetLab/IDEC, 2020[73].

É no momento de extração dos atributos (item iv) que são retiradas as informações úteis da face da pessoa para a análise desejada. As informações seriam as características geométricas de forma, localização e distância da boca, olhos, nariz, orelhas, entre outras. Após esse passo, existem duas possibilidades a depender da finalidade do emprego da tecnologia de reconhecimento facial: (a) descarte imediato dos dados coletados do rosto; ou (b) armazenamento desses dados. A primeira situação seria apenas para os casos em que o objetivo seja gerar relatórios estatísticos sobre os indivíduos, o que poderia ser usado, por exemplo, para o direcionamento de propagandas para consumidores em tempo real. O não armazenamento dos dados inviabilizaria a comparação entre imagens (sexto subprocesso), portanto, impediria a verificação ou identificação de uma pessoa.

Além disso, segundo o Parecer 02/2012 (*WP 192*) do Artigo 29, os objetivos mais comuns da comparação são a identificação e a autenticação/verificação, o que, portanto, pressupõe o armazenamento. A categorização é outro objetivo de um sistema de reconhecimento facial, contudo, este seria para classificar o indivíduo em categorias amplas, por exemplo, idade, sexo, cor da roupa etc, não sendo necessário passar por um subprocesso de registro (item v).

Conforme o InternetLab, para melhores esclarecimentos, a identificação é um procedimento que ocorre a partir de uma base de dados de imagens de pessoas com identidades conhecidas (galeria). Então, o algoritmo realiza a comparação de uma nova imagem apresentada

[73] SIMÃO; FRAGOSO; ROBERTO, op. cit., p. 25.

com a galeria (comparação de um para muitos) e produz uma lista classificatória de semelhança com os possíveis candidatos da galeria. A verificação, por sua vez, é um procedimento de comparação entre duas imagens dadas e conhecidas (comparação de um para um), por exemplo, entre a imagem contida em um documento apresentado por uma pessoa e a imagem tirada dela no mesmo momento da apresentação do documento. Assim, o algoritmo decide se as imagens são da mesma pessoa ou não, como acontece em uma verificação de passaporte ou em aplicativos que verificam se o usuário remoto é quem ele diz ser[74].

Nos três casos as imagens capturadas são transformadas em representações numéricas para que seja possível a execução de qualquer uma das duas tarefas, ou seja, existe nesses casos o tratamento[75] dos dados pessoais de biometria. Nesse momento é importante destacar que, independentemente do objetivo da máquina, ou do que se faça com as informações após a extração de atributos (item iv), seja o descarte ou armazenamento, a mera leitura da imagem para detecção facial basta para se dizer que houve o tratamento de rostos de um ou mais indivíduos. As repercussões conceituais, legais e práticas serão discutidas em momento oportuno desta pesquisa.

De forma semelhante ao Grupo de Trabalho do Artigo 29, o parecer técnico desenvolvido pelo InternetLab expressou sete passos[76] a serem realizados para que um sistema realize o reconhecimento facial, sendo eles: (i) 1º passo: captura da imagem por uma câmera digital com qualidade para capturar detalhes da face; (ii) 2º passo: um sistema de detecção é acionado; (iii) 3º passo: filtragem da imagem para avaliação da qualidade; (iv) 4º passo: localização da face na imagem (procurar pixel a pixel partes que se parecem com face humana); (v) 5º passo: localização de características (processo de modelagem 3D da face através de estimação e triangulação) para colocar a rotação da face alinhada em perspectiva frontal e escalar a imagem em tamanho requerido pelo sistema; (vi) 6º passo: classificação de acordo com gênero, idade, etnia etc, ou reconhecimento de faces através da identificação (dizer de quem é aquele rosto a partir da similaridade comparada com um conjunto de imagens de faces) ou da verificação (confirmar a identidade da pessoa com um documento, por exemplo); e (vii) 7° passo: avaliação humana (avaliação se corresponde a mesma pessoa ou não).

---

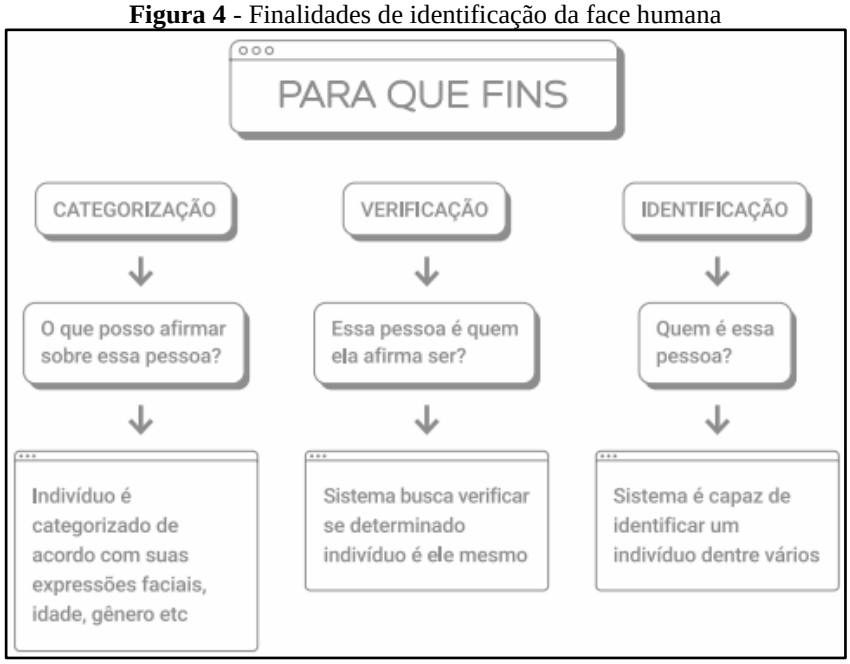
[74] ABELLO; ARAÚJO; HIRATA JR., op.cit., p. 24.

[75] Conceito da Lei Geral de Proteção de Dados (LGPD): Art. 5º, X - "tratamento: toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração;" BRASIL. Lei n. 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). **Diário Oficial da União**, Poder Executivo, Brasília, DF, 14 ago. 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709compilado.htm. Acesso em: 18 jan. 2023.

[76] ABELLO; ARAÚJO; HIRATA JR., op. cit., p. 6-8.

Assim como o Artigo 29, o parecer do InternetLab também destaca que, após esses passos, a sistemática de detecção de faces permite a execução de diferentes tarefas (objetivos), sendo as mais comuns (a) a categorização, (b) a verificação e (c) a identificação, conforme apontado no 6º passo.

Figura 4 - Finalidades de identificação da face humana



Fonte: Reconhecimento Facial e o Setor Privado: Guia para a adoção de boas práticas. InternetLab/IDEC, 2020[77].

Enquanto a primeira tarefa irá extrair características da imagem do indivíduo para categorizá-lo conforme seu humor, idade, gênero etc, as duas últimas tarefas, em sua essência, vão apontar quão próximas, ou distantes, duas imagens de rostos são uma da outra[78]. É possível compreender, de forma didática, as finalidades desses processos mapeadas na Figura 4 acima.

Cada objetivo da máquina terá diferentes utilidades comerciais. No caso, a categorização de indivíduos tem sido aplicada para rotulagem de emoções baseada nas características que a face humana apresenta conforme a expressão de reações. Os potenciais campos de aplicação do reconhecimento de emoções faciais (*Face Emotion Recognition* - FER) variam entre publicidade, saúde, emprego, educação, segurança pública, detecção de crimes, serviços personalizados, entre outros. As possibilidades são diversificadas, por exemplo, na área da publicidade, as emoções dos clientes são analisadas durante as compras com foco nas

[77] SIMÃO; FRAGOSO; ROBERTO, op.cit., p. 7.
[78] Ibid., p. 24.

mercadorias ou em sua disposição na loja, enquanto que, na área da saúde, as condições dos pacientes podem ser acompanhadas durante um tratamento[79].

De modo geral, a categorização é basicamente empregada para reconhecer "(i) estados psicológicos (emoções básicas, orientação da cabeça e dos olhos), (ii) características sociodemográficas (gênero, idade, etnia) e (iii) reações dos clientes à loja (quantidade de tempo despendido na loja ou com determinado produto (...) etc.)"[80].

A seu turno, a verificação é bastante comum em cadastros em aplicativos bancários ou de documentos digitais e também em desbloqueio de tela de celulares em substituição a uma senha. Diferente do processo anterior, neste o indivíduo participa do processo e está ciente do porquê seus dados são usados.

Por fim, o uso da identificação por meio do reconhecimento facial ocorre, por exemplo, em câmeras de vídeo vigilância instaladas nos ambientes monitorados e nos embarques de passageiros nos aeroportos. Outro exemplo de aplicação bastante conhecida são as tags de identificação automática em fotos sugeridas aos usuários de redes sociais.

Geralmente, a identificação e a categorização não são direcionadas para pessoas específicas, já que possuem a capacidade de extrair dados, inclusive biométricos, de todos aqueles que forem alcançados pela câmera de forma automática e indiscriminada. Nestes processos, a coleta de dados é em tempo real e em larga escala, muitas vezes sem a consciência, escolha ou controle dos indivíduos[81].

A diferenciação entre os objetivos dos sistemas de reconhecimento facial feita acima é necessária e importante para esclarecer os processos de funcionamento e de uso dessa tecnologia, bem como para entender a participação dos indivíduos em cada situação - se informados ou não e qual a qualidade e eficiência da informação -, o que é extremamente relevante para a análise de proteção de dados pessoais pretendida pelo trabalho.

1.4 PREMISSAS: ALGUMAS IMPLICAÇÕES DOS SISTEMAS DE DETECÇÃO E RECONHECIMENTO DE FACES EM RELAÇÃO AO USO DE DADOS PESSOAIS

[79] VEMOU, Konstantina; HORVATH, Anna; ZERDICK, Thomas (ed.). EDPS TechDispatch: facial emotion recognition. Issue 1, 2021. **Publications Office of the European Union**, 2012. Disponível em: https://data.europa.eu/doi/10.2804/014217. Acesso em: 2 fev. 2023. p. 2.
[80] SIMÃO; FRAGOSO; ROBERTO, op.cit., p. 32.
[81] INFORMATION COMMISSIONER'S OFFICE. Information Commissioner's Opinion: The use of live facial recognition technology in public places. **Information Commissioner's Office (ico.)**, 2021. Disponível em: https://ico.org.uk/media/2619985/ico-opinion-the-use-of-lfr-in-public-places-20210618.pdf. Acesso em: 2 fev. 2023. p. 4.

Feitas as considerações sobre o que é um sistema de reconhecimento facial, como sucede o passo a passo para seu funcionamento e quais são os seus principais objetivos presentes na sua abordagem, parte-se, neste ponto, para assimilar algumas implicações decorrentes disso.

Em um primeiro momento, cabe destacar que as implicações aqui descritas não buscam exaurir as possibilidades, mas procuram somente alcançar aquelas ideias que servirão como base para o pensamento e raciocínio do objetivo principal desta pesquisa. As premissas serão pontos de partida para a proposição de condutas adequadas que possam orientar o uso e oferta consciente e responsável pelo setor privado de produtos e serviços com base em tecnologias de reconhecimento facial.

Portanto, considerando o exposto até aqui, é possível estabelecer a primeira premissa de que **(i)** nem todas as câmeras possuem *softwares* de detecção facial, bem como a mera captura de rostos por câmeras, como em filmagens ou fotografias, não constitui um dispositivo de reconhecimento facial. Entretanto **(ii)** toda câmera com tecnologia capacitada para detectar e reconhecer um rosto humano e dele extrair informações biométricas será considerada como um sistema de reconhecimento facial. "Ainda que o objetivo final da tecnologia não seja a identificação de uma pessoa determinada, para que a detecção aconteça, é necessário coletar e tratar dados de rostos humanos, ocorrendo um processo de leitura dos atributos e pontos de referência de uma face"[82].

Apesar da separação de definição entre o que se entende como tecnologia de reconhecimento facial ou não, ainda que o objetivo final de uma câmera com *software* de visão computacional não seja extrair informações a partir do rosto de alguém, **(iii)** para que a detecção facial aconteça, é preciso o treinamento do *software*, ou seja, é necessária a manipulação de um enorme conjunto de dados de características físicas de rostos humanos para o aprendizado de máquina.

Além disso, admite-se que **(vi)** dados referentes a rostos humanos são dados pessoais, uma vez que é uma informação relacionada a uma pessoa natural identificada ou identificável, nos termos do Artigo 5º, inciso I, da Lei Geral de Proteção de Dados (LGPD)[83], a ser melhor explorado posteriormente.

Consequentemente, **(v)** é impossível pensar em detecção facial e em reconhecimento facial sem pressupor operações realizadas com dados pessoais. Independente do objetivo que

---

[82] SIMÃO; FRAGOSO; ROBERTO, op.cit., p. 7.

[83] Artigo 5º, inciso I: "dado pessoal: informação relacionada a pessoa natural identificada ou identificável". BRASIL. Lei n. 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). **Diário Oficial da União**, Poder Executivo, Brasília, DF, 14 ago. 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709compilado.htm. Acesso em: 12 jan. 2023.

se queira chegar com o emprego dessa tecnologia, seja para uma simples detecção de um rosto humano na imagem[84] ou seja para categorização, verificação ou identificação de um indivíduo, afirmar-se que esses sistemas necessariamente operacionalizam dados pessoais, tanto no momento da coleta da imagem do indivíduo que se posiciona ou passa em frente à câmera que integra a tecnologia (primeira etapa do funcionamento) quanto em momento prévio, ou seja, no treinamento do *software* com conjuntos de dados, que também compõe a tecnologia, o que possibilita a detecção de um rosto na imagem apresentada na câmera (segunda etapa) e as demais etapas que se sucedem até o objetivo final. A distinção entre esses dois momentos de uso de imagens de pessoas é importante para, ao longo do texto, compreender os diferentes problemas que surgem.

Ademais, com base nos objetivos anteriormente estabelecidos para o funcionamento do reconhecimento facial, como classificação, verificação e identificação, constata-se que, **(vi)** para se chegar a qualquer uma dessas finalidades, ocorre a extração de características faciais exclusivas de cada um dos indivíduos, isto é, existe a intenção de capturar atributos pessoais únicos de cada um. Constata-se que o mesmo não pode ser referido para a simples detecção de faces em imagens.

Nesse sentido, **(vii)** a depender do tipo de dado pessoal auferido pelo *software* de reconhecimento facial, pode-se afirmar que são realizadas operações com dados pessoais de natureza sensível. Isso ocorre quando o propósito de existência e utilização do dispositivo seja obter de uma pessoa seus dados correspondentes 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", que são tipos de dados definidos como sensíveis pelo Artigo 5º, inciso II, da LGPD[85]. A partir do momento em que um sistema de reconhecimento facial analisa pontos de referência de uma face e com base neles faz inferências sobre características pessoais para classificação de gênero e origem racial ou para a extração da biometria, conclui-se que há o tratamento de dados pessoais sensíveis.

A busca, nesta pesquisa, pela estruturação de medidas destinadas ao setor privado para o desenvolvimento e implementação responsável das tecnologias de reconhecimento facial, em

[84] Por exemplo, dispositivo de localização de um rosto humano em imagens para câmeras de celulares que capturam fotos pela detecção de um sorriso, ou então que capturam retratos criando profundidade mantendo nítida a pessoa detectada e desfocando o fundo.

[85] Artigo 5º, inciso II: "dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural;" BRASIL. Lei n. 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). **Diário Oficial da União**, Poder Executivo, Brasília, DF, 14 ago. 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709compilado.htm. Acesso em: 12 jan. 2023.

especial para a proteção dos dados pessoais sensíveis, depende das premissas apresentadas neste tópico. Isso porque as medidas estarão relacionadas, em suma, com (a) a extração da biometria dos indivíduos pelos sistemas de reconhecimento facial e com (b) o enquadramento dos dados biométricos como dados pessoais biométricos sensíveis, conforme recorte deste estudo. Portanto, estabelecidas as premissas, parte-se para a identificação dos problemas que as tecnologias de reconhecimento facial suscitam e que demandam atenção e reflexão.

1.5 CONSEQUÊNCIAS SOCIAIS E OS RISCOS DA TECNOLOGIA DE RECONHECIMENTO FACIAL

Os sistemas de reconhecimento facial têm recebido grande atenção de autoridades públicas, pesquisadores e organizações da sociedade civil nos últimos anos. O aumento significativo de casos de implementação dessa tecnologia em múltiplos setores da vida despertou preocupações em razão das consequências problemáticas que ela acarreta.

Apesar da modernidade e benefícios que o reconhecimento facial pode proporcionar para a experiência humana, a realidade tem mostrado outro ponto de vista originado pelo seu emprego irresponsável e em desconformidade com os direitos fundamentais. Alguns fatos noticiados pela grande mídia evidenciam que o uso de *softwares* de reconhecimento facial apresenta questões bastante preocupantes por propiciar um perigoso controle social de vigilância em massa e por reforçar comportamentos discriminatórios através de resultados imprecisos e enviesados, que ocasionaram constrangimentos, prisões arbitrárias e violações aos direitos humanos[86].

A disseminação das tecnologias de reconhecimento facial, como mencionado no início do tópico, parecem ser inevitáveis e, diante disso, alguns problemas que se apresentam devem ser destacados para conscientização, não apenas por quem é afetado, mas também pelo setor privado que desenvolve esses recursos e os oferece como produtos e serviços.

É necessário considerar que, por trás dos problemas experienciados pela sociedade, existem discussões éticas em torno da justificativa e pertinência do uso de sistemas de reconhecimento facial. As reflexões referem-se tanto ao estado de desenvolvimento e

[86] OLHAR DIGITAL. Mulher é detida no Rio por erro em câmera de reconhecimento facial. **Olhar Digital**, 10 jul. 2019. Disponível em: https://olhardigital.com.br/2019/07/10/seguranca/mulher-e-detida-no-rio-por-erro-em-camera-de-reconhecimento-facial/. Acesso em: 9 jan. 2023.; O PANÓPTICO. Levantamento revela que 90,5% dos presos por monitoramento facial no Brasil são negros. **O Panóptico**, 21 nov. 2019. Disponível em: https://opanoptico.com.br/exclusivo-levantamento-revela-que-905-dos-presos-por-monitoramento-facial-no-brasil-sao-negros/. Acesso em 9 jan. 2023.

confiabilidade da tecnologia quanto às implicações sociais que ela reforça. O Doutor David Leslie destaca que foram deixadas de lado as preocupações com os efeitos transformadores que esses sistemas causam sobre o indivíduo em desenvolvimento, sobre a democracia, a coesão social, a intimidade das pessoas e o bem-estar individual e coletivo.

> No seu desenvolvimento não foram consideradas as indagações como "deveríamos estar fazendo isso?", "essas tecnologias são eticamente admissíveis dada as consequências a curto e longo prazo?", "os tecnólogos estão em um terreno ético sólido ao encher a sociedade, qualquer que seja o custo, com essas capacidades em expansão para automatizar globalmente a identificação pessoal ilimitada e a vigilância inteligente e onipresente?"[87] (tradução nossa).

A ética é uma disciplina acadêmica e uma subdivisão da filosofia, que "trata de questões como "O que é uma boa ação?", "Qual é o valor de uma vida humana?", "O que é justiça?", ou "O que é uma vida boa?""[88]. A ética aplicada é um dos grandes campos de pesquisa explorado nessa disciplina e se refere "ao que somos obrigados (ou autorizados) a fazer numa situação específica (muitas vezes historicamente nova) ou num determinado domínio (muitas vezes sem precedentes históricos) de possibilidades de ação"[89]. As questões éticas levantadas pelo desenvolvimento e implementação de inteligência artificial são um bom exemplo de ética aplicada. Nesse sentido:

> A ética aplicada trata de situações da vida real, em que as decisões têm de ser tomadas sob pressão do tempo e muitas vezes com uma racionalidade limitada. A ética da IA é geralmente encarada como um exemplo de ética aplicada e centra-se nas questões normativas suscitadas pela conceção, pelo desenvolvimento, pela implantação e pela utilização da inteligência artificial[90].

Segundo entendimento da Comissão Europeia, publicado no documento de "Orientações Éticas para uma IA de Confiança", produzido por um independente Grupo de Peritos de Alto Nível em Inteligência Artificial (GEPAN IA ou, em inglês, AI HLEG)[91], para garantir que os sistemas de IA sejam desenvolvidos, implantados e usados de maneira confiável, deverão seguir e respeitar princípios éticos pautados em direitos fundamentais, como (i) respeito à autonomia humana (*respect for human autonomy*); (ii) prevenção de danos

[87] LESLIE, op.cit., p. 9.
[88] COMISSÃO EUROPEIA. Orientações éticas para uma IA de confiança. **Comissão Europeia**, 2019. Disponível em: https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai. Acesso em: 25 jan. 2023. p. 48.
[89] Ibidem, p.48
[90] Ibidem.
[91] Conheça o Grupo de Especialistas de Alto Nível em Inteligência Artificial (*High-level expert group on artificial intelligence - AI HLEG*) em: https://digital-strategy.ec.europa.eu/en/policies/expert-group-ai.

(*prevention of harm*); (iii) equidade (*fairness*) e (iv) explicabilidade (*explicability*). O guia deixa claro que, embora muitos princípios éticos já estejam refletidos em obrigações legais, a adesão a esses princípios vai além da conformidade com as leis existentes[92].

De acordo com os princípios éticos, as tecnologias de reconhecimento facial, sendo um tipo de inteligência artificial, devem ser projetadas com foco no ser humano para garantir a oportunidade de escolha humana, o que consiste em assegurar a supervisão do homem sobre esses sistemas. Além disso, elas devem evitar a ocorrência ou intensificação de danos e não devem afetar desfavoravelmente o ser humano, o que significa que os ambientes em que operam necessitam ser protegidos e seguros, assim como que a tecnologia não seja aberta a usos maliciosos, dê maior atenção e proteção aos grupos mais vulneráveis e não permita assimetrias de poder ou de informação (isto é, entre empregadores e empregados, empresas e consumidores ou governos e cidadãos)[93].

Em respeito ao princípio da equidade, os sistemas de reconhecimento facial devem manifestar senso de justiça, ou seja, seguir o compromisso de garantir igual distribuição em benefícios e custos e de impedir preconceitos, discriminações e rotulações, enquanto que os profissionais devem equilibrar interesses e objetivos. O senso de justiça também engloba a possibilidade de contestação e reparação contra decisões tomadas por esses sistemas e pelos humanos que os operam, de modo que, para isso, deve haver a identificação de uma entidade responsável pela decisão[94].

Por último, pelo princípio da explicabilidade, os processos precisam ser transparentes e os recursos e objetivos dos sistemas devem ser comunicados abertamente, ao passo que as decisões, considerando as possibilidades de cada caso, necessitam ser explicáveis aos afetados[95].

Segundo a Comissão Europeia, os princípios éticos podem conflitar entre si, sem que exista uma solução definida para os casos. Por exemplo, o princípio da prevenção de danos colide com o princípio da autonomia quando o reconhecimento facial é empregado com a intenção de reduzir a criminalidade, mas, para isso, acaba recorrendo à vigilância e, portanto, afeta a liberdade e a privacidade dos indivíduos. Embora os princípios éticos sejam orientações abstratas, sem que exista uma solução correta, os profissionais desenvolvedores e aplicadores dessa tecnologia não podem agir aleatoriamente ignorando qualquer discrição, o que demanda

[92] COMISSÃO EUROPEIA. op.cit., p. 14.
[93] Ibidem, p. 14-15.
[94] Ibidem, p. 15.
[95] Ibidem, p. 15-16.

reflexão e a abordagem de dilemas éticos. Também é importante considerar que em alguns casos não haverá compensação ética aceitável, como é o caso do princípio da dignidade da pessoa humana[96] de inegável valor supremo[97].

O progresso das tecnologias biométricas tem desconsiderado preceitos éticos e consequentemente causado violações a direitos humanos básicos para alguns, a custo de lucro e conveniência de outros. O Doutor David Leslie, do Instituto Alan Turing, citado anteriormente, em seus estudos sobre preconceito e discriminação envolvendo esse tipo de tecnologia, afirmou que "desde as primeiras inovações em detecção facial baseada em dados no início dos anos 2000 até as arquiteturas de redes neurais convolucionais que alimentam o reconhecimento facial hoje, o viés e a discriminação têm sido tanto parte do desenvolvimento e uso dessas tecnologias quanto os pixels, parâmetros e dados"[98].

O Doutor Leslie explica sua afirmação trazendo três considerações. A primeira aponta que os conjuntos de dados utilizados para treinamento dessas tecnologias são desproporcionais quando se trata de representação de grupos demográficos marginalizados e, até pouco tempo, eram super representativos de homens brancos e sub-representativos de pessoas negras e mulheres. Além disso, a discriminação promovida pelas tecnologias de reconhecimento facial também surgiu da rotulagem de conjuntos de dados "onde categorias de "raça", "etnia" e "gênero" são instáveis e refletem normas culturais e categorizações subjetivas que podem levar a formas de racismo e preconceito científico"[99]. O terceiro fator considerado por ele é a questão técnica, que faz com que o desempenho seja diferente para grupos dominantes em relação aos subordinados[100].

Em confirmação, os estudos desenvolvidos pelo Instituto Nacional de Padrões e Tecnologia (NIST)[101], nos Estados Unidos (EUA), apontam que os sistemas de reconhecimento

---

[96] No Brasil, o Princípio da dignidade da pessoa humana está previsto no Artigo 1º, inciso III, da Constituição Federal de 1988. BRASIL. Constituição da República Federativa do Brasil, de 5 de outubro de 1988. **Diário Oficial da União**, Poder Legislativo, Brasília, DF, 5 out. 1988. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/ConstituicaoCompilado.htm. Acesso em: 30 jan. 2023.

[97] COMISSÃO EUROPEIA. **Orientações éticas para uma IA de confiança.** op.cit., p. 16.

[98] No original: "Throughout the evolution of FDRTs, from the very first innovations in data-driven facial detection in the early 2000s to the churning architectures of the convolutional neural networks that power facial recognition today, bias and discrimination have been as much a part of the development and use of these technologies as pixels, parameters and data have." LESLIE, op.cit., p. 5.

[99] No original: "Such an entrenchment of systemic discrimination has also cropped up in the labelling and annotating of datasets where categories of "race," "ethnicity," and "gender" are unstable and reflect cultural norms and subjective categorisations that can lead to forms of scientific racism and prejudice." Ibidem, p. 6.

[100] Ibidem, p. 6.

[101] "O estudo foi conduzido por meio do programa Face Recognition Vendor Test (FRVT) do NIST, que avalia algoritmos de reconhecimento facial, enviados por desenvolvedores da indústria e acadêmicos, em sua capacidade de executar tarefas diferentes. Embora o NIST não teste os produtos comerciais finalizados que fazem uso desses algoritmos, o programa revelou rápidos desenvolvimentos no campo florescente. O estudo do NIST avaliou 189 algoritmos de software de 99 desenvolvedores – a maioria da indústria" (tradução nossa). NATIONAL

facial funcionam de maneira diferente conforme o grupo demográfico, de modo que revelaram diferenças de precisão entre gênero, idade e grupos raciais, sendo que os mais altos índices de imprecisão nos resultados de identificação ocorrem em populações historicamente marginalizadas e não dominantes.[102] Esses resultados confirmam que vieses raciais e de gênero são largamente usados em sistemas de reconhecimento facial.

De modo geral, a precisão dessas ferramentas para identificação de pessoas de diferentes sexos, idades e origens raciais depende do algoritmo e do conjunto de dados utilizado para seu treinamento. Portanto, um algoritmo treinado a partir de conjunto de dados que contenha vieses raciais e de gênero vai gerar resultados imprecisos e perpetuar padrões racistas e discriminatórios, o que consiste em violação a direitos humanos fundamentais.

Essas constatações são verificáveis, por exemplo, a partir de duas classes de erros presentes nos resultados, que são os falsos positivos e os falsos negativos. Em um resultado falso positivo o sistema entende que dois indivíduos diferentes são a mesma pessoa, enquanto que em um falso negativo o sistema deixa de reconhecer que duas imagens se referem a mesma pessoa. A depender do erro e do objetivo para o qual o *software* é utilizado, as consequências são diferentes. Por exemplo, quando um sistema é mais propenso a gerar falsos positivos ao analisar pessoas negras do que ao analisar pessoas brancas, isso comprova a discriminação de um algoritmo enviesado e, em um contexto de vigilância policial para identificação de investigados por crimes, pode também ferir a presunção de inocência[103].

Ainda, no contexto da segurança pública, as tecnologias biométricas faciais também colocam em risco as liberdades constitucionais de expressão, reunião e associação[104], previstas no Artigo 5º, incisos IV, XVI e XVII, da Constituição Federal de 1988, isso porque, uma pessoa que sabe que é vigiada não se sente totalmente livre para expressar-se e comportar-se plenamente, assim como pode ficar receosa de participar de manifestações políticas. A

INSTITUTE OF STANDARDS AND TECHNOLOGY. **NIST Study Evaluates Effects of Race, Age, Sex on Face Recognition Software**. NIST, 2019. Disponível em: https://www.nist.gov/news-events/news/2019/12/nist-study-evaluates-effects-race-age-sex-face-recognition-software. Acesso em: 27 jan. 2023.

[102] GROTHER, Patrick; NGAN, Mei; HANAOKA Kayee. Face Recognition Vendor Test (FRVT) Part 3: Demographic effects. **National Institute of Standards and Technology**, Tech. Rep. NISTIR 8280, 2019. Disponível em: https://doi.org/10.6028/NIST.IR.8280. Acesso em: 27 jan. 2023.

[103] Artigo 5º, inciso LVII, da Constituição Federal de 1988: "ninguém será considerado culpado até o trânsito em julgado de sentença penal condenatória". BRASIL. Constituição da República Federativa do Brasil, de 5 de outubro de 1988, op. cit.

[104] Artigo 5º, incisos IV, XVI e XVII, da Constituição Federal de 1988: "IV - é livre a manifestação do pensamento, sendo vedado o anonimato", "XVI - todos podem reunir-se pacificamente, sem armas, em locais abertos ao público, independentemente de autorização, desde que não frustrem outra reunião anteriormente convocada para o mesmo local, sendo apenas exigido prévio aviso à autoridade competente" e "XVII - é plena a liberdade de associação para fins lícitos, vedada a de caráter paramilitar". BRASIL. Constituição da República Federativa do Brasil, de 5 de outubro de 1988, op. cit.

democracia sempre esteve condicionada à liberdade de movimento sem constante monitoramento governamental, considerando a habilidade dos indivíduos de se reunirem, interagirem e debaterem seus posicionamentos tanto em âmbito público quanto privado.

De qualquer forma, o reconhecimento facial ocasiona maior vigilância e amplo acesso a dados das pessoas por meio da coleta de imagens, da biometria e de outros dados que possam ser inferidos, como de gênero, idade, origem racial, humor e localização. O acesso a essas informações por entes públicos ou privados pode acarretar violações à privacidade, tanto em sentido estrito quanto em suas novas concepções de violação de dados pessoais e de autodeterminação informativa. Isso porque normalmente a vigilância é massiva e compulsória, com pouca ou nenhuma transparência na implementação da tecnologia, de modo que não há respeito ao direito de cada indivíduo controlar e proteger seus dados pessoais. Além disso, poderia haver o vazamento da enorme quantidade de dados utilizados por essas tecnologias, deixando vulnerável todos que foram afetados por elas.

O avanço na implementação da tecnologia e os contextos de irregularidades têm levado a movimentações por organizações civis para requisição de regulamentação do reconhecimento facial e, em alguns casos, pela reivindicação de seu banimento parcial ou até completo, principalmente quando o objetivo é a identificação de indivíduos sob pretexto da segurança pública, como observa-se nas organizações "LAPIN"[105], "Artigo 19"[106], "Data Privacy Brasil"[107], "InternetLab"[108], "Idec"[109], entre outras que endossaram a campanha "#Tire Meu Rosto da Sua Mira"[110].

As preocupações não são apenas por parte da sociedade civil organizada, mas também por grandes empresas de tecnologia que compartilham a ideia da necessidade de regulamentação governamental e de medidas responsáveis a serem adotadas pela indústria para abordar o avanço da tecnologia de reconhecimento facial. Empresas como a Microsoft[111], a

[105] Conheça o Laboratório de Pesquisa em Políticas Públicas e Internet – LAPIN em: https://lapin.org.br/. Acesso em: 31 jan. 2023.
[106] Conheça o Artigo 19 em: https://artigo19.org/. Acesso em: 31 jan. 2023.
[107] Conheça o Data Privacy Brasil em: http://www.dataprivacybr.org/. Acesso em: 31 jan. 2023.
[108] Conheça o InternetLab em: https://internetlab.org.br/pt/. Acesso em: 31 jan. 2023.
[109] Conheça o Instituto Brasileiro de Defesa do Consumidor - Idec em: https://idec.org.br/. Acesso em: 31 jan. 2023.
[110] Conheça o Tire Meu Rosto da Sua Mira em: https://tiremeurostodasuamira.org.br/en/home-eng/. Acesso em: 31 jan. 2023.
[111] SMITH, Brad. Reconhecimento facial: é hora de agir. **Microsoft**, 2018. Disponível em: https://blogs.microsoft.com/on-the-issues/2018/12/06/facial-recognition-its-time-for-action/. Acesso em: 31 jan. 2023.

Meta[112] e a Amazon[113] estão cientes dos problemas decorrentes do uso de tecnologias de reconhecimento facial e defendem o seu desenvolvimento e aplicabilidade com cautela, sem, contudo, apoiarem o discurso de banimento, já que acreditam ser uma ferramenta poderosa para muitas situações e que, ao mesmo tempo, pode respeitar a diversidade, a privacidade, a transparência e o controle das pessoas sobre seus dados pessoais se for regulamentada.

De forma resumida e conforme o exposto até aqui, o presidente da Microsoft, Brad Smith, elencou três problemas causados pela tecnologia de reconhecimento facial que suscitam serem resolvidos pelos governos por meio de legislações: (i) os resultados tendenciosos e o consequente preconceito e discriminação; (ii) a invasão às liberdades democráticas pela vigilância em massa; e (iii) o uso generalizado e a violação à privacidade das pessoas[114].

Diante disso, em razão do caráter controvertido dessa tecnologia, o presente estudo, a seguir, será voltado para a investigação de legislações na União Europeia (UE), nos Estados Unidos (EUA) e no Brasil que regulamentam o seu uso e, portanto, o uso de dados biométricos faciais, com o objetivo de pesquisar e identificar medidas e salvaguardas que mitiguem ou eliminem os problemas decorrentes do emprego desses sistemas de identificação facial e que possam fornecer maiores certezas no seu uso pelo setor privado.

O primeiro tópico possibilitou a passagem por uma rápida digressão histórica de como as tecnologias evoluíram em um curto espaço de tempo e passaram a ser alimentadas por um grande volume de informações que foram transportadas do mundo real para o digital. De modo geral, as modernas tecnologias de informação e comunicação em conjunto com a massiva quantidade de dados digitalizados formaram um substrato para a criação e desenvolvimento das atuais ferramentas que detectam e reconhecem as faces humanas.

Após as considerações sobre o funcionamento da detecção de rostos pelas tecnologias, bem como sobre a definição, funcionamento e objetivos do reconhecimento facial em si, algumas premissas foram estabelecidas. Falou-se que somente é caracterizado como reconhecimento facial um sistema que seja capaz de detectar e identificar alguém e que assim o faça a partir da extração de características pessoais e da biometria, o que exclui as tecnologias que apenas capturam imagens faciais sem interpretá-las. Estabeleceu-se que os *softwares* que compõem essas tecnologias são treinados por amplo conjunto de dados de rostos humanos e

---

[112] PESENTI, Jerome. Uma atualização sobre nosso uso de reconhecimento facial. **Meta**, 2021. Disponível em: https://about.fb.com/news/2021/11/update-on-use-of-face-recognition/. Acesso em: 31 jan. 2023.
[113] AMAZON. Os fatos sobre a tecnologia de reconhecimento facial com inteligência artificial. **AWS**, c2023. Disponível em: https://aws.amazon.com/pt/rekognition/the-facts-on-facial-recognition-with-artificial-intelligence/. Acesso em: 30 abr. 2023.
[114] SMITH, op. cit.

que as câmeras que também compõe a tecnologia coletam imagens digitais de faces, o que implica que o reconhecimento facial operacionaliza dados pessoais, além de dados pessoais sensíveis ao extrair características das imagens para realizar a categorização, verificação ou identificação.

Por derradeiro, os próximos tópicos serão reservados para o conhecimento de legislações, nacionais e internacionais, destinadas à regulamentação de tecnologias de reconhecimento facial, que servirão como base para os parâmetros a serem adotados como melhores práticas na implementação dessas tecnologias pelas empresas.

2 A REGULAMENTAÇÃO JURÍDICA DA TECNOLOGIA DE RECONHECIMENTO FACIAL NA LEGISLAÇÃO ESTRANGEIRA: UNIÃO EUROPEIA E ESTADOS UNIDOS

Para este trabalho, o ponto principal na discussão sobre a utilização da tecnologia de reconhecimento facial é a proteção destinada aos dados biométricos faciais, justamente porque são informações compreendidas como diretamente atreladas à personalidade de um ser humano, que, se violadas ou usadas inadequadamente, afetam a sua identidade física, psíquica e moral, como o corpo, a privacidade, a liberdade, a honra, cuja proteção é constitucionalmente garantida em sociedades democráticas. Nas palavras de Chiara Teffé: "tutelar integralmente a dignidade da pessoa humana significa hoje, na sociedade da informação, proteger de forma ampla dados pessoais, permitindo que ela possa expressar sua autodeterminação informativa e não sofra discriminações ilícitas ou abusivas (...)"[115].

A proteção conferida especialmente aos dados pessoais por meio do ordenamento jurídico nacional e internacional não é recente. Embora a regulamentação específica sobre o tema esteja proliferando pelo mundo, principalmente após o GDPR do direito europeu de 2016, os dados pessoais sempre integraram a esfera de proteção necessária para a garantia do direito à privacidade[116] dos cidadãos, há tempos pertencente ao rol de direitos humanos. Ainda que exista a crença de que a tutela dos dados pessoais seja uma preocupação atual, na verdade foi o direito à privacidade que ganhou novos contornos em razão dos avanços tecnológicos, como um resgate ao respeito pelos direitos humanos[117].

---

[115] TEFFÉ, Chiara Spadaccini de. 49. Compliance de Dados em Tecnologias de Segurança e Vigilância. In: FRAZÃO, Ana; CUEVA, Ricardo Villas Bôas. **Compliance e Políticas de Proteção de Dados.** São Paulo: Editora Revista dos Tribunais, 2022. Disponível em: https://thomsonreuters.jusbrasil.com.br/doutrina/secao/1506551452/49-compliance-de-dados-em-tecnologias-de-seguranca-e-vigilancia-parte-v-topicos-especiais-de-compliance-e-politica-de-protecao-de-dados#ftn.DTR.2021.47943-n1. Acesso em 11 mar. 2023.

[116] Segundo o Artigo 5º da Constituição Federal brasileira, "(...) X - 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; XI - 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; XII - é 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; (...)". BRASIL. Constituição da República Federativa do Brasil, de 5 de outubro de 1988, op. cit.

[117] "Em maio de 2020, em julgamento histórico, o Supremo Tribunal Federal (STF) reconheceu a proteção de dados pessoais como um direito fundamental, simbolizando um grande avanço mediante a urgência que o tema demanda. (...) O acórdão dispõe que "a proteção de dados pessoais e a autodeterminação informativa são direitos fundamentais autônomos, que envolvem uma tutela jurídica e âmbito de incidência específicos". Além disso, deixa claro que o entendimento foi extraído da "interpretação integrada da garantia da inviolabilidade da intimidade e da vida privada (art. 5º, X), do princípio da dignidade da pessoa humana (art. 1º, III) e da garantia processual do habeas data (art. 5º, LXXII), todos previstos na Constituição Federal de 1988"". Ver mais em ADI 6387 MC-Ref, Relator(a): ROSA WEBER, Tribunal Pleno, julgado em 07/05/2020, PROCESSO ELETRÔNICO DJe-270 DIVULG 11-11-2020 PUBLIC 12-11-2020. BACCARIN, Cínthia; CANAVEZ, Luciana Lopes. Instrumentos de

A esfera de proteção jurídica conferida em específico aos dados pessoais ocorreu, pois, após inquietações despertadas em razão da utilização abusiva de dados pelas instituições, sem que as pessoas tivessem conhecimento sobre isso. Assim, na União Europeia (UE), foi levantada uma bandeira em defesa da retomada, na atual era tecnológica, dos direitos básicos dos seres humanos estabelecidos pela Organização das Nações Unidas (ONU) na Declaração Universal dos Direitos Humanos (DUDH) de 1948[118]. Com o objetivo de proteger a dignidade, a liberdade e a privacidade humana em risco com o progresso da tecnologia, a globalização e o comércio de informações, era preciso que as pessoas soubessem o que as empresas estavam fazendo com seus dados para que lhes fosse dada uma oportunidade de escolha[119].

Desde a década de noventa, a União Europeia já demonstrava preocupação com os maus usos de dados pessoais. Na época, foi editada a Diretiva 46/1995[120], que vigorou por mais de vinte anos e orientou os países integrantes a atuarem conforme regras sobre proteção de dados pessoais. Após amadurecimentos sobre o tema, em 2016, foi aprovado o GDPR, que entrou em vigor em maio de 2018. O GDPR "ocasionou um "efeito dominó", visto que passou a exigir que os demais países e as empresas que buscassem manter relações comerciais com a UE também deveriam ter uma legislação de mesmo nível que o GDPR"[121] para que não sofressem algum tipo de barreira comercial.

Atualmente, o mundo todo está se adaptando às exigências. Essa movimentação é possível de ser acompanhada através do site da Associação Internacional de Profissionais de Privacidade (*International Association of Privacy Professionals* - IAPP) que disponibiliza um mapa interativo e ilustrativo dos países que possuem leis de proteção de dados e suas respectivas autoridades fiscalizadoras[122].

Proteção de Direitos Fundamentais na Lei Geral de Proteção de Dados: a finalidade no tratamento de dados pessoais e a inversão na lógica da fiscalização. **Revista Pensamento Jurídico**, São Paulo, v. 16, nº 2, p. 272-299, maio/ago, 2022. Disponível em: https://fadisp.com.br/revista/ojs/index.php/pensamentojuridico/article/view/356. Acesso em: 11 mar. 2023.

[118] "Artigo 12° Ninguém sofrerá intromissões arbitrárias na sua vida privada, na sua família, no seu domicílio ou na sua correspondência, nem ataques à sua honra e reputação. Contra tais intromissões ou ataques toda a pessoa tem direito a proteção da lei." ORGANIZAÇÃO DAS NAÇÕES UNIDAS (ONU). **Declaração Universal dos Direitos Humanos**, 1948. Disponível em: https://brasil.un.org/pt-br/91601-declaracao-universal-dos-direitos-humanos. Acesso em: 11 mar. 2023.

[119] PINHEIRO, Patrícia Peck. **Proteção de dados pessoais:** comentários à Lei n. 13.709/2018 (LGPD). São Paulo: Saraiva Educação, 2018. p. 12.

[120] UNIÃO EUROPEIA. Directiva 95/46/CE do Parlamento Europeu e Conselho da União Europeia, de 24 de outubro de 1995. Relativa à protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados. **Jornal Oficial das Comunidades Europeias**, Parlamento Europeu e Conselho da União Europeia, Luxemburgo, 24 out. 1995. Disponível em: http://data.europa.eu/eli/dir/1995/46/oj. Acesso em: 11 mar. 2023.

[121] PINHEIRO, op.cit., p. 13.

[122] GLOBAL Privacy Law and DPA Directory. **International Association of Privacy Professionals (IAPP)**, c2023. Disponível em: https://iapp.org/resources/global-privacy-directory/. Acesso em: 13 mar. 2023.

O estabelecimento de novos parâmetros em proteção de dados, pois, desencadeou a necessidade de adequação das sociedades do mundo todo a esse novo modelo a partir da criação e implementação de novas normas, práticas e costumes em suas rotinas. Nesse sentido, principalmente as tecnologias avançadas de inteligência artificial, como o reconhecimento facial, passaram a ser alvo de maior preocupação, considerando suas particularidades complexas para a implementação de uma efetiva proteção aos dados pessoais e aos direitos humanos. Assim, além de leis sobre proteção de dados pessoais, alguns países estão adotando leis mais rigorosas para o uso da tecnologia de reconhecimento facial, o que ressalta a pertinência em analisá-las para identificar as diferentes abordagens e estratégias de regulação, proporcionando um cenário de reflexão, debate e auxílio para a utilização responsável dessa tecnologia.

A regulamentação jurídica das tecnologias de reconhecimento facial varia de acordo com o país e a região em que se encontram. No entanto, existem algumas tendências globais que podem ser observadas. Destacam-se, a seguir, algumas informações sobre as legislações sobre o assunto na União Europeia (UE) e nos Estados Unidos (EUA) para, posteriormente, seguir o estudo no Brasil.

2.1 A REGULAMENTAÇÃO JURÍDICA DAS TECNOLOGIAS DE RECONHECIMENTO FACIAL NA UNIÃO EUROPEIA

Na ordem jurídica da União Europeia[123], não há, até o momento, uma legislação específica que regulamente o desenvolvimento e uso das tecnologias de reconhecimento facial. Entretanto, regras relevantes que impõem limitações podem ser encontradas em diferentes níveis de regulamentação.

Nesse sentido, os membros da UE devem respeitar os Tratados e os princípios gerais, que ocupam a primeira posição na hierarquia das normas. A Carta de Direitos Humanos Fundamentais da UE (*Charter of Fundamental Rights* - CFR ou "Carta")[124] possui valor

[123] "A União Europeia tem personalidade jurídica e, como tal, a sua ordem jurídica própria, que é distinta do direito internacional. Além disso, o direito da UE tem um efeito direto ou indireto nas legislações dos Estados-Membros e torna-se parte integrante do sistema jurídico de cada Estado-Membro. A União Europeia é em si mesma uma fonte de direito. A ordem jurídica divide-se habitualmente em direito primário (os Tratados e os princípios jurídicos gerais), direito derivado (baseado nos Tratados) e direito complementar." BUX, Udo; MACIEJEWSKI, Mariusz. O ordenamento jurídico e os processos de tomada de decisão da União Europeia. **Parlamento Europeu**, jun. 2022. Disponível em: https://www.europarl.europa.eu/factsheets/pt/sheet/6/as-fontes-e-o-ambito-de-aplicacao-do-direito-da-uniao-europeia. Acesso em: 1º abr. 2023.

[124] MARZOCCHI, Ottavio. Proteção dos valores referidos no artigo 2.º do TUE na UE. **Parlamento Europeu**, maio de 2022. Disponível em: https://www.europarl.europa.eu/factsheets/pt/sheet/146/protecao-dos-valores-referidos-no-artigo-2.o-do-tue-na-ue. Acesso em: 1º abr. 2023.

idêntico aos Tratados e, embora represente um compromisso político, é um mecanismo de controle interno da UE que consagra um conjunto de garantias básicas primárias, onde estão previstos os direitos fundamentais à privacidade, à proteção de dados e à não driscriminação. Uma vez que o uso de tecnologias de reconhecimento facial implica na coleta e uso de dados pessoais biométricos faciais, então a sua utilização deve estar em conformidade com esses direitos fundamentais citados e previstos, respectivamente, nos arts. 7º, 8º e 21 do CFR[125], de forma que qualquer limitação desses direitos deve respeitar a necessidade e a proporcionalidade em relação a uma finalidade autorizada em lei (art. 52(1), CFR[126])[127].

Na prática, os direitos fundamentais dificilmente fornecem uma orientação para o uso das tecnologias de reconhecimento facial, diferentemente do que acontece com as regulamentações mais específicas. Na UE, tanto o Regulamento Geral de Proteção de Dados (GDPR)[128] quanto a Diretiva de *Law Enforcement* (LED)[129] são legislações que se aplicam às tecnologias de reconhecimento facial em vista que regulamentam os processos automatizados

[125] CFR, "Artigo 7.º Respeito pela vida privada e familiar. Todas as pessoas têm direito ao respeito pela sua vida privada e familiar, pelo seu domicílio e pelas suas comunicações."
CFR, "Artigo 8.º Proteção de dados pessoais. 1. Todas as pessoas têm direito à proteção dos dados de caráter pessoal que lhes digam respeito. 2. Esses dados devem ser objeto de um tratamento leal, para fins específicos e com o consentimento da pessoa interessada ou com outro fundamento legítimo previsto por lei. Todas as pessoas têm o direito de aceder aos dados coligidos que lhes digam respeito e de obter a respetiva retificação. 3. O cumprimento destas regras fica sujeito a fiscalização por parte de uma autoridade independente."
CFR, "Artigo 21.º Não discriminação. 1. É proibida a discriminação em razão, designadamente, do sexo, raça, cor ou origem étnica ou social, características genéticas, língua, religião ou convicções, opiniões políticas ou outras, pertença a uma minoria nacional, riqueza, nascimento, deficiência, idade ou orientação sexual. 2. No âmbito de aplicação dos Tratados e sem prejuízo das suas disposições específicas, é proibida toda a discriminação em razão da nacionalidade." UNIÃO EUROPEIA. Carta dos Direitos Fundamentais da União Europeia, de 26 de outubro de 2012. **Jornal Oficial da União Europeia**, 26 out. 2012. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX:12012P/TXT#document1. Acesso em: 25 mar. 2023.
[126] CFR, "Artigo 52.º Âmbito e interpretação dos direitos e dos princípios. 1. Qualquer restrição ao exercício dos direitos e liberdades reconhecidos pela presente Carta deve ser prevista por lei e respeitar o conteúdo essencial desses direitos e liberdades. Na observância do princípio da proporcionalidade, essas restrições só podem ser introduzidas se forem necessárias e corresponderem efetivamente a objetivos de interesse geral reconhecidos pela União, ou à necessidade de proteção dos direitos e liberdades de terceiros. [...]". Ibidem.
[127] MADIEGA, Tambiama; MILDEBRATH, Hendrik. Regulating facial recognition in the EU: in-depth analysis. **European Parliament**, Directorate-General for Parliamentary Research Services: Brussels, 2021. Disponível em: https://data.europa.eu/doi/10.2861/140928. Acesso em: 25 mar. 2023.
[128] UNIÃO EUROPEIA. Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016. Relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados). **Jornal Oficial da União Europeia:** Bruxelas, em 27 de abril de 2016. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX:32016R0679&qid=1679851495324#document1. Acesso em: 26 mar. 2023.
[129] UNIÃO EUROPEIA. Diretiva (UE) 2016/680 do Parlamento Europeu e do Conselho, de 27 de abril de 2016. Relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas autoridades competentes para efeitos de prevenção, investigação, deteção ou repressão de infrações penais ou execução de sanções penais, e à livre circulação desses dados e que revoga a Decisão-Quadro 2008/977/JAI do Conselho. **Jornal Oficial da União Europeia**: Bruxelas, 27 abr. 2016. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX:32016L0680. Acesso em: 26 mar. 2023.

de tratamento[130] de dados pessoais, o que inclui os dados biométricos, conforme art. 2(1), do GDPR e art. 2 da LED, que dispõem, respectivamente:

> Artigo 2.º
> Âmbito de aplicação material
> 1. O presente regulamento aplica-se ao tratamento de dados pessoais por meios total ou parcialmente automatizados, bem como ao tratamento por meios não automatizados de dados pessoais contidos em ficheiros ou a eles destinados[131].

> Artigo 2.º
> Âmbito de aplicação
> 1. A presente diretiva aplica-se ao tratamento de dados pessoais pelas autoridades competentes para os efeitos estabelecidos no artigo 1.º, n.º 1.
> 2. A presente diretiva aplica-se ao tratamento de dados pessoais por meios total ou parcialmente automatizados, bem como ao tratamento de dados pessoais contidos num ficheiro ou a ele destinados por meios não automatizados.
> 3. A presente diretiva não se aplica ao tratamento de dados pessoais:
> a) Efetuado no exercício de atividades não sujeitas à aplicação do direito da União;
> b) Efetuado pelas instituições, organismos, serviços e agências da União[132].

A LED, por ser estritamente aplicável às autoridades públicas nas situações em que utilizam dados pessoais para a prevenção, investigação, deteção e repressão de infrações penais, não será aprofundada neste estudo que se destina ao setor privado.

O GDPR, por sua vez, conforme art. 2º(2), somente não é aplicado, do ponto de vista material, quando o tratamento de dados pessoais for efetuado (i) no exercício de atividades não sujeitas à aplicação do direito da UE; (ii) pelos Estados-Membros no exercício de atividades no contexto de política externa e de segurança da UE; (iii) por uma pessoa singular no exercício de atividades exclusivamente pessoais ou domésticas; (iv) pelas autoridades competentes sujeitas à LED.

No âmbito de aplicação territorial (art. 3º), o GDPR é aplicado a todas as empresas e organizações que processam dados pessoais de cidadãos da UE, independentemente de onde estejam localizadas, o que inclui empresas estabelecidas na UE, bem como empresas não estabelecidas que oferecem bens ou serviços na UE ou que monitoram o comportamento de indivíduos que ali residem. Assim, a pesquisa dará enfoque para os mecanismos deste regulamento a respeito das decisões individuais automatizadas, incluindo definição de perfis, e

---

[130] Para o GDPR (art. 4º(2)), tratamento de dados pessoais é "uma operação ou um conjunto de operações efetuadas sobre dados pessoais ou sobre conjuntos de dados pessoais, por meios automatizados ou não automatizados, tais como a recolha, o registo, a organização, a estruturação, a conservação, a adaptação ou alteração, a recuperação, a consulta, a utilização, a divulgação por transmissão, difusão ou qualquer outra forma de disponibilização, a comparação ou interconexão, a limitação, o apagamento ou a destruição". UNIÃO EUROPEIA. Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, op.cit.

[131] Ibidem.

[132] UNIÃO EUROPEIA. Diretiva (UE) 2016/680 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, op. cit.

da proteção aos dados biométricos, que consequentemente devem guiar o uso das tecnologias de reconhecimento facial.

2.1.1 Tratamento de dados biométricos por decisões exclusivamente automatizadas

O GDPR, em seu art. 22º, aborda especificamente a respeito das "decisões individuais automatizadas, incluindo a definição de perfis" (*automated individual decision-making, including profiling*), nestes termos:

> Artigo 22.º
> Decisões individuais automatizadas, incluindo definição de perfis
> 1. O titular dos dados tem o direito de não ficar sujeito a nenhuma decisão tomada exclusivamente com base no tratamento automatizado, incluindo a definição de perfis, que produza efeitos na sua esfera jurídica ou que o afete significativamente de forma similar.
> 2. O n.º 1 não se aplica se a decisão:
> a) For necessária para a celebração ou a execução de um contrato entre o titular dos dados e um responsável pelo tratamento;
> b) For autorizada pelo direito da União ou do Estado-Membro a que o responsável pelo tratamento estiver sujeito, e na qual estejam igualmente previstas medidas adequadas para salvaguardar os direitos e liberdades e os legítimos interesses do titular dos dados; ou
> c) For baseada no consentimento explícito do titular dos dados.
> 3. Nos casos a que se referem o n.º 2, alíneas a) e c), o responsável pelo tratamento aplica medidas adequadas para salvaguardar os direitos e liberdades e legítimos interesses do titular dos dados, designadamente o direito de, pelo menos, obter intervenção humana por parte do responsável, manifestar o seu ponto de vista e contestar a decisão.
> 4. As decisões a que se refere o n.º 2 não se baseiam nas categorias especiais de dados pessoais a que se refere o artigo 9.º, n.º 1, a não ser que o n.º 2, alínea a) ou g), do mesmo artigo sejam aplicáveis e sejam aplicadas medidas adequadas para salvaguardar os direitos e liberdades e os legítimos interesses do titular[133].

De acordo com o *WP 251* do Artigo 29, "as decisões exclusivamente automatizadas correspondem à capacidade de tomar decisões através de meios tecnológicos e sem intervenção humana"[134], podendo basear-se em qualquer tipo de dados, como os fornecidos pela própria pessoa, os dados observados sobre alguém (por exemplo, localização) e dados obtidos ou inferidos a partir de um perfil (por exemplo, pontuação de crédito). Já a "definição de perfis" (*profiling*) encontra explicação no art. 4º(4) do GDPR, que dispõe ser:

---

[133] UNIÃO EUROPEIA. Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, op. cit.
[134] WORKING PARTY. Article 29. **Orientações sobre as decisões individuais automatizadas e a definição de perfis para efeitos do Regulamento (UE) 2016/679** (WP 251 rev.01). Bruxelas, 2017. Disponível em: https://ec.europa.eu/newsroom/article29/items/612053. Acesso em: 19 abr. 2023. p. 8.

> [...] qualquer forma de tratamento automatizado de dados pessoais que consista em utilizar esses dados pessoais para avaliar certos aspectos pessoais de uma pessoa singular, nomeadamente para analisar ou prever aspetos relacionados com o seu desempenho profissional, a sua situação econômica, saúde, preferências pessoais, interesses, fiabilidade, comportamento, localização ou deslocações; [...][135].

O documento de diretrizes *WP 251* do Artigo 29 ainda elucida que "as decisões automatizadas podem ser realizadas com ou sem definição de perfis; [assim como] a definição de perfis pode ocorrer sem serem realizadas decisões automatizadas"[136]. No entanto, ambas não são atividades necessariamente separadas, em razão de que um procedimento iniciado como um simples processo de decisão automatizada poderia passar a constituir uma definição de perfis, dependendo da forma de tratamento dos dados.[137] Além disso, "as decisões que não sejam exclusivamente automatizadas podem igualmente incluir a definição de perfis"[138].

Conforme visto anteriormente, as tecnologias de reconhecimento facial são projetadas para identificar rostos com base em características únicas (os dados biométricos), como a distância entre os olhos, o formato do nariz e das orelhas, entre outros. A partir dessas informações, a tecnologia pode ter como objetivo (i) classificar um indivíduo; ou (ii) comparar a imagem capturada com outra imagem apresentada no mesmo momento para verificar se são correspondentes; ou (iii) comparar a imagem capturada com um conjunto de dados de rostos já registrados em um banco de dados para identificar um indivíduo. Em vista disso, conforme o *WP 129* do Artigo 29, considera-se que essa tecnologia "depende de várias etapas de processamento automatizado [...]. Assim, o reconhecimento facial constitui uma forma automatizada de tratamento de dados pessoais, incluindo os dados biométricos"[139]. Independentemente do objetivo pelo qual o reconhecimento facial é utilizado, essa tecnologia é um meio para a tomada de decisões automatizadas, podendo ou não ter interferência humana.

---

[135] UNIÃO EUROPEIA. Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, op. cit.

[136] WORKING PARTY, op. cit., p. 8.

[137] Por exemplo, "a aplicação de coimas por excesso de velocidade com base exclusivamente em provas obtidas através de radares de velocidade constitui um processo de decisão automatizada que não implica necessariamente uma definição de perfis. No entanto, passaria a constituir uma decisão tomada com base na definição de perfis se os hábitos de condução da pessoa fossem controlados ao longo do tempo e, por exemplo, se o montante da coima aplicada resultasse de uma avaliação que tivesse em conta outros fatores, como a reincidência ou não do excesso de velocidade ou o facto de o condutor ter incorrido recentemente em infrações rodoviárias". Ibidem, p. 8.

[138] Por exemplo, "antes da concessão de um crédito hipotecário, um banco poderá tomar em consideração a pontuação de crédito do mutuário, com uma intervenção humana adicional e significativa antes de ser aplicada qualquer decisão a uma pessoa". Ibidem, p. 9.

[139] No texto original: "Facial recognition relies on a number of automated processing stages as previously described. Therefore, facial recognition constitutes an automated form of processing of personal data, including biometric data." WORKING PARTY. Article 29. **Parecer 02/2012 sobre reconhecimento facial em serviços online e móveis.** (WP 192). Bruxelas, 2012. Disponível em: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp192_en.pdf. Acesso em: 19 abr. 2023. p. 5.

A identificação e a verificação não acarretam uma definição de perfis, enquanto o mesmo não pode ser afirmado em relação à classificação. De acordo com o entendimento do *WP 251* do Artigo 29, "uma simples classificação de pessoas com base em características conhecidas, como a idade, o sexo e a altura, não acarreta necessariamente uma definição de perfis. Tal dependerá da finalidade da classificação"[140]. Por exemplo, a classificação de clientes de uma empresa em idade ou gênero para fins estatísticos, cujo objetivo seja a visão geral do conjunto de clientes, sem que exista a apreciação de características individuais, não se trata de uma definição de perfis. Entretanto, se a tecnologia de reconhecimento facial for usada em conjunto com outras informações, como nome, idade, endereço e outros dados pessoais, é possível a criação de um perfil detalhado de uma pessoa, podendo ser usado para rastrear as atividades particulares de um indivíduo, analisar suas preferências e comportamentos e criar um perfil de personalidade, por exemplo.

Nesse sentido, dentre as preocupações do GDPR, está a regulamentação da definição de perfis e das decisões individuais automatizadas, que podem ter um impacto injustificado nos direitos das pessoas. Por exemplo, se uma empresa usa a definição de perfis para tomar decisões sobre um indivíduo, como aprovar ou negar acesso a determinado local, sem permitir a chance de contestação da decisão, isso pode ser considerado uma violação dos direitos da pessoa. Para evitar violações como esta, o GDPR introduz disposições específicas para o tratamento de dados pessoais por decisões automatizadas, incluindo a definição de perfis, como:

> requisitos específicos de transparência e lealdade; obrigações acrescidas em matéria de responsabilidade; fundamentos jurídicos especificados para o tratamento; direitos das pessoas de oposição à definição de perfis e, concretamente, à definição de perfis para efeitos de comercialização; e, sob reserva do cumprimento de determinadas condições, a necessidade de proceder a uma avaliação de impacto sobre a proteção de dados[141].

O *WP 251* do Artigo 29 dispõe sobre orientações para aplicação das disposições do GDPR tanto para os processamentos de dados pessoais relacionados a (i) decisões individuais automatizadas, incluindo definição de perfis, em que os processos decisórios *não sejam exclusivamente automatizados* (possuem intervenção humana no processo decisório), quanto para os processamentos que envolvem (ii) as decisões tomadas *exclusivamente com base no tratamento automatizado* (não possuem intervenção humana no processo decisório). Essa

[140] WORKING PARTY. Article 29. **Orientações sobre as decisões individuais automatizadas e a definição de perfis para efeitos do Regulamento (UE) 2016/679**, op. cit., p. 7.
[141] WORKING PARTY. Article 29. **Orientações sobre as decisões individuais automatizadas e a definição de perfis para efeitos do Regulamento (UE) 2016/679**, op. cit., p. 6.

distinção foi feita em razão do segundo caso (item ii) possuir disposições específicas no GDPR a serem aplicadas[142].

Apesar dessa divisão didática, as disposições do GDPR sobre princípios (art. 5º), bases legais (arts. 6º e 9º) e direitos dos titulares de dados (arts. 13º ao 21º) aplicam-se a *todas* as decisões automatizadas, incluindo definição de perfis, com ou sem intervenção humana no processo decisório. Cada um desses artigos será explorado com maior profundidade no tópico seguinte em razão da importância, entretanto, cabe nesse momento elencar, de modo geral, quais são as obrigações a serem seguidas decorrentes dessas disposições.

As empresas responsáveis pelo tratamento de dados pessoais por meio de tecnologia de reconhecimento facial, com ou sem intervenção humana no processo decisório, para estarem em conformidade com as regras de privacidade e proteção de dados pessoais da UE, devem dar atenção aos seguintes requisitos essenciais: (i) o tratamento deve ser leal, transparente, lícito - fundamentado em uma base legal - e limitado a finalidades específicas; (ii) os dados pessoais devem ser adequados e necessários para cumprimento das finalidades, sempre exatos, atualizados e armazenados até atingir as finalidades; (iii) o tratamento deve ser seguro e adotar medidas técnicas para proteção dos dados pessoais contra tratamentos não autorizados ou ilícitos e contra qualquer perda, destruição ou danificação acidental; (iv) o tratamento de categorias especiais de dados pessoais (por exemplo, os dados biométricos) deve satisfazer uma das condições estabelecidas no art. 9º(2) do GDPR (licitude); (v) o responsável pelo tratamento tem a responsabilidade de comprovar sua adequação às disposições do GDPR; (vi) o responsável pelo tratamento deve garantir os direitos dos titulares dos dados, como o direito de serem informados sobre o tratamento dos seus dados, o direito de acesso aos dados sob tratamento, o direito de retificação desses dados, o direito ao apagamento, o direito à limitação do tratamento e o direito de oposição ao tratamento[143].

Com relação às decisões tomadas com base *exclusivamente* no tratamento automatizado, o art. 22º(1) do GDPR[144], estabelece uma proibição geral. Essa interpretação do art. 22º(1) como uma proibição, em vez de considerá-la um direito de titular de dados, segundo as orientações do *WP 251* do Artigo 29, é feita pela redação do próprio artigo em conjunto com o Considerando 71 do GDPR. Nesses termos:

---

[142] Ibidem, p. 9.

[143] WORKING PARTY. Article 29. **Orientações sobre as decisões individuais automatizadas e a definição de perfis para efeitos do Regulamento (UE) 2016/679,** op. cit., p. 10-20.

[144] GDPR, Art. 22.º: "1. O titular dos dados tem o direito de não ficar sujeito a nenhuma decisão tomada exclusivamente com base no tratamento automatizado, incluindo a definição de perfis, que produza efeitos na sua esfera jurídica ou que o afete significativamente de forma similar [...]". UNIÃO EUROPEIA. Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, op. cit.

> Esta interpretação reforça a ideia do controle do titular dos dados sobre os seus dados pessoais, o que obedece aos princípios fundamentais do RGPD. A interpretação do artigo 22.º como uma proibição, em vez de um direito que pode ser invocado, significa que as pessoas estão automaticamente protegidas dos possíveis efeitos deste tipo de tratamento. A redação do artigo deixa entender que é esse o objetivo, sendo apoiada pelo considerando 71, que refere o seguinte: ["]No entanto, a tomada de decisões com base nesse tratamento, incluindo a definição de perfis, deverá ser permitida se expressamente autorizada pelo direito da União ou dos Estados-Membros […], ou se for necessária para a celebração ou execução de um contrato […], ou mediante o consentimento explícito do titular["]. Assim, está implícito que o tratamento ao abrigo do artigo 22.º, n.º 1, não é, de modo geral, permitido[145].

Contudo, essa proibição aos tratamentos de dados pessoais ao abrigo do artigo 22º(1) do GDPR, aplica-se *especificamente* "quando uma decisão tomada exclusivamente com base no tratamento automatizado, incluindo a definição de perfis, produz efeitos jurídicos ou afeta alguém significativamente de forma similar"[146]. Os "efeitos jurídicos" podem relacionar-se, no sentido deste artigo da lei, com a interferência nos direitos de alguém, por exemplo, nos direitos de liberdade de associação, não discriminação e privacidade; ou podem verificar-se no contexto de um contrato afetado, como na recusa de concretização de um contrato. Todavia, ainda que o tratamento de dados pessoais por decisão exclusivamente automatizada, incluindo a definição de perfis, não produza efeitos jurídicos na esfera de direitos de um indivíduo, mas afete alguém "significativamente de forma similar", esse tratamento também estará proibido por força do art. 22º(1) do GDPR[147].

De acordo com o *WP 251* do Artigo 29, "para que um tratamento de dados afete significativamente alguém, os seus efeitos devem ser suficientemente grandes ou importantes para merecerem atenção"[148], por exemplo, "afetar significativamente as circunstâncias, o comportamento ou as escolhas das pessoas em causa; ter um impacto prolongado ou permanente no titular dos dados; ou nos casos mais extremos, dar origem a uma exclusão ou discriminação das pessoas"[149].

A tomada de decisões com base exclusivamente em tratamento automatizado apenas será permitida se for aplicável uma das exceções dispostas no art. 22º(2) do GDPR[150]:

> 2. O n.º 1 não se aplica se a decisão:

[145] WORKING PARTY. Article 29. **Orientações sobre as decisões individuais automatizadas e a definição de perfis para efeitos do Regulamento (UE) 2016/679**, op. cit., p. 22.
[146] Ibidem.
[147] Ibidem, p. 23-24.
[148] Ibidem, p. 24.
[149] Ibidem.
[150] Ver também o Considerando 71 do GDPR. UNIÃO EUROPEIA. Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, op. cit.

> a) For necessária para a celebração ou a execução de um contrato entre o titular dos dados e um responsável pelo tratamento;
> b) For autorizada pelo direito da União ou do Estado-Membro a que o responsável pelo tratamento estiver sujeito, e na qual estejam igualmente previstas medidas adequadas para salvaguardar os direitos e liberdades e os legítimos interesses do titular dos dados; ou
> c) For baseada no consentimento explícito do titular dos dados[151].

Ademais, o Considerando 71 e o art. 22º(3) do GDPR[152] dispõem que, independentemente da situação (a, b ou c), é imprescindível que haja medidas de proteção adequadas, incluindo informações claras e específicas para o titular dos dados que estão sendo tratados, incluindo o direito de obter intervenção humana, de expressar opinião, de receber explicações sobre decisões tomadas e de contestá-las.

Em resumo de todo o exposto até o momento:

> i) em regra, existe uma proibição geral das decisões individuais totalmente automatizadas, incluindo a definição de perfis com efeitos jurídicos ou similarmente significativos,
> ii) há exceções a essa regra;
> iii) sempre que se aplique uma dessas exceções, devem existir medidas para salvaguardar os direitos e liberdades e os legítimos interesses do titular dos dados[153].

Ressalta-se que o art. 22º não menciona qualquer distinção para o tratamento de dados pessoais de crianças[154]. Todavia, o Considerando 71 menciona que as decisões exclusivamente automatizadas, incluindo a definição de perfis, com efeitos jurídicos ou similarmente significativos não devem dizer respeito a crianças. O Artigo 29, em seu *WP 251*, considera que,

---

[151] Ibidem.
[152] Ibidem.
[153] WORKING PARTY. Article 29. **Orientações sobre as decisões individuais automatizadas e a definição de perfis para efeitos do Regulamento (UE) 2016/679**, op. cit., p. 21.
[154] GDPR, Considerando 38: "As crianças merecem proteção especial quanto aos seus dados pessoais, uma vez que podem estar menos cientes dos riscos, consequências e garantias em questão e dos seus direitos relacionados com o tratamento dos dados pessoais. Essa proteção específica deverá aplicar-se, nomeadamente, à utilização de dados pessoais de crianças para efeitos de comercialização ou de criação de perfis de personalidade ou de utilizador, bem como à recolha de dados pessoais em relação às crianças quando da utilização de serviços disponibilizados diretamente às crianças. O consentimento do titular das responsabilidades parentais não deverá ser necessário no contexto de serviços preventivos ou de aconselhamento oferecidos diretamente a uma criança." e GDPR, Art. 8º: "Condições aplicáveis ao consentimento de crianças em relação aos serviços da sociedade da informação 1. Quando for aplicável o artigo 6.º, n.º 1, alínea a), no que respeita à oferta direta de serviços da sociedade da informação às crianças, dos dados pessoais de crianças é lícito se elas tiverem pelo menos 16 anos. Caso a criança tenha menos de 16 anos, o tratamento só é lícito se e na medida em que o consentimento seja dado ou autorizado pelos titulares das responsabilidades parentais da criança. Os Estados-Membros podem dispor no seu direito uma idade inferior para os efeitos referidos, desde que essa idade não seja inferior a 13 anos. 2. Nesses casos, o responsável pelo tratamento envia todos os esforços adequados para verificar que o consentimento foi dado ou autorizado pelo titular das responsabilidades parentais da criança, tendo em conta a tecnologia disponível. 3. O disposto no n.o 1 não afeta o direito contratual geral dos Estados-Membros, como as disposições que regulam a validade, a formação ou os efeitos de um contrato em relação a uma criança." UNIÃO EUROPEIA. Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, op. cit.

como o entendimento do Considerando 71 não está previsto no texto do artigo, então "não representa uma proibição absoluta deste tipo de tratamento relativamente às crianças. Contudo, [...] recomenda que, regra geral, os responsáveis pelo tratamento não invoquem as exceções previstas no artigo 22.º, n.º 2, para justificar esse tratamento"[155].

O GDPR ainda determina que, sempre que a decisão estiver relacionada às categorias especiais de dados descritas no art. 9º(1), nas quais estão incluídos os dados biométricos, é obrigação do responsável pelo tratamento garantir que este esteja em conformidade com os requisitos estabelecidos no art. 22º(4)[156]. Isso quer dizer que as decisões a que se refere o art. 22º(2) - necessárias para execução de contrato; autorizadas pelo direito da União ou de Estado-Membro; ou baseadas no consentimento explícito do titular dos dados - somente poderão se referir a dados de categorias especiais se o tratamento estiver fundamentado em uma das hipóteses do art. 9(2)(a) ou (g) - consentimento explícito ou interesse público, respectivamente -, bem como, ao mesmo tempo, forem aplicadas medidas adequadas para salvaguardar os direitos e liberdades e os legítimos interesses do titular[157].

Em conclusão, uma decisão exclusivamente automatizada baseada em tratamento de dados biométricos somente é permitida pela lei de proteção de dados da UE se for contemplada por uma entre as seis hipóteses dispostas no Quadro 1 abaixo.

Quadro 1 - Hipóteses autorizadoras de decisões exclusivamente automatizadas baseadas em tratamento de categorias especiais de dados pessoais

Nº	**Artigo 22º(2)(a)(b) e (c) do GDPR** **(exceções à proibição geral das decisões individuais totalmente automatizadas, incluindo a definição de perfis com efeitos jurídicos ou similarmente significativos)**	**Artigo 9º(2)(a) e (g) do GDPR** **(exceções à proibição geral de tratamento de categorias especiais de dados pessoais)**
1	**(a)** A decisão exclusivamente automatizada for necessária para a celebração ou a execução de um contrato entre o titular dos dados e um responsável pelo tratamento; **+**	**(a)** Se o titular dos dados tiver dado o seu consentimento explícito para o tratamento de categorias especiais de dados pessoais para uma ou mais finalidades específicas, exceto se o direito da União ou de um Estado-Membro previr que a proibição geral a que se refere o n.º 1 do art. 9º não

[155] WORKING PARTY. Article 29. **Orientações sobre as decisões individuais automatizadas e a definição de perfis para efeitos do Regulamento (UE) 2016/679**, op. cit., p. 31.
[156] GDPR, Art. 22 (4): "As decisões a que se refere o n.º 2 não se baseiam nas categorias especiais de dados pessoais a que se refere o artigo 9.º, n.º 1, a não ser que o n.º 2, alínea a) ou g), do mesmo artigo sejam aplicáveis e sejam aplicadas medidas adequadas para salvaguardar os direitos e liberdades e os legítimos interesses do titular." UNIÃO EUROPEIA. Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, op. cit.
[157] Ibidem.

			pode ser anulada pelo titular dos dados;
2	**(a)** A decisão exclusivamente automatizada for necessária para a celebração ou a execução de um contrato entre o titular dos dados e um responsável pelo tratamento;	+	**(g)** Se o tratamento de categorias especiais de dados pessoais for necessário por motivos de interesse público importante, com base no direito da União ou de um Estado-Membro, que deve ser proporcional ao objetivo visado, respeitar a essência do direito à proteção dos dados pessoais e prever medidas adequadas e específicas que salvaguardem os direitos fundamentais e os interesses do titular dos dados;
3	**(b)** A decisão exclusivamente automatizada for autorizada pelo direito da União ou do Estado-Membro a que o responsável pelo tratamento estiver sujeito, e na qual estejam igualmente previstas medidas adequadas para salvaguardar os direitos e liberdades e os legítimos interesses do titular dos dados;	+	**(a)** Se o titular dos dados tiver dado o seu consentimento explícito para o tratamento de categorias especiais de dados pessoais para uma ou mais finalidades específicas, exceto se o direito da União ou de um Estado-Membro previr que a proibição geral a que se refere o n.º 1 do art. 9º não pode ser anulada pelo titular dos dados;
4	**(b)** A decisão exclusivamente automatizada for autorizada pelo direito da União ou do Estado-Membro a que o responsável pelo tratamento estiver sujeito, e na qual estejam igualmente previstas medidas adequadas para salvaguardar os direitos e liberdades e os legítimos interesses do titular dos dados;	+	**(g)** Se o tratamento de categorias especiais de dados pessoais for necessário por motivos de interesse público importante, com base no direito da União ou de um Estado-Membro, que deve ser proporcional ao objetivo visado, respeitar a essência do direito à proteção dos dados pessoais e prever medidas adequadas e específicas que salvaguardem os direitos fundamentais e os interesses do titular dos dados;
5	**(c)** A decisão exclusivamente automatizada for baseada no consentimento explícito do titular dos dados;	+	**(a)** Se o titular dos dados tiver dado o seu consentimento explícito para o tratamento de categorias especiais de dados pessoais para uma ou mais finalidades específicas, exceto se o direito da União ou de um Estado-Membro previr que a proibição geral a que se refere o n.º 1 do art. 9º não pode ser anulada pelo titular dos dados;
6	**(c)** A decisão exclusivamente automatizada for baseada no consentimento explícito do titular dos dados;	+	**(g)** Se o tratamento de categorias especiais de dados pessoais for necessário por motivos de interesse público importante, com base no direito da União ou de um

		Estado-Membro, que deve ser proporcional ao objetivo visado, respeitar a essência do direito à proteção dos dados pessoais e prever medidas adequadas e específicas que salvaguardem os direitos fundamentais e os interesses do titular dos dados;

Fonte: elaborado pela autora com base no Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho (GDPR)[158].

Pela leitura do Quadro 1, existem seis hipóteses em que o GDPR autoriza a utilização de decisões exclusivamente automatizadas que estiverem relacionadas às categorias especiais de dados pessoais. Entretanto, dentre as seis hipóteses, três delas (2, 4 e 6) são condicionadas aos tratamentos necessários para motivos de interesse público importante[159], enquanto que as outras três hipóteses (1, 3 e 5) são condicionadas ao consentimento explícito dado pelo titular dos dados para o tratamento de categorias especiais de dados pessoais para uma ou mais finalidades específicas.

2.1.2 Tratamento de categorias especiais de dados pessoais em todas as decisões automatizadas: base legal, princípios e direito dos titulares

O GDPR introduziu uma definição de "dados biométricos" ao considerá-los como dados "resultantes de um tratamento técnico específico relativo às características físicas, fisiológicas ou comportamentais de uma pessoa singular que permitam ou confirmem a identificação única dessa pessoa singular, nomeadamente imagens faciais ou dados dactiloscópicos"[160] (art. 4(14), GDPR). Além disso, o GDPR considerou os dados biométricos como pertencentes a categorias

[158] UNIÃO EUROPEIA. Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, op. cit.

[159] "O interesse público abrange uma ampla gama de valores e princípios relacionados ao bem público, ou ao que é do melhor interesse da sociedade. Precisa ser real e substancial. Dados os riscos inerentes aos dados de categoria especial, não basta fazer um argumento vago ou genérico de interesse público. Você deve ser capaz de apresentar argumentos específicos sobre os benefícios mais amplos e concretos do seu processamento." No original: "The public interest covers a wide range of values and principles relating to the public good, or what is in the best interests of society. It needs to be real and of substance. Given the inherent risks of special category data, it is not enough to make a vague or generic public interest argument. You should be able to make specific arguments about the concrete wider benefits of your processing." INFORMATION COMMISSIONER'S OFFICE. Guide to the General Data Protection Regulation (GDPR). Special category data. **Information Commissioner's Office (ico.)**, 2022. Disponível em: https://ico.org.uk/media/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr-1-1.pdf. Acesso em: 21 abr. 2023. p. 71.

[160] UNIÃO EUROPEIA. Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, op. cit.

especiais de dados pessoais e, assim, impôs requisitos mais rigorosos para o seu processamento que para outros dados pessoais, eis que o seu art. 9(1) dispõe:

> Artigo 9.º
> Tratamento de categorias especiais de dados pessoais
> 1. É proibido o tratamento de dados pessoais que revelem a origem racial ou étnica, as opiniões políticas, as convicções religiosas ou filosóficas, ou a filiação sindical, bem como o tratamento de dados genéticos, dados biométricos para identificar uma pessoa de forma inequívoca, dados relativos à saúde ou dados relativos à vida sexual ou orientação sexual de uma pessoa[161].

Assim, o início do art. 9º do GDPR consagrou a proibição geral para o tratamento de dados pessoais que revelem dados biométricos para identificação de uma pessoa de forma inequívoca. Apesar desse impedimento extensivo, o mesmo artigo ainda dispõe algumas exceções (art. 9º(2) do GDPR), que traduzem hipóteses em que o referido tratamento pode ocorrer. Existe, pois, a possibilidade de tratar dados pessoais biométricos (i) se houver o consentimento explícito do seu titular para finalidades específicas; (ii) se for necessário para cumprimento de obrigação legal e do exercício de direitos específicos do responsável do tratamento ou titular dos dados em razão de legislação laboral, de segurança social e de proteção social; (iii) se for necessário para a proteção dos interesses vitais do titular incapacitado de dar seu consentimento ou de outra pessoa; (iv) se for efetuado por uma fundação, associação ou qualquer outro organismo sem fins lucrativos e que prossiga fins políticos, filosóficos, religiosos ou sindicais; (v) se disser respeito à dados que tenham sido manifestamente tornados públicos pelo seu titular; (vi) se for necessário no contexto de um processo judicial ou em função jurisdicional dos tribunais; (vii) se for necessário por motivos de interesse público importante, que deve ser proporcional ao objetivo visado; (viii) se for necessário para efeitos de medicina preventiva ou do trabalho; (ix) se for necessário por motivos de interesse público no domínio da saúde pública; (x) se for necessário para fins de arquivo de interesse público, para fins de investigação científica ou histórica ou para fins estatísticos, que deve ser proporcional ao objetivo visado[162].

O consentimento[163], como visto, é uma entre as dez bases legais que regularizam o tratamento de dados biométricos. No entanto, existem algumas condições específicas dispostas

---

[161] Ibidem.
[162] UNIÃO EUROPEIA. Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, op. cit.
[163] GDPR, Art. 4.º (11): "«Consentimento» do titular dos dados, uma manifestação de vontade, livre, específica, informada e explícita, pela qual o titular dos dados aceita, mediante declaração ou ato positivo inequívoco, que os dados pessoais que lhe dizem respeito sejam objeto de tratamento;". Ibidem.

no GDPR que devem ser atendidas para que ele seja considerado válido. Assim, o consentimento dado pelo titular dos dados deve ser (i) livre, baseado em uma escolha real, sem coerção, intimidação ou influência indevida; (ii) específico, ou seja, solicitado para uma finalidade específica, não podendo ser usado para outras finalidades sem um novo consentimento; (iii) informado, de modo que o titular dos dados receba informações claras e compreensíveis sobre quem está tratando os dados, a finalidade do processamento, as categorias de dados pessoais envolvidos, os destinatários dos dados, o direito de retirar o consentimento a qualquer momento e outras informações relevantes; (iv) inequívoco, o consentimento deve ser dado por meio de uma ação afirmativa clara e positiva, como marcar uma caixa de seleção ou assinar um termo de consentimento[164].

Além disso, o GDPR estabelece que o consentimento deve ser documentado, de modo que o responsável pelo tratamento dos dados pessoais possa comprovar que o coletou. Isso significa que o controlador dos dados deve manter registros do consentimento dado, incluindo o momento em que foi obtido, a forma em que foi obtido e todas as informações relevantes que foram fornecidas ao titular dos dados[165].

A princípio, o uso ou venda de serviços de reconhecimento facial que envolvam o tratamento de dados biométricos para fins de identificação única de uma pessoa seria proibido pelo GDPR por força do art. 9º(1), a menos que o tratamento desses dados seja fundamentado em uma das condições definidas no art. 9º(2) do GDPR. Portanto, para que uma empresa que opera dados pessoais de titulares pertencentes à UE possa utilizar ou comercializar serviços com tecnologia de reconhecimento facial, isso dependerá das circunstâncias específicas do caso, incluindo a finalidade para a qual a tecnologia será aplicada, se possui ou não intervenção humana e a identificação de qual fundamentação legal dará legitimidade ao tratamento de dados biométricos para esse fim.

Convém mencionar que as orientações do *WP 251* do Artigo 29 são no sentido de que, além de satisfazer uma das condições dispostas no art. 9º(2) do GDPR, o tratamento de categorias especiais de dados decorrente de decisão automatizada também deve ser fundamentado em uma das bases legais previstas no art. 6º do GDPR.[166] Entretanto, essa obrigação cumulativa não foi encontrada em outros materiais[167], sendo que o "Manual sobre a

---

[164] Ver Considerandos nº 32 e nº 43 do GDPR. Ibidem.
[165] Ver Considerando nº 42 do GDPR. Ibidem.
[166] WORKING PARTY. Article 29. **Orientações sobre as decisões individuais automatizadas e a definição de perfis para efeitos do Regulamento (UE) 2016/679**, op. cit., p. 16.
[167] A Autoridade de proteção de dados do Reino Unido (*Information Commissioner's Office - ico.*), apesar de não fazer parte da UE, é uma importante fonte de informações sobre privacidade e proteção de dados e de implementação do GDPR do Reino Unido, que possui disposições semelhantes ao GDPR do Parlamento Europeu

lei europeia de proteção de dados" (*Handbook on European data protection law*)[168] apenas menciona a obrigação derivada do art. 9º, entendimento que será adotado.

Além de garantir a legalidade por meio de uma base legal, nos termos referidos acima, o tratamento de dados biométricos deve ser justo e transparente, bem como estar em conformidade com todos os demais princípios previstos no GDPR em seu art. 5º. Os princípios incorporam o espírito de todo o regime de proteção de dados pessoais e, portanto, formam o alicerce para boas práticas nas operações envolvendo esses dados. Foram estabelecidos sete: (i) princípio da licitude, equidade e transparência (art. 5º(1)(a)); (ii) princípio da limitação das finalidades (art. 5º(1)(b)); (iii) princípio da minimização dos dados (art. 5º(1)(c)); (iv) princípio da exatidão (art. 5º(1)(d)); (v) princípio da limitação da conservação (art. 5º(1)(e)); (vi) princípio da integridade e confidencialidade (art. 5º(1)(f)); (vii) princípio da responsabilidade (art. 5º(2))[169].

Em vista disso, destaca-se o Considerando 39 do GDPR[170], que estabelece as principais diretrizes a serem seguidas para que o tratamento de dados pessoais esteja em conformidade com os princípios. O Considerando reforça a necessidade de uma atuação transparente, de modo que as pessoas singulares saibam que seus dados pessoais estão sujeitos a qualquer tipo de tratamento e a medida em que isso ocorre. As informações devem ser de fácil acesso e compreensão e em linguagem clara e simples, bem como devem esclarecer quem é o responsável pelo tratamento e as finalidades a que se destina. Deve-se também alertar as pessoas "para os riscos, regras, garantias e direitos associados ao tratamento dos dados pessoais e para os meios de que dispõem para exercer os seus direitos"[171].

De acordo com o princípio da limitação das finalidades, os dados pessoais somente devem ser coletados "para finalidades determinadas, explícitas e legítimas e não podendo ser tratados posteriormente de uma forma incompatível com essas finalidades"[172].

---

e Conselho. O Guia do ico, assim dispõe: "Para processar dados de categoria especial legalmente, você deve identificar uma base legal sob o Artigo 6 do GDPR do Reino Unido e uma condição separada para processamento sob o Artigo 9. Eles não precisam estar vinculados." (tradução do autor). INFORMATION COMMISSIONER'S OFFICE. Guide to the General Data Protection Regulation (GDPR), op. cit., p. 68.

[168] COUNCIL OF EUROPE; EUROPEAN COURT OF HUMAN RIGHTS; EUROPEAN DATA PROTECTION SUPERVISOR; EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS. **Handbook on European data protection law**: 2018 edition. Publications Office of the European Union, 2019. Disponível em: https://data.europa.eu/doi/10.2811/343461. Acesso em 21 abr. 2023. p. 159 e ss.

[169] UNIÃO EUROPEIA. Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, op. cit.

[170] Ver Considerando nº 39 do GDPR. Ibidem.

[171] Ibidem.

[172] Ibidem.

A seu turno, o princípio da minimização revela que os dados pessoais devem ser adequados, pertinentes e limitados ao necessário para as finalidades as quais são tratados, ou seja, para que isso ocorra, (i) os dados pessoais apenas deverão ser tratados se a finalidade do tratamento não puder ser atingida por outros meios; (ii) o prazo de conservação dos dados deverá ser limitado ao mínimo; e (iii) deverão ser fixado prazos para o apagamento ou a revisão periódica.

O princípio da exatidão, por sua vez, estabelece que os dados pessoais devem ser "exatos e atualizados sempre que necessário"[173]. Isso significa que o responsável pelo tratamento dos dados deve garantir que as informações pessoais sejam precisas e completas, de forma que, se houver alguma mudança, medidas deverão ser tomadas para atualização dessas informações e exclusão das inexatas ou incompletas. Se um titular perceber que suas informações estão incorretas, incompletas ou desatualizadas, ele tem o direito de solicitar as correções necessárias.

De acordo com o princípio da limitação da conservação, os dados pessoais devem ser mantidos apenas durante o tempo necessário para atingir a finalidade para a qual foram coletados. Após esse período, os dados devem ser eliminados ou anonimizados, a menos que haja uma justificativa legal para mantê-los por mais tempo, como obrigações legais e regulamentares aplicáveis[174]. O responsável pelo tratamento deve determinar um período de retenção adequado e documentar as razões de armazenamento.

O princípio da integridade e confidencialidade exige que os dados pessoais sejam tratados de forma a garantir a sua segurança, proteção e confidencialidade, por meio da implementação de medidas técnicas e organizacionais adequadas para proteção contra perda, destruição ou danificação acidental, bem como para impedir qualquer acesso, divulgação ou destruição não autorizada ou ilegal.

Por fim, o princípio da responsabilidade destaca a importância da implementação de medidas proativas para garantir a conformidade com as normas de proteção de dados e a capacidade de comprová-la às autoridades reguladoras e aos titulares dos dados.

Assim como todas as leis de proteção de dados, um dos objetivos do GDPR é assegurar que as empresas protejam de maneira responsável a privacidade e os dados pessoais dos indivíduos, o que levou ao fortalecimento dos direitos dos titulares dos dados em relação às

---

[173] Ibidem.

[174] GDPR, Art. 5º (1) (e): "[...] os dados pessoais podem ser conservados durante períodos mais longos, desde que sejam tratados exclusivamente para fins de arquivo de interesse público, ou para fins de investigação científica ou histórica ou para fins estatísticos, em conformidade com o artigo 89.º, n.º 1, sujeitos à aplicação das medidas técnicas e organizativas adequadas exigidas pelo presente regulamento, a fim de salvaguardar os direitos e liberdades do titular dos dados («limitação da conservação»)." UNIÃO EUROPEIA. Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, op. cit.

empresas e à introdução de novos direitos. Como resultado, o setor privado deve aumentar seus esforços para garantir que esses direitos dos titulares dos dados possam ser exercidos por eles.

Em vista disso, os responsáveis pelo tratamento automatizado de dados pessoais (com ou sem interferência humana, bem como sendo ou não categoria especial de dados) devem garantir os seguintes direitos aos titulares previstos no GDPR: (i) direito de ser informado (arts. 13º e 14º); (ii) direito de acesso (art. 15º); (iii) direito de retificação (art. 16º); direito ao apagamento dos dados (art. 17º); (iv) direito à limitação do tratamento (art. 18º); (v) direito de oposição (art. 21º)[175].

O direito de ser informado (arts. 13º e 14º do GDPR) possui certa relação com o princípio da transparência, em vista que as pessoas afetadas sobre os processos de tomada de decisão automatizada têm o direito de receber dos responsáveis pelo tratamento todas as informações[176] que dizem respeito aos seus dados pessoais, de maneira clara e simples, por exemplo, a forma de coleta; a(s) finalidade(s) do tratamento; a base legal fundamentadora; quem são os terceiros destinatários; nome e contato do responsável; prazo de conservação dos dados; a existência de decisões automatizadas, incluindo a definição de perfis, contendo informações úteis relativas à lógica subjacente[177], bem como a importância e as consequências para o titular dos dados; entre outras informações.[178]

O direito de acesso (art. 15º do GDPR) garante ao titular dos dados que o responsável pelo tratamento tem a obrigação de disponibilizar os dados utilizados. O titular tem o mesmo direito de acesso aos dados relativos às decisões exclusivamente automatizadas, incluindo a definição de perfis, como sobre a sua existência, a lógica subjacente, a sua importância e as suas consequências. O Considerando 63 do GDPR entende que o direito de acesso não deve prejudicar os direitos ou liberdades de terceiros, incluindo o segredo comercial ou a propriedade intelectual, e, em particular, o direito de autor que protege o software. No entanto, a proteção

---

[175] UNIÃO EUROPEIA. Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, op. cit.

[176] Ver WORKING PARTY. Article 29. **Orientações relativas à transparência na aceção do Regulamento 2016/679** (WP 260 rev.01). Bruxelas, 2017. Disponível em: https://ec.europa.eu/newsroom/article29/items/622227/en. Acesso em: 24 abr. 2023.

[177] "O responsável pelo tratamento deverá encontrar formas simples de comunicar ao titular dos dados a lógica subjacente, ou os critérios aplicados para tomar a decisão. O RGPD obriga o responsável pelo tratamento a fornecer informações úteis relativas à lógica subjacente, e não necessariamente uma explicação complexa sobre os algoritmos utilizados ou a divulgação do algoritmo na íntegra. As informações prestadas devem, no entanto, ser suficientemente completas para permitir ao titular dos dados compreender os motivos da decisão." WORKING PARTY. Article 29. **Orientações sobre as decisões individuais automatizadas e a definição de perfis para efeitos do Regulamento (UE) 2016/679**, op. cit., p. 28.

[178] UNIÃO EUROPEIA. Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, op. cit.

do segredo comercial não pode ser usada como pretexto para negar o acesso ou se recusar a fornecer informações ao titular dos dados.[179]

O direito de retificação (art. 16º do GDPR) garante que o titular dos dados pessoais possa exigir do responsável pelo tratamento a retificação ou correção de dados inverídicos, imprecisos ou incompletos. O titular também tem o direito de complementar os dados pessoais incompletos[180].

O direito ao apagamento, também conhecido como direito a ser esquecido (art. 17º do GDPR), permite que o titular de dados solicite ao responsável pelo tratamento a exclusão de seus dados pessoais quando eles não são mais necessários para a finalidade para a qual foram coletados ou quando o titular retirar o consentimento para o seu tratamento. Além disso, o direito ao apagamento pode ser exercido em outras situações descritas na Lei, como quando o tratamento dos dados é ilegal, quando o titular dos dados se opõe ao tratamento dos seus dados e não há motivos legítimos prevalecentes para o tratamento, ou quando os dados pessoais foram coletados em relação a oferta de serviços da sociedade da informação para menores de idade. É importante destacar que, em certas circunstâncias, o direito ao apagamento pode ser limitado pelo interesse público, pela liberdade de expressão e pelo direito à informação, bem como pela necessidade de cumprimento de obrigações legais por parte do responsável pelo tratamento.[181]

O direito à limitação do tratamento (art. 18º do GDPR) confere aos titulares de dados a possibilidade de solicitar a restrição do tratamento dos seus dados pessoais em algumas circunstâncias específicas, tais como, quando contestar a exatidão dos dados pessoais que estão sendo tratados; quando o tratamento dos dados for ilegal, mas o titular não deseja que sejam apagados; quando os dados pessoais não são mais necessários para fins de tratamento, mas ainda podem ser úteis para estabelecer, exercer ou defender reivindicações legais do titular; e quando o titular dos dados se opôs ao tratamento e aguarda a verificação se os motivos legítimos para o tratamento dos dados prevalecem sobre os do titular. Ao exercer o direito à limitação do tratamento, o responsável deve garantir que os dados pessoais só sejam tratados, alternativamente, com o consentimento do titular; para fins de estabelecer, exercer ou defender reivindicações legais; para proteger os direitos de outra pessoa física ou jurídica; ou por motivos de interesse público importante da UE ou de um Estado-Membro[182].

[179] Ibidem.
[180] Ibidem.
[181] Ibidem.
[182] Ibidem.

O art. 21º do GDPR prevê algumas circunstâncias em que o titular dos dados pode se opor ao tratamento de seus dados pessoais, especificamente, quando for baseado em interesses legítimos do responsável ou de terceiros; quando for para fins de pesquisa científica ou histórica ou para fins estatísticos; quando for para fins de marketing direto ou para a tomada de decisão automatizada, incluindo definição de perfil. Caso o titular dos dados se oponha ao tratamento com base nessas circunstâncias, o responsável pelo tratamento deve cessar o tratamento, a menos que este possa demonstrar "razões imperiosas e legítimas" que prevaleçam sobre os interesses, direitos e liberdades do titular dos dados ou para o exercício ou defesa de reivindicações legais.[183] O Artigo 29, em suas orientações do *WP 251*, dispõe que um exemplo possível de razão imperiosa e legítima seria um caso em que o tratamento trouxesse "vantagens para a sociedade no seu todo (ou a comunidade de forma mais ampla) e não apenas para os interesses comerciais do responsável pelo tratamento"[184].

2.1.3 Avaliação de Impacto sobre a Proteção de Dados (AIPD)

O art. 35º do GDPR introduziu a Avaliação de Impacto sobre a Proteção de Dados (AIPD) (*Data Protection Impact Assessment* - DPIA) e a tornou obrigatória para determinados tipos de tratamento de dados pessoais que podem apresentar elevados riscos para os direitos e liberdades das pessoas afetadas, conforme segue:

> Artigo 35.º
> Avaliação de impacto sobre a proteção de dados
> 1. Quando um certo tipo de tratamento, em particular que utilize novas tecnologias e tendo em conta a sua natureza, âmbito, contexto e finalidades, for suscetível de implicar um elevado risco para os direitos e liberdades das pessoas singulares, o responsável pelo tratamento procede, antes de iniciar o tratamento, a uma avaliação de impacto das operações de tratamento previstas sobre a proteção de dados pessoais. Se um conjunto de operações de tratamento apresentar riscos elevados semelhantes, pode ser analisado numa única avaliação[185].

Conforme a abordagem baseada em risco, só será obrigatória a realização do DPIA quando um tratamento implicar em elevado risco aos direitos e liberdades dos titulares de dados. Entretanto, a não satisfação das condições que obrigam a realização do DPIA não exime os

[183] UNIÃO EUROPEIA. Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, op. cit.
[184] WORKING PARTY. Article 29. **Orientações sobre as decisões individuais automatizadas e a definição de perfis para efeitos do Regulamento (UE) 2016/679**, op. cit., p. 20.
[185] UNIÃO EUROPEIA. Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, op. cit.

responsáveis pelo tratamento de dados pessoais de sua obrigação, em geral, de adotar medidas para gerenciar adequadamente os riscos das suas atividades. A avaliação dos riscos deve ser contínua para que identifiquem sempre que um tratamento puder implicar um elevado risco para os direitos e liberdades das pessoas singulares[186].

O Artigo 29 produziu suas "Orientações relativas à Avaliação de Impacto sobre a Proteção de Dados" (WP 248)[187] e considerou que a referência aos "direitos e liberdades das pessoas singulares" no art. 35º(1) do GDPR diz respeito "aos direitos de proteção dos dados e privacidade, mas também envolve outros direitos fundamentais como a liberdade de expressão, a liberdade de pensamento, a liberdade de circulação, a proibição de discriminação, o direito à liberdade, consciência e religião"[188].

Além disso, o final do texto do Considerando 89 do GDPR considera que os tratamentos de dados pessoais suscetíveis de implicar um elevado risco para os direitos e liberdades das pessoas singulares seriam aqueles que "envolvem o uso de novas tecnologias ou são de um novo tipo e onde nenhuma avaliação de impacto na proteção de dados foi realizada anteriormente"[189]. Em complemento, o final do Considerando 91 do GDPR acrescenta que esses tipos de tratamentos podem ser aqueles que "impedem os titulares dos dados de exercer um direito ou utilizar um serviço ou um contrato, ou porque são realizados sistematicamente em grande escala"[190].

O art. 35º(3) do GDPR estabeleceu uma lista não exaustiva para os casos em que a condução de um DPIA é obrigatória, que representam exemplos de risco elevado, nos seguintes termos:

> 3. A realização de uma avaliação de impacto sobre a proteção de dados a que se refere o n.º 1 é obrigatória nomeadamente em caso de:
> a) Avaliação sistemática e completa dos aspectos pessoais relacionados com pessoas singulares, baseada no tratamento automatizado, incluindo a definição de perfis, sendo com base nela adotadas decisões que produzem efeitos jurídicos relativamente à pessoa singular ou que a afetem significativamente de forma similar;
> b) Operações de tratamento em grande escala de categorias especiais de dados a que se refere o artigo 9.º, n.º 1, ou de dados pessoais relacionados com condenações penais e infrações a que se refere o artigo 10.º; ou

[186] WORKING PARTY. Article 29. **Orientações relativas à Avaliação de Impacto sobre a Proteção de Dados (AIPD) e que determinam se o tratamento é «suscetível de resultar num elevado risco» para efeitos do Regulamento (UE) 2016/679** (WP 248 rev.01). Bruxelas, 2017. Disponível em: https://ec.europa.eu/newsroom/article29/items/611236/en. Acesso em: 24 abr. 2023. p. 7.
[187] Ibidem, p. 7.
[188] Ibidem, p. 7.
[189] UNIÃO EUROPEIA. Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, op. cit.
[190] Ibidem.

c) Controlo sistemático de zonas acessíveis ao público em grande escala[191].

O GDPR, portanto, dispõe que é necessário realizar um DPIA se o objetivo do tratamento de dados pessoais for (i) a tomada de decisões que produzam efeitos jurídicos ou efeitos similares aos indivíduos com base em avaliação de seus aspectos pessoais por tratamento automatizado, incluindo a definição de perfis; (ii) processar em larga escala dados de categorias especiais ou relacionados com condenações penais e infrações; ou (iii) monitorar locais acessíveis ao público em larga escala[192].

Apesar dos exemplos acima, o DPIA pode ser obrigatório em outras circunstâncias de elevado risco para os direitos e liberdades das pessoas singulares. Assim, as orientações do *WP 248* do Artigo 29 estabeleceram nove critérios a serem considerados para um direcionamento mais concreto na identificação de operações de tratamento que exigem um DPIA devido ao elevado risco inerente.

O primeiro critério diz respeito ao tratamento de dados destinados à avaliação ou à classificação, incluindo definição de perfis e previsão, por exemplo, conforme disposto nos Considerandos 71 e 91, de "aspetos relacionados com o desempenho profissional, a situação econômica, saúde, preferências ou interesses pessoais, fiabilidade ou comportamento, localização ou deslocações do titular dos dados"[193].

O segundo critério que exige um DPIA é o tratamento de dados destinado à tomada de decisões automatizadas que produzam efeitos jurídicos à pessoa singular ou afetem significativamente de modo similar, conforme art. 35.º(3)(a) do GDPR.[194] O terceiro critério, também previsto no GDPR em seu art. 35.º(3)(c), refere-se ao tratamento de controle sistemático[195] utilizado para observar, monitorar ou controlar os titulares dos dados.

Por sua vez, o quarto critério considera os tratamentos de dados sensíveis ou dados de natureza altamente pessoal, como os de categorias especiais do artigo 9º. O Artigo 29 considerou que estariam inclusos neste critério os "documentos pessoais, mensagens de correio

---

[191] UNIÃO EUROPEIA. Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, op. cit.
[192] Ibidem.
[193] WORKING PARTY. Article 29. **Orientações relativas à Avaliação de Impacto sobre a Proteção de Dados (AIPD) e que determinam se o tratamento é «suscetível de resultar num elevado risco» para efeitos do Regulamento (UE) 2016/679**, op. cit., p. 10.
[194] Ibidem, p. 10.
[195] O Artigo 29 interpreta "sistemático" como um ou mais dos pontos a seguir (ver as orientações sobre o encarregado da proteção de dados - *WP 243*): (i) que ocorre de acordo com um sistema; (ii) pré-determinado, organizado ou metódico; (iii) que acontece como parte de um plano geral de recolha de dados; (iv) realizado como parte de uma estratégia. WORKING PARTY. Article 29. **Orientações relativas à Avaliação de Impacto sobre a Proteção de Dados (AIPD) e que determinam se o tratamento é «suscetível de resultar num elevado risco» para efeitos do Regulamento (UE) 2016/679**, op. cit., p. 11.

eletrônico, diários, notas de dispositivos eletrônicos de leitura equipados com funções de introdução de notas, bem como informações muito pessoais incluídas em aplicações onde ficam registados eventos da vida dos indivíduos"[196].

Os dados pessoais tratados em grande escala são o quinto critério para a condução de um DPIA. Segundo o Considerando 91 do GDPR, as operações de tratamento de larga escala seriam aquelas que

> visem o tratamento de uma grande quantidade de dados pessoais a nível regional, nacional ou supranacional, possam afetar um número considerável de titulares de dados e sejam suscetíveis de implicar um elevado risco, por exemplo, em razão da sua sensibilidade, nas quais, em conformidade com o nível de conhecimentos tecnológicos alcançado, seja utilizada em grande escala uma nova tecnologia, bem como a outras operações de tratamento que impliquem um elevado risco para os direitos e liberdades dos titulares dos dados, em especial quando tais operações dificultem aos titulares o exercício dos seus direitos[197].

O Artigo 29 recomenda que, para determinar se um tratamento é ou não de larga escala, sejam considerados:

> a. o número de titulares de dados envolvidos, quer através de um número específico quer através de uma percentagem da população pertinente;
> b. o volume de dados e/ou a diversidade de dados diferentes a tratar;
> c. a duração da atividade de tratamento de dados ou a sua pertinência;
> d. a dimensão geográfica da atividade de tratamento[198].

O sexto critério diz respeito ao estabelecimento de correspondências ou a combinação de conjuntos de dados que sejam de operações de tratamento de dados distintas com diferentes finalidades e/ou realizadas por diferentes responsáveis, de forma que exceda as expectativas razoáveis do titular dos dados.[199]

Enquanto isso, o sétimo critério para a realização de um DPIA considera os tratamentos com dados relativos a titulares vulneráveis (Considerando 75), incluindo crianças, empregados, pessoas com doenças mentais, idosos, doentes, etc., por entender que existe um desequilíbrio de poder entre esses titulares de dados e os responsáveis pelo tratamento dos dados, o que

---

[196] Ibidem. p. 11.
[197] UNIÃO EUROPEIA. Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, op. cit.
[198] WORKING PARTY. Article 29. **Orientações relativas à Avaliação de Impacto sobre a Proteção de Dados (AIPD) e que determinam se o tratamento é «suscetível de resultar num elevado risco» para efeitos do Regulamento (UE) 2016/679**, op. cit., p. 11-12.
[199] Ibidem, p. 12.

significa uma dificuldade ou até incapacidade em dar o consentimento, opor-se ao tratamento ou mesmo exercer seus direitos de titular[200].

O penúltimo e oitavo critério trata sobre a "utilização de soluções inovadoras ou aplicação de novas soluções tecnológicas ou organizacionais, tais como combinar a utilização da impressão digital e do reconhecimento facial para melhorar o controlo [sic] do acesso físico, etc."[201]. Tal previsão está em concordância com o GDPR (art. 35º(1) e Considerando 89 e 91) que prevê que o emprego de uma nova tecnologia - com conhecimentos tecnológicos avançados - pode exigir a elaboração de um DPIA.

Por fim, o nono critério refere-se a "quando o próprio tratamento impede os titulares dos dados de exercer um direito ou de utilizar um serviço ou um contrato", conforme art. 22.º e Considerando 91 do GDPR.

Como parte do princípio da responsabilização, o art. 30º(1) do GDPR estabelece que cada responsável pelo tratamento de dados deve manter um registro de todas as atividades de tratamento sob sua responsabilidade, o que inclui, de modo geral, informações sobre (i) quais dados são coletados, (ii) as finalidades do tratamento, (iii) as categorias de titulares de dados envolvidas, (iv) se há compartilhamento e/ou transferência internacional de dados, (v) o período de armazenamento dos dados e (vi) uma descrição geral das medidas técnicas e organizacionais de segurança referidas no art. 32º(1) do GDPR. Assim, por meio desse registro, deverá ser feita uma avaliação da probabilidade das atividades envolverem um elevado risco aos direitos e liberdades das pessoas singulares, mesmo que o responsável decida pela não realização de um DPIA. O Artigo 29 pondera, em suas orientações do *WP 248*, que "quantos mais critérios forem satisfeitos pelo tratamento, maior é a probabilidade de este implicar um elevado risco para os direitos e as liberdades dos titulares dos dados e, por conseguinte, de necessitar de uma AIPD"[202].

Os exemplos dispostos no Quadro 2 a seguir demonstram como os critérios determinados acima expostos devem ser empregados para analisar se uma determinada operação de processamento que utiliza tecnologia de reconhecimento facial requer ou não a realização de um DPIA:

---

[200] Ibidem, p. 12.
[201] Ibidem, p. 12.
[202] WORKING PARTY. Article 29. **Orientações relativas à Avaliação de Impacto sobre a Proteção de Dados (AIPD) e que determinam se o tratamento é «suscetível de resultar num elevado risco» para efeitos do Regulamento (UE) 2016/679**, op. cit., p. 12.

Quadro 2 - Avaliação de operações de tratamento segundo os critérios do Artigo 29 para realização de um DPIA

Exemplos de tratamento	**Critérios pertinentes possíveis segundo *WP 248***	**Exige-se realização de um DPIA?**
Uma grande loja de roupas, com filiais por toda UE, que utiliza tecnologia de reconhecimento facial, com a coleta de consentimento específico dos titulares dos dados, para classificá-los em idade, gênero e sexo e fazer uma análise das preferências de seus clientes.	- Avaliação ou classificação; - Controle sistemático; - Dados sensíveis; - Dados tratados em grande escala; - Dados relativos a titulares de dados vulneráveis; - Utilização de soluções inovadoras ou aplicação de novas soluções tecnológicas ou organizacionais.	Sim
Um hospital particular que utiliza tecnologia de reconhecimento facial, com a coleta de consentimento específico dos titulares dos dados, para verificação de colaboradores que acessam o local e para o controle de acesso e de ponto.	- Avaliação ou classificação; - Decisões automatizadas que produzam efeitos jurídicos ou afetem significativamente de modo similar; - Controle sistemático; - Dados sensíveis; - Dados relativos a titulares de dados vulneráveis; - Utilização de soluções inovadoras ou aplicação de novas soluções tecnológicas ou organizacionais.	Sim
Um banco, com agências em toda a UE, que utiliza tecnologia de reconhecimento facial, com a coleta de consentimento específico dos titulares dos dados, para identificação de clientes a partir de uma base de dados e fazer um controle seletivo para concessão de empréstimo.	- Avaliação ou classificação; - Decisões automatizadas que produzam efeitos jurídicos ou afetem significativamente de modo similar; - Dados sensíveis; - Dados tratados em grande escala; - Estabelecer correspondências ou combinar conjuntos de dados; - Dados relativos a titulares de dados vulneráveis; - Utilização de soluções inovadoras ou aplicação de novas soluções tecnológicas ou organizacionais; - O tratamento impede os titulares dos dados de exercer um direito ou de utilizar um serviço ou um contrato.	Sim

Fonte: elaborado pela autora com base nas "Orientações relativas à Avaliação de Impacto sobre a Proteção de Dados", WP 248, do Artigo 29[203].

Um DPIA deve conter, pelo menos: (i) uma descrição sistemática das operações de tratamento previstas e das finalidades do tratamento, incluindo, se for o caso, o interesse legítimo perseguido pelo responsável pelo tratamento; (ii) uma avaliação da necessidade e proporcionalidade das operações de tratamento em relação às finalidades; (iii) uma avaliação dos riscos para os direitos e liberdades dos titulares dos dados; e (iv) as medidas previstas para fazer face aos riscos, incluindo salvaguardas, medidas de segurança e mecanismos para garantir a proteção dos dados pessoais e para demonstrar o cumprimento com o GDPR, considerando os direitos e interesses legítimos dos titulares dos dados e de outras pessoas interessadas (art. 35.º(7) do RGPD)[204].

Se, após a condução de um DPIA, o responsável pelo tratamento dos dados pessoais considerar que os riscos foram suficientemente reduzidos, é possível que o tratamento ocorra sem a realização de uma consulta à autoridade de controle. Contudo, se não for possível a indicação de medidas suficientes para os riscos identificados, então o responsável pelo tratamento dos dados pessoais deve consultar a autoridade de controlo, isto é, quando os riscos residuais permanecem elevados[205].

Além disso, como boa prática, o DPIA representa parte das obrigações gerais em matéria de princípio da responsabilização, de modo que deve ser constantemente revisado e avaliado para uma boa gestão de riscos e para a garantia da privacidade e da proteção dos dados. O DPIA deve ser entendido como um instrumento de apoio e de demonstração de conformidade, assim como um processo contínuo, especialmente porque as operações de tratamento de dados estão sempre sujeitas a mudanças[206].

O não cumprimento dos requisitos da DPIA pode levar a multas administrativas impostas pela autoridade supervisora competente. A não realização de um DPIA quando o documento é obrigatório para o tratamento (art. 35.º(1) e (3)-(4) do GDPR), a realização de um DPIA de forma incorreta (art. 35.º(2) e (7) a (9) do GDPR), ou a não consulta da autoridade de supervisão competente quando necessário (art. 36.º (3)(e) do GDPR), pode resultar numa multa

[203] WORKING PARTY. Article 29. **Orientações relativas à Avaliação de Impacto sobre a Proteção de Dados (AIPD) e que determinam se o tratamento é «suscetível de resultar num elevado risco» para efeitos do Regulamento (UE) 2016/679**, op. cit., p. 10-14.
[204] UNIÃO EUROPEIA. Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, op. cit.
[205] WORKING PARTY. Article 29. **Orientações relativas à Avaliação de Impacto sobre a Proteção de Dados (AIPD) e que determinam se o tratamento é «suscetível de resultar num elevado risco» para efeitos do Regulamento (UE) 2016/679**, op. cit., p. 22.
[206] Ibidem, p. 14.

administrativa de até dez milhões de Euros (10 000 000 EUR) ou, no caso de uma empresa, até 2% do seu volume de negócios anual a nível mundial correspondente ao exercício financeiro anterior, o que for maior (art. 83.º(4)(a) do GDPR)[207].

A intenção desta pesquisa não é esgotar o tema sobre o DPIA, tendo em vista ser um assunto complexo por si só e que possui debates mais aprofundados, mas compreender em quais situações o documento deverá ser elaborado e quais são os seus requisitos mínimos, conforme apresentado até aqui. Esse entendimento permite a conclusão de que o uso das tecnologias de reconhecimento facial depende da condução de um DPIA para mitigação de riscos em relação aos direitos e liberdades das pessoas afetadas pelo tratamento dos seus dados pessoais biométricos faciais. Além disso, o DPIA, sem deixar de lado as disposições do GDPR vistas anteriormente, representa um importante meio de regulamentação das tecnologias de reconhecimento facial.

2.1.4 Regulamentação das Inteligências Artificiais (IAs)

A regulamentação das Inteligências Artificiais (IAs) está atualmente em discussão na UE, o que implicará em disciplinar o uso das tecnologias de reconhecimento facial. Em fevereiro de 2020, a Comissão Europeia publicou o "Livro Branco sobre Inteligência Artificial" (*White Paper on Artificial Intelligence (AI)176*)[208] em que destacou as implicações causadas para os direitos fundamentais decorrentes do uso de sistemas de IA de identificação biométrica remota e de tecnologia de reconhecimento facial na UE. Além disso, a Comissão Europeia ressaltou um cenário em que esses sistemas devem ser regulados por uma avaliação de impacto e por uma proposta de lei da IA. O Parlamento Europeu, responsável pela aprovação de legislações europeias junto com o Conselho da União Europeia, solicitou a consideração de limites para o uso de reconhecimento facial na UE em vários contextos, como em áreas públicas e em estabelecimentos de educação e saúde. Alguns membros do Parlamento expressaram apoio para a proibição do uso de tecnologias de reconhecimento facial em contextos específicos, como para fins educacionais e culturais, enquanto outros membros solicitaram a proibição expressa

[207] UNIÃO EUROPEIA. Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, op. cit.
[208] COMISSÃO EUROPEIA. Livro Branco sobre a inteligência artificial: uma abordagem europeia virada para a excelência e a confiança. COM(2020) 65 final. **Comissão Europeia**: Bruxelas, 2020. Disponível em: https://commission.europa.eu/system/files/2020-03/commission-white-paper-artificial-intelligence-feb2020_pt.pdf. Acesso em: 26 abr. 2023.

na legislação da UE para a vigilância em massa através da coleta de biometria em espaços públicos[209].

Em abril de 2021, a Comissão Europeia apresentou uma proposta de regulamento de IAs para a UE (*Artificial Intelligence Act*), a primeira sobre esse assunto no mundo.[210] Nessa proposta, a Comissão abordou os riscos associados a usos específicos da IA, classificando-os em quatro níveis diferentes: (i) risco inaceitável; (ii) risco elevado; (iii) risco limitado e (iv) risco mínimo. Assim, alguns tipos de sistemas IAs foram considerados de uso proibido por criarem um "risco inaceitável" que contraria os valores da UE. Outros sistemas de IA foram considerados como "alto risco" porque criam impacto negativo na segurança ou nos direitos fundamentais das pessoas. Tais sistemas de IA de "alto risco", segundo a proposta, deverão ser submetidos a uma avaliação de conformidade antes de serem colocados no mercado e cumprir uma série de requisitos de segurança, como gestão de riscos, supervisão humana e governança de dados. Ademais, após inseridos no mercado, esses sistemas também deverão permanecer sob supervisão e vigilância para garantir o cumprimento das obrigações e requisitos de segurança. Por sua vez, os sistemas de IA de "risco limitado" estarão sujeitos a um conjunto limitado de obrigações, como a transparência, enquanto que os sistemas de IA de "risco mínimo" não terão obrigações legais adicionais além das já existentes na UE, podendo ser desenvolvidos e usados[211].

Com relação ao reconhecimento facial e demais sistemas biométricos, a Comissão apresentou, com essa nova proposta, a distinção entre (i) sistemas de identificação biométrica remota em tempo real: "capazes de capturar dados biométricos e executar processos de comparação e identificação instantaneamente (ou sem atraso significativo), com base em material "ao vivo" ou "quase ao vivo", como imagens geradas por câmera ou outro dispositivo"[212]; e (ii) sistemas de identificação biométrica remota posterior: "permitem a captura de dados biométricos e os processos de comparação e de identificação ocorrerem após um atraso significativo, com base em fotos ou imagens de vídeo geradas por câmeras de circuito

[209] MADIEGA; MILDEBRATH, op. cit., p. 23.
[210] EUROPEAN COMMISSION. Proposal for a Regulation of the European Parliament and of the Council: Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts. 2021/0106 (COD). **European Commission**: Brussels, 2021. Disponível em: https://digital-strategy.ec.europa.eu/en/library/proposal-regulation-laying-down-harmonised-rules-artificial-intelligence. Acesso em 26 abr. 2023.
[211] MADIEGA; MILDEBRATH, op. cit., p. 24.
[212] No original: "'Real-time' biometric identification systems would be defined as systems that are able to capture biometric data and run the comparison and identification processes instantaneously (or without a significant delay), based on 'live' or 'near-live' material, such as video footage, generated by a camera or other device." Ibidem, p. 25.

fechado de televisão (CFTV) ou dispositivos privados"[213]. Essa diferenciação seria para sujeitá-los a um conjunto diferente de regras, dependendo do seu uso[214].

A partir dessa divisão, quatro cenários foram delimitados pela Comissão Europeia. O primeiro seria a proibição do "uso de sistemas de IA de alto risco para identificação biométrica remota em tempo real de pessoas naturais em espaços públicos para fins de *law enforcement*"[215], por exemplo, em caso de identificação de pessoas em protestos públicos ou para localizar pessoas que cometeram crimes de menor gravidade.

O segundo cenário compreende três exceções ao cenário anterior, portanto, a permissão do uso de sistemas de IA de alto risco para identificação biométrica remota, em tempo real, de pessoais naturais em espaços públicos para fins de *law enforcement*, conforme o interesse público relevante supere os riscos aos direitos fundamentais. Essa permissão seria para os casos de: (a) "busca direcionada por potenciais vítimas de crime, incluindo crianças desaparecidas"[216]; (b) "prevenção de uma ameaça específica, substancial e iminente à vida ou à segurança física de pessoas ou de um ataque terrorista"[217]; (c) "detecção, localização, identificação ou processamento de um infrator ou indivíduo suspeito de uma infração penal"[218] grave que garanta a sua extradição rápida e eficiente entre os Estados-Membros da UE. Ressalta-se que a proposta dispõe que essas exceções tem implementação facultativa pelos Estados-Membros, que podem adotar regras mais detalhadas em seu direito nacional.

O terceiro cenário diz respeito à permissão de outros sistemas de identificação biométrica remota de alto risco, já que uma ampla gama de situações pode enquadrar-se nessa categoria. A proposta não proíbe esses sistemas por padrão, mas estabelece requisitos obrigatórios aos provedores desses sistemas para impedir riscos inaceitáveis para os interesses públicos da UE. Nesse sentido, estariam obrigados, entre outras coisas, a adotar planos de avaliação e mitigação de riscos, somente empregar conjunto de dados de alta qualidade, assegurar medidas de transparência, implementar supervisão humana de maneira adequada e certificar que os sistemas possuam nível satisfatório de precisão, robustez e cibersegurança. Ademais, a Comissão entende ser importante que os provedores desses sistemas do terceiro

[213] No original: "'Post' biometric identification systems, in contrast, would be systems enabling capture of biometric data and comparison and identification processes to run after a significant delay, based on pictures or video footage generated by closed circuit television (CCTV) cameras or private devices. Ibidem, p. 25.
[214] Ibidem, p. 25.
[215] Ibidem, p. 25.
[216] MADIEGA; MILDEBRATH, op. cit., p. 25.
[217] Ibidem, p. 25-26.
[218] Ibidem, p. 26.

cenário cumpram com procedimentos de avaliação de conformidade, antes da implementação no mercado, para obtenção de certificação emitida por órgãos independentes[219].

O quarto cenário consiste na permissão de tecnologias de reconhecimento facial que são consideradas de categorização biométrica, ou seja, aqueles sistemas cujo objetivo é categorizar as pessoas, por exemplo, em idade, sexo, cor dos cabelos, com base nos seus dados biométricos. Tais sistemas, por não serem classificados como de alto risco quando usados para fins que não seja a identificação, somente estariam sujeitos a implementação de medidas de transparência e de fornecimento de informações[220].

Observa-se que a proposta da Comissão Europeia de regulamento de IAs para a UE dá amplo destaque para as tecnologias biométricas, conferindo atenção para a urgência que o tema demanda. Entretanto, mesmo com pontos positivos e considerável avanço na regulamentação das tecnologias de reconhecimento facial, a publicação da proposta de lei da IA foi alvo de críticas.

O Serviço de Estudos do Parlamento Europeu (ERPS) examinou a proposta de regulamento da IA em uma publicação de análise aprofundada sobre o assunto e destacou quatro pontos de atenção: (i) a preocupação com a arbitrariedade na classificação dos sistemas biométricos em alto risco e baixo risco, em razão de ser "questionável fazer uma distinção entre sistemas de identificação biométrica remota "em tempo real" e "posterior", bem como entre sistemas de "categorização biométrica" e sistemas de "identificação biométrica""[221]; (ii) a necessidade de estabelecer regras mais rígidas, já que muitos sistemas de identificação biométrica remota continuariam permitidos, principalmente em espaços públicos; (iii) a margem de manobra atribuída aos Estados-Membros, que podem decidir sobre a implementação das exceções - segundo cenário; e (iv) as críticas à prática da Comissão em delegar a elaboração de regras de padronização para órgãos independentes (organismos regidos pelo direito privado), em razão da falta de supervisão democrática, de participação das partes afetadas e interessadas, de controle judicial sobre as regras de padronização, de poder de veto do Parlamento sobre essas regras.

O Conselho Europeu de Proteção de Dados (*European Data Protection Board* - EDPB) e a Autoridade Europeia para a Proteção de Dados (*European Data Protection Supervisor* - EDPS), em conjunto, também se posicionaram em relação a proposta de lei da IA e defenderam uma proibição geral de qualquer uso de IA para reconhecimento automatizado de características

[219] Ibidem, p. 26-27.
[220] Ibidem, p. 27.
[221] MADIEGA; MILDEBRATH, op. cit., p. 28.

humanas em espaços publicamente acessíveis em qualquer contexto, bem como recomendaram que os sistemas de IA, incluindo o reconhecimento facial, não sejam usados para categorizar indivíduos com base em sua etnia, gênero, orientação política ou sexual. Essa recomendação se aplicaria tanto para autoridades públicas quanto para entidades privadas, uma vez que a categorização baseada em características pessoais pode resultar em discriminação injusta e violar os direitos humanos fundamentais[222].

De modo geral, a proposta de lei europeia da IA pretende limitar o uso de sistemas de IA de identificação biométrica, incluindo o reconhecimento facial. Até o momento, a proposta está em discussão no Parlamento Europeu e traz grandes expectativas para o futuro em termos de implementação de novas regras para o uso das tecnologias de reconhecimento facial, além das legislações aplicáveis já existentes, por exemplo, os princípios gerais da Carta de Direitos Humanos Fundamentais da UE e o GDPR, conforme visto até aqui.

2.2 A REGULAMENTAÇÃO JURÍDICA DAS TECNOLOGIAS DE RECONHECIMENTO FACIAL NOS ESTADOS UNIDOS

Os Estados Unidos é o país que mais investe em tecnologia no mundo, principalmente em IA, com o maior número registrado de pedidos de patentes em relação à China e à União Europeia, conforme infografia feita pela Comissão Europeia[223]. Apesar da ampla investida, o país tem se destacado com relação a proibições, restrições ou moratórias em relação às tecnologias de reconhecimento facial, seja nos estados ou nas cidades. Por exemplo, cidades como São Francisco, Boston e Portland, de modo geral, proibiram a tecnologia em espaços públicos, enquanto que o estado da Califórnia, em 2020, impôs uma moratória de três anos em qualquer tecnologia de reconhecimento facial usada em câmeras utilizadas pelas polícias.[224] Tal cenário desperta curiosidade de estudo para compreender como ocorrem as limitações a fim de estabelecer uma comparação que possa agregar à temática de regulamentação dessas tecnologias.

---

[222] EUROPEAN DATA PROTECTION BOARD; EUROPEAN DATA PROTECTION SUPERVISOR. EDPB-EDPS Joint Opinion 5/2021 on the proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act). **EDPB-EDPS**: Brussels, 2021. Disponível em: https://edps.europa.eu/system/files/2021-06/2021-06-18-edpb-edps_joint_opinion_ai_regulation_en.pdf. Acesso em 26 abr. 2023. p. 11-13.

[223] REGULAR a Inteligência Artificial na UE: as propostas do Parlamento. **Parlamento Europeu**, 2023. Disponível em: https://www.europarl.europa.eu/news/pt/headlines/society/20201015STO89417/regular-a-inteligencia-artificial-na-ue-as-propostas-do-parlamento. Acesso em: 27 abr. 2023.

[224] MADIEGA; MILDEBRATH, op. cit., p. 32-33.

Verifica-se que, atualmente, não há uma legislação federal que regulamenta o uso de reconhecimento facial por empresas privadas ou no contexto de *law enforcement* nos Estados Unidos (EUA)[225], embora já existam movimentações para que isso aconteça[226].

A Comissão Federal de Comércio dos EUA (*Federal Trade Commission* - FTC), agência independente do governo, cuja missão é a aplicação das leis antitruste civil e a promoção da proteção do consumidor, emitiu algumas orientações comerciais sobre IA e algoritmos, como (i) pensar, desde o início, em maneiras de melhorar o conjunto de dados utilizado; (ii) testar o algoritmo antes de usá-lo e com periodicidade para evitar discriminações com base em raça, gênero ou outro; (iii) agir com transparência e independência, conduzindo e publicando resultados de auditorias internas e abrindo o código-fonte para auditoria externa; (iv) atenção para não prometer o que o algoritmo não pode cumprir, de modo que as declarações para os consumidores devem ser verdadeiras e não enganosas; (v) dizer a verdade cobre como os dados são utilizados; (vi) cuidado para não causar mais danos do que benefícios, o que é considerado uma prática injusta pela FTC; e (vii) responsabilizar-se pelo desempenho do algoritmo adotado[227].

Apesar dessas orientações da FTC, a diversidade de regulamentações estaduais e locais existentes nos EUA "não proporciona segurança jurídica para as autoridades públicas, a indústria e os cidadãos"[228].

Além disso, os EUA também não possuem uma lei abrangente a nível nacional que regule a proteção aos dados pessoais de modo geral, tampouco aos dados biométricos, como ocorre na UE. Contudo, existem algumas leis direcionadas a assuntos específicos, por exemplo, a Lei de Proteção da Privacidade Online das Crianças (*Children's Online Privacy Protection*

---

[225] Ibidem.

[226] "Federal law is required to regulate both commercial and government use of the FRT and establish quality and credibility standards for the facial recognition software" PANAHOV, Huseyn. Why the US Needs Federal Law on Facial Recognition Technology. **Intersect: The Stanford Journal of Science, Technology, and Society**, Stanford University, v. 15, n. 2, p. 1-9, april, 2022. Disponível em: https://ojs.stanford.edu/ojs/index.php/intersect/article/view/2168. Acesso em: 27 abr. 2023. ""When it comes to issues such as safeguards for facial recognition, we have no national law at all," Microsoft president Brad Smith wrote. "We need new laws fit for the future." IBM CEO Arvind Krishna told Biden his company was "ready to work with you" on prohibiting use of the technology for "mass surveillance, racial profiling, or violations of basic human rights and freedoms."." SIMONITE, Tom. Congress Is Eyeing Face Recognition, and Companies Want a Say. **Wired**, New York, 23 nov. 2020. Disponível em: https://www.wired.com/story/congress-eyeing-face-recognition-companies-want-say/. Acesso em: 27 abr. 2023. "Without federal regulation, what we have is patchwork regulation from various states. That's not a good fit in an economy where companies do business nationally," Rowe said." CLARK, Alisson. Why the U.S. needs federal regulation of facial recognition — and how to get it right. **University of Florida News**, 7 dec. 2020. Disponível em: https://news.ufl.edu/2020/12/facial-recognition/. Acesso em: 27 abr. 2023.

[227] JILLSON, Elisa. Aiming for truth, fairness, and equity in your company's use of AI. **Federal Trade Commission**, 2021. Disponível em: https://www.ftc.gov/business-guidance/blog/2021/04/aiming-truth-fairness-equity-your-companys-use-ai. Acesso em: 27 abr. 2023.

[228] MADIEGA; MILDEBRATH, op. cit., p. 32-33.

Rule - COPPA)[229], de 1998, aplicável a empresas que coletam, em *sites* ou outros ambientes *online*, dados pessoais de crianças com menos de 13 anos de idade. A COPPA exige que essas empresas obtenham o consentimento dos pais ou responsáveis legais dessas crianças antes da coleta das informações delas e forneça informações claras e transparentes sobre como esses dados serão usados.

Segundo a Associação Internacional de Profissionais de Privacidade (*International Association of Privacy Professionals* - IAPP), providências foram tomadas para a criação de uma lei federal de privacidade nos EUA, entretanto, ainda sem previsão para a sua conclusão e publicação[230]. Até o momento, existe um esforço conjunto para trabalhar na nova legislação, com numerosos projetos de lei propostos no Congresso que abordam "todas as facetas da privacidade, desde direitos individuais e obrigações comerciais até proteções especiais para informações e acesso confidenciais, registros de autoridades policiais e tecnologias emergentes, como reconhecimento facial e inteligência artificial."[231] Enquanto a lei federal de privacidade e proteção de dados não fica pronta, os estados americanos foram adotando suas próprias leis, como será visto em alguns exemplos a seguir[232].

2.2.1 Legislação estadual sobre dados biométricos nos Estados Unidos: Califórnia, Illinois, Washington e Texas

Nos EUA, a Califórnia é o estado mais desenvolvido em relação a padrões de privacidade. A Lei de Privacidade do Consumidor da Califórnia (*California Consumer Privacy Act* - CCPA)[233], que está em vigor desde 2020, discorre somente sobre dados dos consumidores pessoas físicas residentes na Califórnia (art. 1798.140(g) da CCPA). A definição de "informações pessoais" (art. 1798.140(o) da CCPA) inclui informações que possam ser razoavelmente associadas a um consumidor ou domicílio, direta ou indiretamente, e a Lei

---

[229] FEDERAL TRADE COMMISSION (FTC). 16 CFR Part 312. Children's Online Privacy Protection Act of 1998. **Electronic Code of Federal Regulations (eCFR)**, Federal Trade Commission, 17 jan. 2013. Disponível em: https://www.ecfr.gov/current/title-16/chapter-I/subchapter-C/part-312. Acesso em: 28 abr. 2023.

[230] US Federal Privacy. **International Association of Privacy Professionals (IAPP)**, *[s.d.]*. Disponível em: https://iapp.org/resources/topics/us-federal-privacy/. Acesso em: 27 abr. 2023.

[231] FAZLIOGLU, Müge. US Federal Privacy Legislation Tracker: Introduced in the 117th Congress (2021-2022). **International Association of Privacy Professionals (IAPP)**, dec., 2022. Disponível em: https://iapp.org/resources/article/us-federal-privacy-legislation-tracker/. Acesso em: 27 abr. 2023.

[232] US State Privacy. **International Association of Privacy Professionals (IAPP)**, 2023. Disponível em: https://iapp.org/resources/topics/us-state-privacy/. Acesso em: 27 abr. 2023.

[233] CALIFORNIA (State). California Consumer Privacy Act of 2018. **California Legislative Information**, 2018. Disponível em: https://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?division=3.&part=4.&lawCode=CIV&title=1.81.5. Acesso em: 27 abr. 2023.

especifica vários exemplos de informações pessoais, incluindo dados de geolocalização e informações biométricas. Além disso, a Lei não tem efeitos quando outras leis específicas[234] se aplicam ao caso.

De modo geral, a CCPA prevê aos consumidores o direito de saber quais informações foram coletadas e para quem foram vendidas ou compartilhadas, o direito de solicitar que suas informações sejam apagadas, o direito de se opor à venda de suas informações pessoais, o direito a não discriminação e o direito privado de ação em casos de violações de dados.[235] Dessa maneira, os indivíduos da Califórnia "têm a possibilidade de solicitar essas informações de caráter pessoal (e biométrico) juntamente com outras informações de identificação pessoal que as empresas venham a coletar por conta do reconhecimento facial"[236].

A Lei de Privacidade de Informações Biométricas (*Biometric Information Privacy Act* - BIPA)[237], do estado de Illinois de 2008, é pioneira nos EUA sobre a regulamentação do tratamento de dados pessoais biométricos.[238] Essa lei impõe que as empresas que operam no estado de Illinois com informações biométricas[239] devem respeitar alguns requisitos, dentre eles: (i) disponibilizar informações escritas aos titulares dos dados sobre coleta, compra, armazenamento, finalidade específica e duração do tratamento dos dados biométricos; (ii) coletar uma liberação específica e por escrito para o tratamento, inclusive para divulgação.[240]

---

[234] *Health Insurance Portability and Accountability Act* de 1996 (1798.145(c)(1) da CCPA), *Fair Credit Reporting Act* (1798.145(d) da CCPA), *Gramm-Leach-Bliley Act* (1798.145(e) da CCPA), *Driver's Privacy Protection Act* de 1994 (1798.145(f) da CCPA), e outras. Ibidem.

[235] GOLDMAN, Eric. An Introduction to the California Consumer Privacy Act (CCPA). **Santa Clara University School of Law Legal Studies Research Paper Series**, p. 1-7, 1 jul. 2020. Disponível em: http://dx.doi.org/10.2139/ssrn.3211013. Acesso em: 27 abr. 2023.

[236] PEREIRA, Fábio Luiz Barbosa; SILVA, Cecília Alberton Coutinho. Capítulo 24. A Regulação do Reconhecimento Facial e Seus Impactos para os Setores Público e Privado no Brasil: Uma Análise Comparativa Internacional. In: FRANCOSKI, Denise; TASSO, Fernando. **A Lei Geral de Proteção de Dados Pessoais:** Lgpd: Aspectos Práticos e Teóricos Relevantes no Setor Público e Privado. São Paulo: Editora Revista dos Tribunais, 2021. Disponível em: https://thomsonreuters.jusbrasil.com.br/doutrina/secao/1279975781/capitulo-24-a-regulacao-do-reconhecimento-facial-e-seus-impactos-para-os-setores-publico-e-privado-no-brasil-uma-analise-comparativa-internacional#a-263118690. Acesso em: 37 abr. 2023.

[237] ILLINOIS (State). Civil liabilities (740 ILCS 14/) Biometric Information Privacy Act, of 3 oct. 2008. **Illinois General Assembly**, Springfield, 3 oct. 2008. Disponível em: https://www.ilga.gov/legislation/publicacts/fulltext.asp?Name=095-0994. Acesso em: 27 abr. 2023.

[238] Ler comentários sobre o "BIPA" em: DUBALL, Joseph. The rise of US state-level BIPA: Illinois leads, others catching up. **International Association of Privacy Professionals (IAPP)**, 28 mar. 2023. Disponível em: https://iapp.org/news/a/the-rise-of-us-state-level-bipa-illinois-leads-others-catching-up/. Acesso em: 27 abr. 2023.

[239] BIPA, Section 10: "Definitions. In this Act: "Biometric identifier" means a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry. [...] "Biometric information" means any information, regardless of how it is captured, converted, stored, or shared, based on an individual's biometric identifier used to identify an individual. Biometric information does not include information derived from items or procedures excluded under the definition of biometric identifiers." ILLINOIS (State), op. cit.

[240] BIPA, (740 ILCS 14/15) "(b) No private entity may collect, capture, purchase, receive through trade, or otherwise obtain a person's or a customer's biometric identifier or biometric information, unless it first: (1) informs the subject or the subject's legally authorized representative in writing that a biometric identifier or biometric information is being collected or stored; (2) informs the subject or the subject's legally authorized representative in writing of the specific purpose and length of term for which a biometric identifier or biometric information is

O estado de Washington aprovou, em 2017, o Projeto de Lei Substituto nº 1493 da Câmara (*Engrossed Substitute House Bill No 1493* - ESHB 1493/2017)[241], adicionado ao Título 19, Capítulo 19.375, do Código Revisado de Washington (*Revised Code of Washington* - RCW). Tal legislação visa regular o uso de dados biométricos para fins comerciais. Conforme a seção 2: "(1) Uma pessoa não pode registrar um identificador biométrico em um banco de dados para fins comerciais, sem primeiro notificar, obter consentimento ou fornecer um mecanismo para impedir o uso subsequente de um identificador biométrico para fins comerciais"[242]. Nota-se na legislação que essas exigências não se estendem à coleta, captura, registro ou armazenamento de identificador biométrico para propósitos de segurança.

Ainda, o ESHB 1493 (Seção 2, (3) e (4)) dispõe que, a menos que o titular tenha dado seu consentimento, não é permitido que uma pessoa venda, alugue ou divulgue o identificador biométrico de alguém a terceiros para fins comerciais, exceto em certas circunstâncias específicas listadas na legislação, por exemplo, para fornecer um produto ou serviço solicitado pelo próprio titular ou em resposta a uma ordem judicial ou a obrigações legais. Além disso, aqueles que possuem conscientemente um identificador biométrico devem tomar medidas para protegê-lo contra acesso não autorizado, de modo que só podem retê-lo pelo tempo necessário para cumprir as obrigações legais ou para cumprir o objetivo para os quais os dados foram acessados. O uso ou divulgação do identificador biométrico posterior, diferente dos objetivos originais, necessita de novo consentimento[243].

No início de 2020, o estado de Washington aprovou o Projeto de Lei Substitutivo do Senado nº 6280 (*Engrossed Substitute Senate Bill No 6280* - ESSB 6280/2020)[244], adicionado ao Título 43, Capítulo 43.386, do RCW, relativo à utilização de serviços de reconhecimento facial por agências governamentais estaduais ou locais. Nesse sentido, sempre que essas agências usarem ou pretenderem desenvolver, adquirir ou usar um serviço de reconhecimento facial deverão: (i) apresentar a uma autoridade legislativa um aviso de intenção e especificar a finalidade para a qual a tecnologia será usada; (ii) produzir previamente um relatório de prestação de contas (*Accountability Report*); (iii) permitir ao menos três consultas públicas à

being collected, stored, and used; and (3) receives a written release executed by the subject of the biometric identifier or biometric information or the subject's legally authorized representative." Ibidem.

[241] WASHINGTON. Engrossed Substitute House Bill 1493, of 23 jul. 2017. An act relating to biometric identifiers; and adding a new chapter to Title 19 RCW. **Washington State Legislature**, 65th Legislature, Washington, 23 jul. 2017. Disponível em: https://lawfilesext.leg.wa.gov/biennium/2017-18/Pdf/Bills/Session%20Laws/House/1493-S.sl.pdf. Acesso em: 28 abr. 2023.

[242] "Sec. 2. (1) A person may not enroll a biometric identifier in a database for a commercial purpose, without first providing notice, obtaining consent, or providing a mechanism to prevent the subsequent use of a biometric identifier for a commercial purpose." WASHINGTON, op. cit.

[243] Ibidem.

[244] Ibidem.

comunidade e considerar as questões levantadas; (iv) atualizar o relatório a cada dois anos e submetê-lo a uma autoridade legislativa; e (v) comunicar o relatório ao público com noventa dias de antes de implementar os serviços de reconhecimento facial.

O relatório de prestação de contas referido acima deve conter: (i) informações claras e compreensíveis, contendo o nome do serviço de reconhecimento facial, seu fornecedor e a versão da tecnologia, bem como a descrição das suas capacidades e limitações; (ii) os tipo(s) de *inputs* que a tecnologia utiliza, como os dados são gerados, coletados e processados; (iii) descrição do(s) propósito(s) de uso do serviço, incluindo se é um sistema de decisão final ou de suporte e quais são os benefícios pretendidos; (iv) política de uso e gerenciamento de dados com protocolos específicos nos termos do RCW; (v) procedimentos de teste da agência; (vi) informações sobre taxa de correspondências falsas; (vii) descrição dos impactos potenciais nos direitos e liberdades civis e medidas específicas para mitigar esses impactos[245].

Somado a isso, o ESSB 6280 (Seção 4) exige que as agências garantam a revisão humana significativa quando um serviço de reconhecimento facial é usado para tomar decisões que produzam efeitos legais sobre os indivíduos ou efeitos igualmente significativos, ou seja, aqueles que "resultam na prestação ou negação de serviços financeiros e de empréstimos, moradia, seguro, matrícula escolar, justiça criminal, oportunidades de emprego, serviços de saúde ou acesso a necessidades básicas como alimentos e água, ou que afetem os direitos civis dos indivíduos"[246].

O estado do Texas possui o Código de Negócios e Comércio do Texas (*Texas Business and Commerce Code – BUS&COM*)[247], que, em seu Título 11, Subtítulo A, Capítulo 503: Captura ou Uso de Identificador Biométrico (*Chapter 503: Capture or Use of Biometric Identifier*), adicionado em 2009 pelo Projeto de Lei da Câmara (*House Bill* - HB) nº 2278, exige que a coleta de dados biométricos[248] para fins comerciais somente aconteça após fornecimento de informações prévias e coleta de consentimento do titular.

Em resumo, o curto texto da Lei não permite a venda, aluguel ou divulgação de identificadores biométricos, exceto em situações específicas, como quando o indivíduo

---

[245] WASHINGTON. Engrossed Substitute Senate Bill 6280, of 24 jan. 2020. An act relating to the use of facial recognition services; adding a new chapter to Title 43 RCW; providing an effective date; and providing an expiration date. **Washington State Legislature**, 66th Legislature, Washington, 24 jan. 2020. Disponível em: https://lawfilesext.leg.wa.gov/biennium/2019-20/Pdf/Bills/Senate%20Passed%20Legislature/6280-S.PL.pdf?q=20200331170240. Acesso em: 28 abr. 2023.

[246] Ibidem.

[247] TEXAS. Business and Commerce Code. Chapter 503 Biometric Identifiers, of 1º apr. 2009. **Texas Constitution and Statutes**, Texas, 1º apr. 2009. Disponível em: https://statutes.capitol.texas.gov/Index.aspx. Acesso em: 28 abr. 2023.

[248] "(a) In this section, "biometric identifier" means a retina or iris scan, fingerprint, voiceprint, or record of hand or face geometry." Ibidem.

consente, quando exigido por lei ou quando a divulgação é feita por agência de *law enforcement* para cumprir um mandado. A pessoa detentora desses dados é obrigada a armazenar, transmitir e proteger os identificadores biométricos de maneira cuidadosa. Além disso, os dados devem ser destruídos dentro de um prazo razoável, mas antes de expirar o propósito de coleta ou conforme determinação específica[249].

O Quadro 3 abaixo sintetiza as principais informações que podem ser observadas nas legislações dos estados norte-americanos abordados nesta pesquisa.

Quadro 3 - Principais informações a respeito das legislações sobre proteção de dados da Califórnia, Illinois, Washington e Texas, dos EUA

Estado	**Legislação**	**Assunto**	**Requisitos**		
			Informação ao titular	**Consentimento do titular**	**Relatório**
Califórnia	California Consumer Privacy Act – CCPA	Dados dos consumidores pessoas físicas residentes na Califórnia, incluindo dados biométricos	Sim	N/A[250]	N/A
Illinois	Biometric Information Privacy Act – BIPA	Informações biométrica tratadas por empresas que operam no estado de Illinois	Sim	Sim	N/A
Washington	Revised Code of Washington - RCW - Chapter 19.375 (Engrossed Substitute House Bill No 1493 - ESHB 1493/2017)	Dados biométricos para fins comerciais	Sim	Sim	N/A

[249] TEXAS, op. cit.

[250] A legislação da Califórnia não fala em consentimento para a coleta dos dados, mas garante ao consumidor o direito de opt-out. Ademais, consumidores entre 13 e 16 anos precisam consentir expressamente para a coleta dos seus dados, enquanto que menores de 13 anos precisam da autorização dos pais ou responsáveis.

	Revised Code of Washington - RCW - Chapter 43.386 (Engrossed Substitute Senate Bill No 6280 - ESSB 6280/2020)	Serviços de reconhecimento facial por agências governamentais estaduais ou locais	Sim	N/A	Sim
Texas	Texas Business and Commerce Code – BUS & COM - Chapter 503: Capture or Use of Biometric Identifier	Dados biométricos para fins comerciais	Sim	Sim	N/A

Fonte: criação da autora com base nas legislações estaduais dos EUA.

Conclui-se, pois, que as legislações desses estados apontados no Quadro 3 regulamentam de forma específica os dados biométricos, principalmente em contextos de comércio e consumo, sendo que três delas (Illinois, Washington e Texas) exigem que sejam prestadas informações aos titulares dos dados quanto às operações envolvendo informações biométricas. Enquanto isso, o estado de Washington regulamentou especificamente os serviços de reconhecimento facial pelas agências policiais, exigindo a condução de um relatório de prestação de contas.

Depreende-se, de todo o exposto, que essas disposições apontam relevantes parâmetros teóricos para a proteção de dados biométricos no Brasil, principalmente se conciliados com a LGPD. Além disso, poderão servir de inspiração para futuras regulamentações jurídicas no Brasil, ou mesmo como referências para a Autoridade Nacional de Proteção de Dados (ANPD) em suas eventuais orientações a respeito do uso de sistemas de reconhecimento facial no país.

Os próximos três subtópicos serão destinados ao estudo aprofundado das legislações locais de São Francisco, Boston e Minnesota, cidades de diferentes estados norte-americanos que chamaram a atenção em razão de, dentro dos últimos cinco anos, terem “proibido” o uso de sistemas de reconhecimento facial. A pesquisa, então, procura compreender os termos dessa vedação.

2.2.2 A aquisição de tecnologia de vigilância na cidade de São Francisco, CA

O Conselho de Supervisores da cidade de São Francisco, em 2019, aprovou a Portaria de Aquisição de Tecnologia de Vigilância que proíbe o uso indiscriminado de tecnologias de vigilância, incluindo o reconhecimento facial e exige a publicização dessas tecnologias em posse ou uso pelos departamentos municipais, conforme o que ficou estabelecido no "Capítulo 19B: Aquisição de Tecnologia de Vigilância" do Código Administrativo de São Francisco[251]. O capítulo foi adicionado pela Ordinance No. 107-19, que assim dispõe:

> Determinação municipal que altera o Código Administrativo para exigir que os departamentos da Cidade de São Francisco que adquirirem tecnologia de vigilância, ou que celebrarem acordos para receber informações de tecnologia de vigilância não pertencente à Cidade, submetam à aprovação do Conselho de Supervisores uma Ordem de Política de Tecnologia de Vigilância, com base em uma ou mais políticas desenvolvidas pelo Comitê de Tecnologia da Informação (COIT) e em um Relatório de Impacto de Vigilância. Isso se aplica a qualquer solicitação para apropriação de fundos para a compra de tal tecnologia, para aceitar e gastar fundos de concessão para esse fim, ou de outra forma para adquirir equipamentos ou serviços de tecnologia de vigilância. Além disso, cada departamento da Cidade que possua e opere equipamentos ou serviços de tecnologia de vigilância existentes deve apresentar ao Conselho uma Ordem de Política de Tecnologia de Vigilância proposta que regule o uso da tecnologia de vigilância. A determinação municipal também exige que o Controlador da Cidade, como Auditor de Serviços, audite anualmente o uso de equipamentos ou serviços de tecnologia de vigilância e a conformidade desse uso com uma Ordem de Política de Tecnologia de Vigilância aprovada. O Controlador deve fornecer um relatório de auditoria ao Conselho de Supervisores para revisão (tradução nossa)[252].

Nesse sentido, os departamentos da Cidade de São Francisco poderão adquirir, possuir e operar equipamentos ou serviços de tecnologia de vigilância, ou celebrar acordos para receber informações a partir deles, desde que obtenham por decreto do Conselho de Supervisores (*Board of Supervisors*) a aprovação de uma Política de Tecnologia de Vigilância (*Surveillance Technology Policies*). Para isso, os departamentos deverão submeter Relatório de Impacto de

---

[251] SÃO FRANCISCO. Código Administrativo de São Francisco. Chapter 19B: acquisition of surveillance technology. **American Legal Publishing**, *[s.l.]*, 14 jun. 2019. Disponível em: https://codelibrary.amlegal.com/codes/san_francisco/latest/sf_admin/0-0-0-47320. Acesso em: 21 fev. 2023.

[252] No original: "Ordinance amending the Administrative Code to require that City departments acquiring surveillance technology, or entering into agreements to receive information from non-City owned surveillance technology, submit a Board of Supervisors approved Surveillance Technology Policy Ordinance, based on a policy or policies developed by the Committee on Information Technology (COIT), and a Surveillance Impact Report to the Board in connection with any request to appropriate funds for the purchase of such technology or to accept and expend grant funds for such purpose, or otherwise to procure surveillance technology equipment or services; require each City department that owns and operates existing surveillance technology equipment or services to submit to the Board a proposed Surveillance Technology Policy Ordinance governing the use of the surveillance technology; and requiring the Controller, as City Services Auditor, to audit annually the use of surveillance technology equipment or services and the conformity of such use with an approved Surveillance Technology Policy Ordinance and provide an audit report to the Board of Supervisors." Ibidem.

Vigilância (*Surveillance Impact Report*) ao Comitê de Tecnologia da Informação (*Committee on Information Technology* - COIT)[253], que ajudará a desenvolver a Política que deverá passar pela aprovação do Conselho. A Portaria exige que o COIT ajude os departamentos a desenvolver, revisar e aprovar políticas para todas as tecnologias de vigilância em posse ou em uso por cada departamento da cidade antes de enviar suas recomendações ao Conselho de Supervisores (Seção 19B.2 (b))[254].

Em suma, para cada tecnologia de vigilância, os departamentos da cidade são obrigados a criar um Relatório de Impacto de Vigilância, uma Política de Tecnologia de Vigilância e Relatórios de Impacto Anuais. Assim, o uso de "tecnologias de vigilância, como drones ou leitores automáticos de placas de carros, passa a ser submetido a um rigoroso processo de avaliação pela Câmara de Supervisão de São Francisco"[255].

Convém esclarecer que, para fins do decreto, uma "Tecnologia de Vigilância" é definida como:

> um software, dispositivo eletrônico, sistema usando um dispositivo eletrônico ou dispositivo semelhante usado, projetado ou principalmente destinado a coletar, reter, processar ou compartilhar informações de áudio, eletrônicas, visuais, de localização, térmicas, biométricas, olfativas ou similares, especificamente associadas ou capaz que possam ser associadas a qualquer indivíduo ou grupo (Seção 19B.1)[256].

Compreende-se, pois, que os sistemas de reconhecimento facial estão contemplados na descrição de tecnologias de vigilância da legislação de São Francisco.

O Relatório de Impacto de Vigilância, conforme as definições apresentadas no Capítulo 19B do Código Administrativo de São Francisco, deve conter, pelo menos, as seguintes informações (Seção 19B.1): (i) descrição detalhada da tecnologia de vigilância proposta e como ela funciona, incluindo informações do fabricante; (ii) informações sobre a(s) finalidade(s) para a qual a tecnologia de vigilância será empregada; (iii) se aplicável, informações sobre o(s) local(is) onde a tecnologia de vigilância será implantada e as estatísticas criminais para cada um desses locais; (iv) avaliação que identifica potenciais impactos sobre as liberdades e direitos

---

[253] No site do Comitê de Tecnologia da Informação (COIT) de São Francisco, Califórnia, Estados Unidos, é possível acessar a lista dos departamentos da cidade e um inventário com todas as Políticas de Tecnologia de vigilância e Relatórios de Impacto futuros e concluídos, bem como um inventário com Relatórios Anuais de Vigilância concluídos para as políticas aprovadas pelo Conselho de Supervisores. Disponível em: https://sf.gov/departments/committee-information-technology-coit. Acesso em: 24 fev. 2023.

[254] SÃO FRANCISCO, op. cit.

[255] BIONI, Bruno R.; RIELLI, Mariana; LUCIANO, Maria. Regulação de reconhecimento facial em São Francisco. **Jota**: *[s.l.]*, 2019. Disponível em: https://www.jota.info/opiniao-e-analise/colunas/agenda-da-privacidade-e-da-protecao-de-dados/regulacao-de-reconhecimento-facial-em-sao-francisco-25062019. Acesso em: 27 abr. 2023.

[256] SÃO FRANCISCO, op. cit.

civis e que discute planos para proteger os direitos do público; (v) descrição dos custos fiscais da tecnologia de vigilância, incluindo a compra inicial, pessoal e outros custos contínuos, bem como quaisquer fontes atuais ou potenciais de financiamento; (vi) se o uso ou a manutenção da tecnologia exigirá que os dados coletados pela tecnologia sejam manipulados ou armazenados por um fornecedor terceirizado continuamente; e (vii) se houver, resumo da experiência de outras entidades governamentais com a tecnologia proposta, incluindo informações sobre sua eficácia e quaisquer problemas ou falhas conhecidos, incluindo abusos de direitos e liberdades civis[257].

Por sua vez, a Política de Tecnologia de Vigilância, a ser aprovada pelo Conselho de Supervisores, deve incluir (Seção 19B.1): (i) informações sobre o produto e serviços abordados pela tecnologia de vigilância, incluindo a identidade do fornecedor; (ii) a(s) finalidade(s) para a qual os equipamentos ou serviços de tecnologia de vigilância são propostos para aquisição e o(s) tipo(s) de dado(s) que podem ser coletados; (iii) informações sobre os usos autorizados, as regras e processos necessários antes de tal uso, bem como os usos proibidos; (iv) descrição das formas em que as informações são armazenadas, copiadas e/ou acessadas; (v) as categorias e títulos específicos de indivíduos autorizados a acessar ou usar as informações coletadas; (vi) mecanismos de proteção contra acesso não autorizado; (vii) período de retenção das informações e motivo; (viii) como as informações coletadas podem ser acessadas ou usadas pelo público; (ix) quais agências governamentais, departamentos, divisões ou unidades que podem receber dados coletados pela tecnologia de vigilância operada pelo departamento, incluindo sua justificativa; (x) qual será o treinamento necessário para qualquer indivíduo autorizado a usar a tecnologia de vigilância ou acessar informações coletadas; (xi) mecanismos para garantir que a política seja seguida; (xii) procedimentos para registrar reclamações, questionamentos ou preocupações do público e como o departamento irá responder a isso.[258] Em geral, a Política de Tecnologia de Vigilância é uma importante medida de transparência e responsabilidade que ajuda a garantir que a tecnologia de vigilância seja usada de maneira responsável e de acordo com a lei.

De acordo com a Seção 19B.4 “Padrão de Aprovação”, o Conselho de Supervisores só aprovará uma Política de Tecnologia de Vigilância se concluir que os benefícios da tecnologia serão maiores do que seus custos, além de considerar se a política é capaz de proteger os direitos e liberdades civis. O Conselho também irá considerar se os usos da tecnologia de vigilância não serão discriminatórios ou prejudiciais para alguma comunidade ou grupo específico. Ou seja,

[257] SÃO FRANCISCO, op. cit.
[258] Ibidem.

antes da aprovação, será preciso ter certeza de que a tecnologia é benéfica, justa, não viola direitos e/ou discrimina pessoas ou grupos de pessoas[259].

Os departamentos que, antes da data de vigência da determinação municipal, possuíam e utilizavam tecnologia de vigilância tiveram prazo de 60 dias, a partir da data de vigência, para apresentar um inventário ao COIT, bem como, 180 dias, prorrogáveis por mais 90 dias, para apresentar proposta de Política de Tecnologia de Vigilância ao Conselho de Supervisores para revisão e aprovação (Seção 19B.5)[260].

Além disso, todo departamento que obtiver aprovação para a aquisição de tecnologia de vigilância deve enviar ao Conselho e ao COIT um Relatório Anual de Vigilância para cada tecnologia e disponibilizá-lo em seu site, dentro de 12 meses após a aprovação da Política aplicável e anualmente[261].

Algumas "circunstâncias exigentes" (*demanding circumstances)* permitem que um departamento adquira ou utilize temporariamente uma tecnologia de vigilância sem que precise seguir as disposições do Capítulo 19B do Código Administrativo de São Francisco. No entanto, o departamento deverá, conforme a Seção 19B.7: (i) deixar de usar a tecnologia dentro de sete dias ou quando as circunstâncias exigentes terminarem, o que ocorrer primeiro; (ii) guardar e manter apenas os dados relacionados às circunstâncias exigentes e descartar quaisquer dados irrelevantes para uma investigação em andamento, a menos que sua retenção seja (a) autorizada por um tribunal com base em uma constatação de causa provável de que constitui prova de um crime; ou (b) de outra forma exigida em lei; (iii) não divulgar informações a terceiros, a menos que a divulgação seja autorizada da mesma forma que os itens (a) e (b) acima expostos; (iv) apresentar um relatório ao Conselho de Supervisores dentro de 60 dias após início das circunstâncias exigentes; e (v) qualquer tecnologia de vigilância temporariamente adquirida nessas circunstâncias deve ser devolvida no prazo de sete dias após a conclusão das exigências, a menos que seja adquirida de acordo com os requisitos de todo o Capítulo 19B[262].

Como visto até aqui, o Capítulo 19B do Código Administrativo de São Francisco, restringe, por meio da imposição de requisitos, a aquisição e o uso de tecnologias de vigilância pelos departamentos da cidade. Além disso, as empresas privadas não são diretamente proibidas pela portaria de usar tecnologia de reconhecimento facial em São Francisco, embora possam

[259] SÃO FRANCISCO, op. cit.
[260] Ibidem.
[261] Ibidem.
[262] Ibidem.

estar sujeitas a outras leis e regulamentações aplicáveis ao caso, como as de proteção à privacidade e à segurança dos dados pessoais em nível estadual e federal.

2.2.3 O uso de sistemas de vigilância facial na cidade de Boston, MA

No estado de Massachusetts, a cidade de Boston, desde 2020, proíbe o uso de qualquer sistema de vigilância facial ou de informações derivadas desses sistemas pelos departamentos e funcionários municipais, conforme dispõe o item 62, do Capítulo XVI, do Código Municipal da Cidade de Boston:

> 16-62 PORTARIA QUE PROÍBE A TECNOLOGIA DE VIGILÂNCIA FACIAL EM BOSTON.
> a. Definições.
> "Boston" significa qualquer departamento, agência, escritório e/ ou divisão subordinada da cidade de Boston.
> "Oficial de Boston" significa qualquer pessoa ou entidade que atue em nome da cidade de Boston, incluindo qualquer oficial, funcionário, agente, contratante, subcontratado ou fornecedor.
> (...)
> b. Proibição do uso de vigilância facial pela cidade.
> 1. Será ilegal para Boston ou qualquer funcionário de Boston:
> (a) Obter, reter, possuir, acessar ou usar (i) qualquer sistema de vigilância facial ou (ii) informações derivadas de um sistema de vigilância facial;
> (b) Celebrar um contrato com terceiros com o objetivo de obter, reter, possuir, acessar ou usar, por ou em nome da Boston ou de qualquer funcionário da Boston, qualquer sistema de vigilância facial; ou
> (c) Emitir qualquer permissão ou celebrar qualquer outro contrato que autorize terceiros, em nome da Boston ou de qualquer funcionário da Boston, a obter, reter, possuir, acessar ou usar (i) qualquer sistema de vigilância facial ou (ii) informações derivadas de um sistema de vigilância facial[263].

Apesar da proibição expressa, a determinação legal prevê algumas exceções permissivas para o uso de vigilância facial pela cidade ou por oficiais de Boston, como: (i) usar evidências relacionadas à investigação de um crime específico, desde que não tenham sido geradas por ou a pedido da cidade de Boston ou de qualquer funcionário da cidade; (ii) obter ou possuir

[263] No original: “a. Definitions. "Boston" shall mean any department, agency, bureau, and/or subordinate division of the City of Boston. "Boston official" shall mean any person or entity acting on behalf of the City of Boston, including any officer, employee, agent, contractor, subcontractor, or vendor. (...) b. Ban on City use of face surveillance. 1. It shall be unlawful for Boston or any Boston official to: (a) Obtain, retain, possess, access, or use (i) any face surveillance system, or (ii) information derived from a face surveillance system; (b) Enter into an agreement with any third party for the purpose of obtaining, retaining, possessing, accessing, or using, by or on behalf of Boston or any Boston official any face surveillance system; or (c) Issue any permit or enter into any other agreement that authorizes any third party, on behalf of Boston or any Boston official, to obtain, retain, possess, access, or use (i) any face surveillance system, or (ii) information derived from a face surveillance system.” BOSTON. City of Boston Municipal Code. **American Legal Publishing**, *[s.l.]*, 2020. Disponível em: https://codelibrary.amlegal.com/codes/boston/latest/boston_ma/0-0-0-18988. Acesso em: 21 fev. 2023.

dispositivo eletrônico para fins probatórios ou dispositivo eletrônico que realiza vigilância facial com o único propósito de autenticação do usuário; (iii) usar o reconhecimento facial em um dispositivo eletrônico de propriedade de Boston ou de qualquer funcionário de Boston, com o único objetivo de autenticação do usuário; (iv) utilizar meios de comunicação social ou software de comunicação ou aplicações para comunicar com o público, desde que não inclua qualquer vigilância facial; (v) utilizar software de redação automatizado que não tenha a capacidade de realizar vigilância facial; ou (vi) quando em conformidade com a Lei Nacional de Assistência à Busca de Crianças[264].

Além disso, Boston ainda possui disposições legais no item 63, do Capítulo XVI, do seu Código Municipal, para supervisão em relação à aquisição e uso de tecnologia de vigilância e dados de vigilância pelos departamentos e oficiais da cidade, que são assim considerados: a Polícia, Escolas Públicas, Comissão de Saúde Pública, Guardas Florestais do Departamento de Parques, Autoridade de Habitação, Serviços de Proteção Municipal e Escritório de Gerenciamento de Emergências. Nesse sentido, a portaria dispõe:

> 16-63 PORTARIA SOBRE SUPERVISÃO DE VIGILÂNCIA E COMPARTILHAMENTO DE INFORMAÇÕES
> 16-63.1 Finalidade.
> O objetivo desta portaria é fornecer responsabilidade, transparência e supervisão em relação à aquisição e uso de tecnologia de vigilância e dados de vigilância pela cidade de Boston e suas agências e oficiais, e proteger a privacidade, direitos civis e justiça racial e imigrante enquanto permitindo o uso adequado para auxiliar na melhoria da prestação de serviços e da segurança pública[265].

Os departamentos e oficiais de Boston acima dispostos possuem permissão para o uso temporário de "Tecnologia de Vigilância em Circunstâncias Exigentes" (*Surveillance Technology in Exigent Circumstances*) sem seguir todas as disposições da portaria por até 30 dias antes da aquisição ou uso permanente. No entanto, passado esse período e adquirida a tecnologia, deverão cumprir várias obrigações, incluindo: (i) a notificação da aquisição e uso, por escrito, à Câmara Municipal, dentro de 30 dias após o término das circunstâncias exigentes; (ii) a apresentação de um Relatório de Impacto da Tecnologia de Vigilância e, se necessário, uma Política de Uso de Vigilância Específica da Tecnologia à Câmara Municipal, dentro de 30 dias (prorrogáveis) após o término das circunstâncias exigentes; (iii) a inclusão dessa tecnologia

[264] BOSTON, op. cit.
[265] No original: "16-63 ORDINANCE ON SURVEILLANCE OVERSIGHT AND INFORMATION SHARING 16-63.1 Purpose. The purpose of this ordinance is to provide accountability, transparency, and oversight regarding the acquisition and use of Surveillance Technology and Surveillance Data by the City of Boston and its agencies and officers, and to protect privacy, civil rights, and racial and immigrant justice while allowing for appropriate use to assist in the charge of improving delivery of services and public safety." Ibidem.

de vigilância no próximo Relatório Anual de Fiscalização do Departamento ou Órgão a ser enviado à Câmara Municipal após o término dessas circunstâncias exigentes; e (iv) a disponibilização pública do Relatório de Impacto e da Política de Uso no site da cidade após o envio à Câmara Municipal. Ambos os documentos serão melhor especificados adiante[266].

Segundo o item 63.3(c) do Capítulo XVI, o Prefeito deverá submeter ao Conselho Municipal, para revisão e aprovação, uma proposta de Política de Uso de Vigilância aplicável a cada departamento municipal listado acima que possua ou use tecnologia de vigilância. Caso a Câmara Municipal não aprove a política, ela será enviada ao Conselho Consultivo de Supervisão de Vigilância, que fará recomendações de melhorias ao Prefeito para modificações e nova submissão[267].

A Política de Uso de Vigilância deve especificar o seguinte: (i) a finalidade da tecnologia; (ii) os usos autorizados e proibidos; (iii) os dados coletados; (iv) quem pode acessar dados; (v) as salvaguardas contra acesso não autorizado, incluindo, entre outros, mecanismos de criptografia, controle de acesso e supervisão de acesso; (vi) informações sobre o período de retenção de dados, incluindo motivo, processo de exclusão e condições de retenção além do período; (vii) se e como podem ser acessados pelo público; (viii) informações sobre compartilhamento de dados e obrigações impostas a terceiros; (ix) o treinamento, se houver, oferecido a terceiros; (x) os mecanismos de fiscalização para cumprimento da política, incluindo a indicação de pessoal designado; (xi) os estatutos, regulamentos ou precedentes legais, se houver, que regem o uso de dados e tecnologias de vigilância; e (xii) as considerações especiais relacionados aos Direitos da Criança[268].

A portaria exige que o departamento municipal que pretenda adquirir nova tecnologia de vigilância ou usar tecnologia de vigilância para um propósito não aprovado anteriormente deve obter a aprovação do Conselho. O processo para obter a aprovação de nova aquisição e uso envolve a apresentação de um Relatório de Impacto da Tecnologia de Vigilância e, se necessário, uma Política de Uso de Vigilância Específica da Tecnologia caso a solicitação seja diferente das normas da Política de Uso de Vigilância para tecnologias anteriormente aprovadas. O departamento deve enviar o relatório ao Prefeito para análise e aprovação, que então deverá encaminhar solicitação à Câmara Municipal[269].

---

[266] BOSTON, op. cit.
[267] Ibidem.
[268] Ibidem.
[269] Ibidem.

O relatório deve descrever a tecnologia de vigilância e como ela funciona, suas finalidades propostas, o tipo de vigilância que conduzirá e quais dados de vigilância serão coletados, incluindo quais entidades podem ter acesso aos dados e em quais circunstâncias. Também necessita constar no relatório o local de implementação da tecnologia de vigilância, uma descrição dos direitos de privacidade e anonimato afetados e um plano de mitigação descrevendo como o uso do equipamento será regulado para proteger esses direitos e limitar o risco de abuso. Por último, o relatório precisa apresentar os potenciais impactos na privacidade da cidade e nos direitos e liberdades civis de quaisquer indivíduos, comunidades ou grupos, além de um plano para lidar com esses impactos, bem como a estimativa de custos fiscais e uma explicação de como a Política de Uso de Vigilância se aplicará a tecnologia de vigilância e, se não for suficientemente aplicável, explicação sobre a aplicabilidade da Política de Uso de Vigilância Específica da Tecnologia[270].

Os departamentos de Boston que tiveram a aprovação para o uso de Tecnologia de Vigilância ou Dados de Vigilância devem enviar ao Prefeito um Relatório Anual de Vigilância, que deverá ser encaminhado à Câmara Municipal e ser disponibilizado publicamente no site da cidade após o envio.

Os elementos que devem estar presentes no Relatório Anual de Vigilância são (item 16-63.5(c)): (i) descrição de como a tecnologia de vigilância foi usada, incluindo se capturou imagens, sons ou outras informações sobre membros do público que não são suspeitos de envolvimento em conduta ilegal; (ii) se e com que frequência os dados adquiridos foram compartilhados com autoridades locais, estaduais e federais, o nome de qualquer entidade receptora, os tipos de dados divulgados e a justificativa para a divulgação; (iii) resumo das reclamações ou preocupações da comunidade, se houver; (iv) resultados de auditorias internas, informações sobre violações da Política de Uso de Vigilância e ações tomadas em resposta; (v) contabilidade detalhada para saber a eficácia em alcançar o propósito identificado para uso da tecnologia; (vi) número de solicitações de registros públicos recebidas pela Prefeitura buscando documentos relativos a tecnologias aprovadas no ano anterior; (vii) estimativa dos custos anuais totais e as fontes de financiamento do próximo ano, se conhecida; (viii) se os direitos e liberdades civis de quaisquer comunidades ou grupos são desproporcionalmente afetados; e (ix) divulgação de quaisquer novos acordos feitos nos últimos doze meses com entidades não municipais que possam incluir a aquisição, compartilhamento ou uso de tecnologia de vigilância ou os dados de vigilância fornecidos por ela[271].

---

[270] Ibidem.
[271] BOSTON, op. cit.

Pelo exposto, observa-se que a cidade de Boston proíbe o uso de tecnologias de vigilância facial por parte dos departamentos municipais e funcionários da cidade, com exceção de alguns departamentos que poderão adquirir e utilizar tecnologias de vigilância, mediante autorização do Conselho Municipal a partir de uma Política de Uso de Vigilância aprovada e de relatórios apresentados anualmente.

Tanto a regulamentação de São Francisco quanto a de Boston compartilham o objetivo comum de proteger a privacidade dos cidadãos em relação à vigilância viabilizada pelas tecnologias. Ambas as cidades exigem que os departamentos municipais obtenham aprovação antes de adquirir ou utilizar tecnologia de vigilância, bem como que apresentem políticas de uso, relatórios de impacto e relatórios anuais de fiscalização para monitoramento dessas tecnologias. Ademais, as duas regulamentações abordam tanto sobre a tecnologia de reconhecimento facial quanto sobre outras formas de tecnologias de vigilância e exigem a publicização dos documentos aprovados para manter o público informado sobre seu uso.

Entretanto, apesar das semelhanças, as determinações legais também diferem em alguns aspectos. O escopo de aplicação da portaria de São Francisco considera que todos os departamentos da cidade podem regularizar a sua utilização de tecnologias de vigilância por meio da aprovação do Conselho de Supervisores conforme os requisitos legais abordados anteriormente, enquanto que a legislação de Boston proíbe o uso de tecnologias de vigilância, especificamente do tipo facial, por todos os departamentos e oficiais da cidade, com exceção de alguns departamentos, principalmente as forças policiais, escolas e saúde pública, que podem adquirir e utilizar tecnologias de vigilância de qualquer tipo, desde que autorizado pela Câmara Municipal, considerando as imposições legais.

Nota-se que São Francisco e Boston exigem relatórios anuais a respeito das tecnologias, entretanto, destaca-se que São Francisco não discrimina as exigências desse relatório, enquanto que Boston tem uma preocupação significativa com o levantamento de informações após a implementação da tecnologia, exigindo análises de erros, eficiência, reclamações, custos e impactos em direitos e liberdades civis.

2.2.4 A utilização de tecnologia de reconhecimento facial na cidade de Minnesota, MN

No estado de Minnesota, a cidade de Minneapolis aprovou, em 2021, a *Ordinance* No. 2021-006[272], que alterou o Código de Ordenações de Minneapolis relativo à "Administração: Governança da Informação", acrescentando um novo artigo intitulado "Tecnologia de Reconhecimento Facial" (Artigo II, Capítulo 41, Título 2, do Código), que dispõe que:

> 41.120 - A Cidade não deve adquirir ou utilizar tecnologia de reconhecimento facial.
> (a) Salvo expressamente permitido por este Artigo, será ilegal para a Cidade:
> (1) Adquirir, obter ou reter tecnologia de reconhecimento facial;
> (2) Celebrar um contrato com um terceiro para fins de adquirir, obter ou reter acesso da Cidade à tecnologia de reconhecimento facial;
> (3) Celebrar um contrato com um terceiro que auxilie o terceiro a desenvolver, melhorar ou expandir as capacidades de tecnologia de reconhecimento facial ou forneça ao terceiro acesso a informações que o ajudem a fazê-lo.
> (b) Salvo expressamente permitido por este Artigo, será ilegal para a Cidade solicitar, adquirir ou usar intencionalmente ou conscientemente informações obtidas por meio da tecnologia de reconhecimento facial. A aquisição ou uso inadvertido ou não intencional de informações obtidas por meio da tecnologia de reconhecimento facial pela Cidade não violará esta subseção. No entanto, após a descoberta da aquisição ou uso inadvertido ou não intencional de informações obtidas por meio da tecnologia de reconhecimento facial, as informações não serão mais utilizadas e serão excluídas na medida do permitido por lei. (tradução nossa)[273].

O artigo, apesar de proibir a aquisição e o uso de tecnologia de reconhecimento facial, apresenta algumas exceções permissivas em certas circunstâncias, como quando for para (i) fins de autenticação de usuários em dispositivos eletrônicos; (ii) acesso a mídias sociais ou aplicativos de comunicação que incluam essa tecnologia; (iii) redação automatizada ou semi automática; (iv) custódia ou controle de dispositivos eletrônicos que incluem a tecnologia apenas para fins probatórios; ou (v) controle de acesso de funcionários em locais de trabalho da cidade que não são abertos ao público[274].

---

[272] MINNEAPOLIS (MN). Ordinance No. 2021-006. Amending Title 2, Chapter 41 of the Minneapolis Code of Ordinances relating to Administration: lnformation Governance. **City of Minneapolis**, 2021. Disponível em: https://lims.minneapolismn.gov/Download/MetaData/20406/2021-006_Id_20406.pdf. Acesso em: 21 fev. 2023.

[273] No original: "41.l20. - City Not to Acquire or Use Facial Recognition Technology. (a) Unless expressly permitted by this Article, it shall be unlawful for the City to: (1)Acquire, obtain, or retain facial recognition technology; (2) Enter into a contract with a third party for the purpose of acquiring, obtaining, or retaining City access to facial recognition technology; or (3) Enter into a contract with a third party that assists the third party in developing, improving, or expanding the capabilities of facial recognition technology or provides the third party with access to information that assists the third party in doing so. (b) Unless expressly permitted by this Article, it shall be unlawful for the City to intentionally or knowingly request, acquire, or use information obtained from facial recognition technology. The City's inadvertent or unintentional acquisition or use of information obtained from facial recognition technology shall not violate this subsection. However, upon discovery of the inadvertent or unintentional acquisition or use of information obtained from facial recognition technology, the information shall not be further used and shall be deleted to the extent permitted by law." Ibidem.

[274] MINNEAPOLIS (MN). Minneapolis Code of Ordinances. **Order of the City Council**, Conteúdo online atualizado em 6 de fev. de 2023. Disponível em: https://library.municode.com/mn/minneapolis/codes/code_of_ordinances?nodeId=COOR_TIT2AD_CH41INGO_ARTIIFARETE. Acesso em: 02 mar. 2023.

Além disso, prevê que a aquisição, obtenção ou manutenção de tecnologia de reconhecimento facial não será considerada uma infração ao artigo se atender, cumulativamente, às seguintes condições: (i) ser um recurso integrado em um software, produto ou dispositivo; (ii) as outras funções sejam necessárias ou benéficas para o desempenho das funções da cidade; (iii) a tecnologia não pode ter sido adquirida com o objetivo de realizar o reconhecimento facial; (iv) a tecnologia de reconhecimento facial não pode ser excluída do software, produto ou dispositivo; (v) a cidade não utiliza a tecnologia de reconhecimento facial; e, por fim, (vi) o Conselho Municipal deve ser notificado quando um departamento da cidade desejar ou tentar adquirir a tecnologia[275].

Por último, o artigo prevê que a Câmara Municipal de Minneapolis pode permitir exceções adicionais aos requisitos estabelecidos mediante solicitação e aprovação do Conselho, desde que sejam consistentes com os objetivos de prevenção à discriminação e promoção da privacidade, transparência e confiança pública. As exceções concedidas devem ser monitoradas e relatadas, em um resumo presente em relatório anual, ao secretário municipal, sem incluir informações de identificação pessoal ou informações que não sejam públicas de acordo com os Estatutos de Minnesota[276].

Nesse sentido, a solicitação ao conselho deverá conter (i) a explicação da necessidade do caso de exceção, (ii) a descrição de como a tecnologia ou a informação será utilizada e (iii) um plano para monitorar seu uso conforme os parâmetros aprovados. A partir dessa solicitação de exceção, o conselho realizará uma audiência pública e poderá aprovar a proposta se entender que está de acordo com os objetivos estabelecidos (de prevenção à discriminação e promoção de privacidade, transparência e confiança pública), além de poder exigir revisões do plano proposto para monitoramento da tecnologia[277].

A lei da cidade de Minnesota não permite que dados ou informações decorrentes de violação dessa regulamentação sejam aceitos como prova em qualquer processo legislativo, administrativo, regulatório ou outro sob a jurisdição da cidade. Além disso, após a descoberta de uma violação, o departamento ou funcionário da cidade deverá realizar a exclusão dos dados obtidos ilegalmente e fornecer um resumo, ao secretário municipal, contendo a natureza da violação e as medidas tomadas para excluir os dados. Qualquer oficial ou funcionário da cidade que viole intencionalmente a regulamentação será responsabilizado por suas ações, estando

[275] Ibidem.
[276] Ibidem.
[277] Ibidem.

sujeito à disciplina estabelecida por acordo de negociação coletiva aplicável ou outras leis, políticas e procedimentos aplicáveis[278].

Qualquer pessoa pode apresentar uma petição judicial ("*writ of mandate*"), de acordo com o Estatuto de Minnesota (Capítulo 586), para garantir o cumprimento dessa regulamentação, mas antes a cidade deve ser notificada primeiro sobre a suposta infração e dar a oportunidade de corrigir a violação dentro de um prazo de trinta dias[279].

Ao adotar e fazer cumprir o artigo sobre "Tecnologia de Reconhecimento Facial" em questão, a cidade está agindo para preservar e proteger a segurança, a saúde e o bem-estar geral da população. No entanto, ela não assume a responsabilidade por quaisquer danos que possam ser causados a terceiros em caso de descumprimento do artigo por parte de seus oficiais ou funcionários. Em outras palavras, a cidade não será responsável por indenizar alguém que alegue ter sido prejudicado em decorrência de violações do artigo cometidas pelos funcionários ou agentes da cidade. Além disso, o fato de a cidade não assumir a responsabilidade por quaisquer danos não significa que ela está isenta de cumprir o artigo, ou seja, a cidade ainda tem a obrigação de cumprir as regras e requisitos estabelecidos pelo artigo, sob pena de ser obrigada a fazê-lo por meio de um mandado de segurança[280].

É exigido que o escrivão da cidade forneça um relatório escrito anualmente ao comitê apropriado do Conselho da cidade. O relatório deverá abordar o cumprimento da cidade com relação ao artigo, bem como um resumo de quaisquer violações identificadas e as medidas tomadas para corrigi-las, sem que identifique qualquer pessoa envolvida ou inclua informações de identificação pessoal ou informações que não sejam públicas de acordo com os Estatuto de Minnesota (Capítulo 13)[281].

Os três exemplos de regulamentações de cidades de diferentes estados dos Estados Unidos possibilitam algumas observações. Em primeiro lugar, enquanto São Francisco regulamenta uma ampla gama de tecnologias de vigilância e Boston proíbe o uso de tecnologias de vigilância do tipo facial, Minneapolis especificamente dispõe sobre a tecnologia de reconhecimento facial. Embora exista essa diferença, é possível considerar que os três códigos municipais englobam os sistemas de reconhecimento facial.

O segundo ponto observável é que todas as três cidades implementaram regras para o uso dessas tecnologias pelos departamentos municipais e seus funcionários, sem

[278] MINNEAPOLIS (MN), op. cit.
[279] Ibidem.
[280] Ibidem.
[281] Ibidem.

direcionamento para a iniciativa privada, o que significa crescente preocupação, principalmente, com o uso indevido dessa ferramenta direcionada para a vigilância por órgãos e autoridades públicas.

A terceira consideração diz respeito às exceções. As três previsões legais acima expostas trazem hipóteses que permitem excepcionalmente o uso do reconhecimento facial pelos departamentos e funcionários dos municípios, o que indica que a proibição não é absoluta. Contudo, a cidade de Minnesota é mais rigorosa e, portanto, mais restritiva em relação às hipóteses permissivas.

Outro ponto a ser observado decorre dos documentos que devem ser produzidos como forma de adequação com as disposições legais, como relatórios e políticas, previstos nas três cidades. O Quadro 4 abaixo demonstra a comparação entre os conteúdos mínimos exigidos, demonstrando o grau de rigor de cada um.

Quadro 4 - Comparação entre os conteúdos mínimos exigidos em documentos de impacto de tecnologias de vigilância nas legislações de São Francisco, Boston e Minnesota, dos EUA

	Cidades dos Estados Unidos que regulamentaram o reconhecimento facial				
Informações mínimas	**SF - Relatório**	**SF - Política**	**Boston - Relatório**	**Boston - Política**	**Minneapolis - Relatório**
Descrição detalhada de funcionamento e informações do fabricante	X	X	X	-	-
Finalidade(s)	X	X	X	X	-
Tipos de dados coletados	-	X	X	X	-
Usos autorizados ou proibidos e regras de uso	-	X	X	X	-
Formas de armazenamento e acesso	-	X	-	-	-
Quem pode acessar e/ou coletar as informações	-	X	X	X	-
Mecanismos contra acessos não autorizados	-	X	-	X	-
Período de retenção das informações e motivo	-	X	-	X	-
Como as informações	-	X	-	X	-

coletadas podem ser acessadas ou usadas pelo público					
Quais agências governamentais, departamentos, divisões ou unidades que podem receber os dados coletados e motivo	-	X	X	-	-
Informações sobre compartilhamento de dados e obrigações impostas a terceiros	-	-	-	X	-
Treinamento necessário de pessoal	-	X	-	X	-
Mecanismos de fiscalização para cumprimento com o documento	-	X	-	X	-
Procedimentos para registrar reclamações, questionamentos ou preocupações do público e modelo de resposta	-	X	-	-	-
Se aplicável, local de implementação e as estatísticas criminais para cada um desses locais	X	-	X	-	-
Avaliação de impactos sobre as liberdades e direitos civis e quais os planos para sua proteção	X	-	X	-	-
Considerações especiais relacionados aos direitos da criança	X	-	-	X	-
Os estatutos, regulamentos ou precedentes legais, se houver, que regem o uso de dados e tecnologias de vigilância	X	-	-	X	-
Descrição dos custos e fontes de financiamento	X	-	X	-	-
Se aplicável, fornecedor terceirizado que manipula e armazena os dados	X	-	-	-	-

Se houver, resumo da experiência de outras entidades governamentais, incluindo informações sobre sua eficácia, problemas ou falhas conhecidos, incluindo abusos de direitos civis e liberdades civis	X	-	-	-	-
Cumprimento da cidade com a regulamentação, resumo de violações identificadas e as medidas corretivas, sem incluir informações de identificação pessoal	-	-	-	-	X

Fonte: criação da autora com base nas legislações sobre tecnologias de vigilância e reconhecimento facial das cidades de São Francisco, Boston e Minneapolis (EUA).

Ao passo que a legislação de Minnesota é a mais restritiva quanto às hipóteses em que permite o uso de tecnologia de reconhecimento facial, o relatório anual exigido se refere ao cumprimento da cidade com os termos da legislação de não utilização do reconhecimento facial e, em caso de violação, que seus termos sejam descritos junto com as medidas corretivas. Enquanto isso, ao passo que as legislações das cidades de São Francisco e Boston são mais flexíveis quanto às hipóteses de uso de tecnologias de vigilância, ambas requerem a elaboração de relatórios e políticas mais complexas, munidas de informações detalhadas e direcionadas justamente para a utilização da tecnologia (e não para a ausência dela).

3 A TUTELA JURÍDICA DOS DADOS BIOMÉTRICOS FACIAIS NO BRASIL E A ADOÇÃO DE BOAS PRÁTICAS PELO SETOR PRIVADO

3.1 A CONSTITUIÇÃO FEDERAL E OUTRAS LEIS FEDERAIS

Dentro do ordenamento jurídico brasileiro, os direitos fundamentais a não discriminação - de origem, raça, sexo, cor, idade e quaisquer outras formas - (art. 3º, IV, CF), a intimidade, a vida privada, a honra, a imagem (art. 5º, X, CF) e a proteção de dados (art. 5º, LXXIX, CF)[282] são um conjunto de garantias básicas da Constituição Federal de 1988[283] que estabelecem parâmetros cruciais para o desenvolvimento e uso da tecnologia de reconhecimento facial. Enquanto isso, as regras específicas relevantes que dão maior efeito aos direitos fundamentais são espalhadas por diferentes níveis da ordem jurídica, mas a sua aplicabilidade deve sempre ser coerente com a Constituição, respeitando esses direitos.

Até o momento, não há uma regulamentação jurídica específica sobre a utilização de dados biométricos ou tecnologia de reconhecimento facial ou inteligência artificial a nível federal no Brasil. Entretanto, a Lei Geral de Proteção de Dados (Lei nº 13.709/2018 - LGPD)[284], que passou a vigorar em 2020, acabou regulando, de modo geral, os dados biométricos ao lhes conferir proteção especial - incluindo-os no rol de dados sensíveis -, e exigindo maior transparência e segurança em relação às práticas adotadas com esses dados, tanto por pessoa natural quanto por pessoa jurídica de direito público ou privado.

Devido aos direitos previstos na Constituição Federal, algumas leis federais já vinham regulamentando e garantindo certa proteção aos dados dos titulares em situações particulares, como o Código de Defesa do Consumidor (Lei nº 8.078/1990)[285], a Lei do Cadastro Positivo

---

[282] "Em maio de 2020, em julgamento histórico, o Supremo Tribunal Federal (STF) reconheceu a proteção de dados pessoais como um direito fundamental, simbolizando um grande avanço mediante a urgência que o tema demanda. O Tribunal, por maioria de votos, declarou a inconstitucionalidade da Medida Provisória n. 954/2020, que previa o compartilhamento de dados dos usuários de serviços de telecomunicações com o Instituto Brasileiro de Geografia e Estatística (IBGE) para a produção de estatísticas durante a pandemia do novo coronavírus." BACCARIN; CANAVEZ, op. cit.

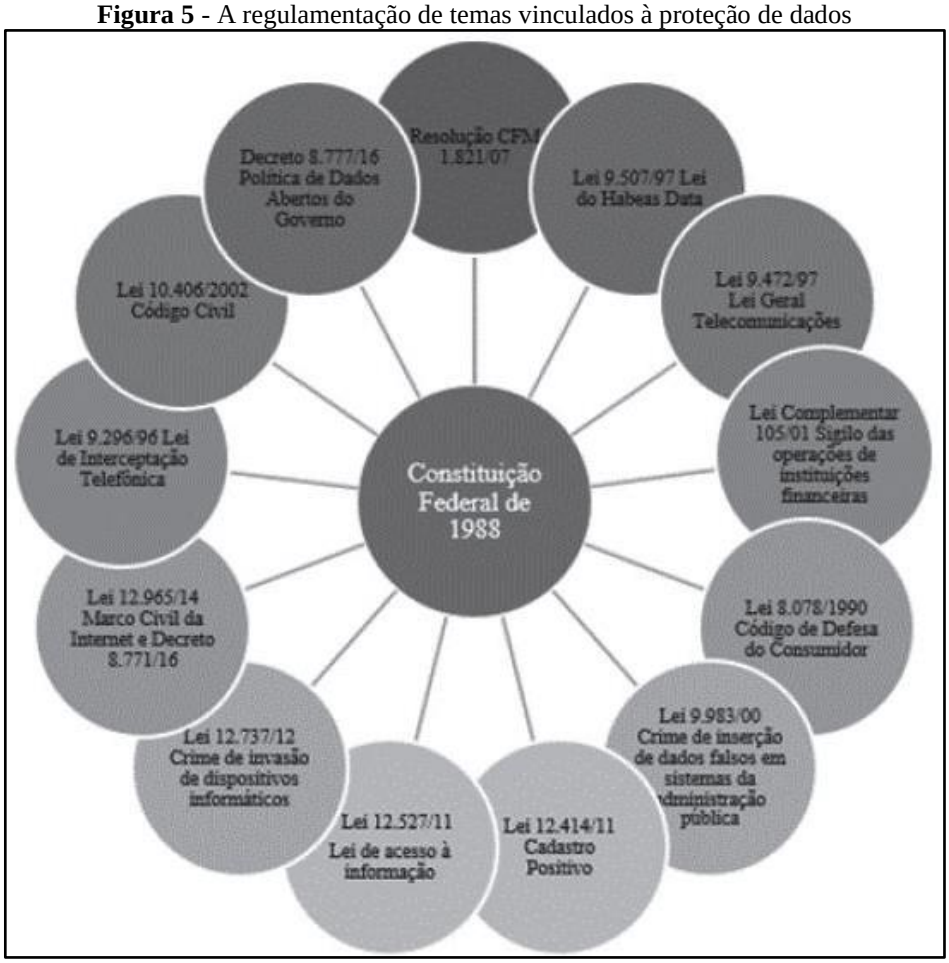
[283] BRASIL. Constituição da República Federativa do Brasil, de 5 de outubro de 1988, op. cit.

[284] BRASIL. Lei n. 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). **Diário Oficial da União**: Brasília, DF, 14 ago. 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709compilado.htm. Acesso em: 14 mar. 2023.

[285] BRASIL. Lei nº 8.078, de 11 de setembro de 1990. Dispõe sobre a proteção do consumidor e dá outras providências. **Diário Oficial da União:** Brasília, DF, 11 set. 1990. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l8078compilado.htm. Acesso em: 13 mar. 2023.

(Lei nº 12.414/2011)[286], a Lei de Acesso à Informação (Lei nº 12.527/2011)[287] e o Marco Civil da Internet (Lei nº 12.965/2014)[288], dentre outras (Figura 5):

Figura 5 - A regulamentação de temas vinculados à proteção de dados



Fonte: A Regulação do Reconhecimento Facial e Seus Impactos para os Setores Público e Privado no Brasil: uma análise comparativa internacional[289].

Embora o Brasil ainda não tenha nenhuma lei federal específica sobre dados biométricos, tecnologia de reconhecimento facial e inteligência artificial, observa-se no Legislativo brasileiro uma movimentação no sentido de regular esses temas.

---

[286] BRASIL. Lei nº 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 União:** Brasília, DF, 9 jun. 2011. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12414.htm. Acesso em: 13 mar. 2023.

[287] BRASIL. Lei nº 12.527, de 18 de novembro de 2011. Regula o acesso a informações previsto no inciso XXXIII do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal; altera a Lei nº 8.112, de 11 de dezembro de 1990; revoga a Lei nº 11.111, de 5 de maio de 2005, e dispositivos da Lei nº 8.159, de 8 de janeiro de 1991; e dá outras providências. **Diário Oficial da União:** Brasília, DF, 18 nov. 2011. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm. Acesso em: 13 mar. 2023.

[288] BRASIL. Lei nº 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. **Diário Oficial da União:** Brasília, DF, 23 abr. 2014. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 13 mar. 2023.

[289] PEREIRA; SILVA, op. cit.

3.2 OS PROJETOS DE LEI NO CONGRESSO NACIONAL

O Quadro 5 abaixo foi desenvolvido a partir de pesquisas realizadas no sítio eletrônico do Congresso Nacional[290], em que os termos de busca utilizados foram (1) “dados biométricos”, (2) “biometria facial”, (3) “dado biométrico facial”, (4) “reconhecimento facial” e (5) “inteligência artificial”, todos entre as aspas. No levantamento das informações foram selecionados os filtros “PL - Projeto de Lei” e “Projetos e Matérias - Proposições”, bem como foram classificados por data. O primeiro termo gerou 10 (dez) resultados, o segundo e o terceiro termo não disponibilizaram nenhum resultado, o quarto termo forneceu 21 (vinte e um) resultados e, por fim, o quinto termo gerou 14 (quatorze) resultados. Alguns PLs apareceram em mais de um termo de busca, sendo assim, para não repetir informação na tabela, a primeira coluna “Termo de Pesquisa” foi preenchida com os termos pelos quais o projeto foi encontrado, ou seja, se o PL foi encontrado por mais de um termo, isso foi identificado na primeira coluna. No total, foram mapeados 42 (quarenta e dois) PLs. Logo abaixo do Quadro serão apontados os destaques interpretativos.

Quadro 5 - Pesquisa de atividade legislativa no Congresso Nacional do Brasil

Termo de Pesquisa	Projeto de Lei	Data/ Iniciativa	Ementa	Status
“Dados biométricos”	PL nº 1515/2022	07/06/2020, Deputado Coronel Armando (PL/SC)	Lei de Proteção de Dados Pessoais para fins exclusivos de segurança do Estado, de defesa nacional, de segurança pública, e de investigação e repressão de infrações penais.	Em tramitação na Câmara (Casa Iniciadora) Situação: Aguardando Criação de Comissão Temporária pela MESA
“Dados biométricos”	PL nº 2628/2020	13/05/2020, Senador Confúcio Moura (MDB/RO)	Altera a Lei nº 13.444, de 11 de maio de 2017, que dispõe sobre a Identificação Civil Nacional (ICN), para dispor sobre a consolidação de informações cadastrais e identitárias dos cidadãos para fins de elegibilidade a políticas públicas e para a concessão e a manutenção de benefícios	Não aprovado Situação: Prejudicada

[290] BRASIL. **Congresso Nacional**. Praça dos Três Poderes, Brasília, DF. Disponível em: https://www.congressonacional.leg.br/. Acesso em: 17 mar. 2023.

			sociais.	
“Dados biométricos”	PL nº 4901/2019	05/09/2019, Deputado Bibo Nunes (PSL/RS)	Dispõe sobre a utilização de sistemas de verificação biométrica e dá outras providências.	Em tramitação na Câmara (Casa Iniciadora) Situação: Apensado ao PL 12/2015
“Dados biométricos”	PL nº 4927/2016	06/04/2016, Deputado Moroni Torgan (DEM/CE)	Altera a Lei 12.681, de 4 de julho de 2012, para dispor sobre bancos biométricos e sistema de identificação criminal geridos pelos órgãos oficiais de identificação no âmbito do SINESP.	Em tramitação na Câmara (Casa Iniciadora) Situação: Arquivada
“Dados biométricos”	PL nº 3715/2015	19/11/2015, Deputado João Campos (PSDB/GO)	Altera a Lei nº 7.116, de 29 de agosto de 2013, que assegura a validade nacional às Carteiras de Identidade e regula sua expedição e dá outras providências.	Em tramitação na Câmara (Casa Iniciadora) Situação: Apensado ao PL 7902/2010
“Dados biométricos” e “Reconhecimento facial”	PL nº 12/2015	02/02/2015, Deputado Lucas Vergilio (SD/GO)	Dispõe sobre a utilização de sistemas de verificação biométrica e dá outras providências.	Em tramitação na Câmara (Casa Iniciadora) Situação: Aguardando Designação de Relator na Comissão de Ciência, Tecnologia e Inovação (CCTI)
“Dados biométricos”	PL nº 8239/2014	11/12/2014, Deputado João Campos (PSDB/GO)	Altera a Lei nº 12.037, de 1º de outubro de 2009, que trata de isenção da identificação criminal do civilmente identificado.	Em tramitação na Câmara (Casa Iniciadora) Situação: Pronta para Pauta no Plenário (PLEN)
“Dados biométricos”	PL nº 4646/2012	31/10/2012, Deputada Aline Corrêa (PP/SP)	Altera a Lei nº 8.934, de 18 de novembro de 1994, que Dispõe sobre o Registro Público de Empresas Mercantis e Atividades Afins e dá outras providências, para os fins de exigir a apresentação de documento de identificação com foto e o registro dos dados biométricos dos sócios e administradores das empresas mercantis.	Em tramitação na Câmara (Casa Iniciadora) Situação: Apensado ao PL 3492/2012
“Dados biométricos”	PL nº 3492/2012	21/03/2012, Deputado Carlos	Altera a Lei nº 8.934, de 18 de novembro de 1994, para tornar mais	Em tramitação na Câmara (Casa Iniciadora)

		Sampaio (PSDB/SP)	rigorosos os atos empresariais levados a registro nas Juntas Comerciais.	Situação: Apensado ao PL 7750/2010
“Dados biométricos”	PL nº 7750/2010 (anterior PLS nº 545/2007)	17/09/2007, Senador Papaléo Paes (PSDB/AP)	Altera a Lei nº 8.934, de 18 de novembro de 1994, e a Lei nº 10.406, de 10 de janeiro de 2002 (Código Civil), para atualizar a terminologia referente ao Registro Público de Empresas e Atividades Afins.	Em tramitação na Câmara (Casa Revisora desde 13/08/2010) Situação: Aguardando Designação de Relator na Comissão de Constituição e Justiça e de Cidadania (CCJC)
“Reconhecimento facial”	PL nº 3069/2022	22/12/2022, Deputado Subtenente Gonzaga (PSD/MG)	Dispõe sobre o uso de tecnologia de reconhecimento facial automatizado no âmbito das forças de segurança pública e dá outras providências.	Em tramitação na Câmara (Casa Iniciadora) Situação: não há
“Reconhecimento facial” e “inteligência artificial”	PL n° 745/2022	29/03/2022, Senador Jorge Kajuru (PODEMOS/ GO)	Altera a Lei nº 13.812, de 16 de março de 2019, que institui a Política Nacional de Busca de Pessoas Desaparecidas, cria o Cadastro Nacional de Pessoas Desaparecidas e altera a Lei nº 8.069, de 13 de julho de 1990 (Estatuto da Criança e do Adolescente), para dispor sobre o uso de aplicações de reconhecimento facial.	Em tramitação no Senado (Casa Iniciadora) Situação: Aguardando despacho
“Dados biométricos” e “Reconhecimento facial”	PL nº 2392/2022	31/08/2022, Deputado Guiga Peixoto (PSC/SP)	Dispõe sobre o uso de tecnologias de reconhecimento facial nos setores público e privado.	Em tramitação na Câmara (Casa Iniciadora) Situação: Aguardando Designação de Relator na Comissão de Trabalho (CTRAB)
“Reconhecimento facial”	PL nº 1756/2022	24/06/2022, Deputado José Nelto (PP/GO)	Dispõe sobre a obrigatoriedade de instalação de câmeras para reconhecimento facial em hospitais públicos.	Em tramitação na Câmara (Casa Iniciadora) Situação: Apensado ao PL 3251/2015
“Reconhecimento facial”	PL nº 807/2022	04/04/2022, Deputada Maria do Rosário (PT/RS)	Estabelece medidas de prevenção e combate ao trabalho infantil em empresas de aplicativos de entregas ou transporte e dá outras providências.	Em tramitação na Câmara (Casa Iniciadora) Situação: Aguardando Designação de Relator na Comissão de Saúde (CSAUDE)

“Reconhecimento facial”	PL nº 3714/2021	22/10/2021, Deputado Julio Lopes (PP/RJ)	Dispõe sobre o reconhecimento facial em todas as fases da persecução penal.	Em tramitação na Câmara (Casa Iniciadora) Situação: Apensado ao PL 1527/2021
“Reconhecimento facial”	PL nº 676/2021	03/03/2021, Senador Marcos do Val (PODEMOS/ ES)	Altera o Decreto-Lei nº 3.689, de 3 de outubro de 1941 (Código de Processo Penal), para disciplinar o reconhecimento fotográfico de pessoa.	Em tramitação na Câmara (Casa Revisora desde 21/10/2021) Situação: Remetida à Câmara Dos Deputados
“Reconhecimento facial”	PL nº 1527/2021	26/04/2021, Deputado Ronaldo Carletto (PP/BA)	Disciplina o reconhecimento pessoal por meio fotográfico para fins criminais.	Em tramitação na Câmara (Casa Iniciadora) Situação: Apensado ao PL 7213/2014
“Reconhecimento facial”	PL nº 572/2021	24/02/2021, Deputado Igor Kannário (DEM/BA)	Altera a Lei nº 13.812, de 16 de março de 2019 e cria o Banco Nacional de Dados de Reconhecimento Facial e Digital.	Em tramitação na Câmara (Casa Iniciadora) Situação: Apensado ao PL 397/2020
“Reconhecimento facial”	PL nº 397/2020	19/02/2020, Deputado Gutemberg Reis (MDB/RJ)	Altera a Lei nº 13.812, de 2019, para criar o banco de informações de pessoas sem identificação atendidas em serviços de saúde e de assistência social no Cadastro Nacional de Pessoas Desaparecidas e dá outras providências.	Em tramitação na Câmara (Casa Iniciadora) Situação: Aguardando Designação de Relator na Comissão de Saúde (CSAUDE)
“Reconhecimento facial”	PL n° 6197/2019	26/11/2019, Senador Acir Gurgacz (PDT/RO)	Altera a Lei n° 12.037, de 1º de outubro de 2009, a Lei nº 7.210, de 11 de julho de 1984 – Lei de Execução Penal, e a Lei nº 11.473, de 10 de maio de 2007, para prever a criação de um banco nacional de padrões de face, de íris e de voz e a instalação de câmeras para reconhecimento facial em locais públicos.	Não aprovado Situação: Retirada pelo autor
“Reconhecimento facial”	PL n° 6299/2019	04/12/2019, Senador Marcos do Val (PODEMOS/ ES)	Altera a Lei nº 12.587, de 3 de janeiro de 2012, para disciplinar o cadastro de usuários, as informações a serem fornecidas aos usuários e aos motoristas e as ferramentas de segurança no transporte	Em tramitação no Senado (Casa Iniciadora) Situação: Aguardando designação do relator

			privado remunerado individual de passageiros.	
“Reconhecimento facial”	PL nº 4612/2019	21/08/2019, Deputado Bibo Nunes (PSL/RS)	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.	Em tramitação na Câmara (Casa Iniciadora) Situação: Apensado ao PL 12/2015
“Reconhecimento facial”	PL nº 2537/2019	25/04/2019, Deputado Juninho do Pneu (DEM/RJ)	Obriga o aviso sobre o reconhecimento facial em estabelecimentos comerciais.	Em tramitação na Câmara (Casa Iniciadora)
“Reconhecimento facial”	PL nº 9736/2018	07/03/2018, Deputado Julio Lopes (PP/RJ), Deputado Paulo Abi-ackel (PSDB/MG)	Acrescenta dispositivo à Lei nº 7.210, de 11 de julho de 1984, para incluir a previsão de identificação por reconhecimento facial.	Em tramitação na Câmara (Casa Iniciadora) Situação: Aguardando Designação de Relator na Comissão de Defesa do Consumidor (CDC)
“Reconhecimento facial”	PL nº 3251/2015	07/10/2015, Deputado Fernando Torres (PSD/BA)	Torna-se obrigatória a instalação de Câmeras de Segurança em Clínicas e Hospitais Públicos e Privados em todo território nacional.	Em tramitação na Câmara (Casa Iniciadora) Situação: Apensado ao PL 3/2015
“Reconhecimento facial”	PL nº 3/2015	02/02/2015, Deputado Ricardo Barros (PP/PR)	Dispõe sobre a obrigatoriedade de instalação de câmeras de monitoramento em Unidades de Terapia Intensiva - UTI de hospitais públicos e privados.	Em tramitação na Câmara (Casa Iniciadora) Situação: Aguardando Designação de Relator na Comissão de Saúde (CSAUDE)
“Reconhecimento facial”	PL nº 7213/2014	28/02/2014, Deputado Alessandro Molon (PT/RJ), Deputado Paulo Teixeira (PT/SP)	Altera os arts. 226, 227 e 228 do Decreto-lei nº 3.689, de 3 de outubro de 1941 - Código de Processo Penal, para fins de regulamentação do reconhecimento de pessoas e coisas.	Em tramitação na Câmara (Casa Iniciadora) Situação: Apensado ao PL 676/2021
“Reconhecimento facial”	PL nº 1230/2007	31/05/2007, Deputado Eduardo	Dispõe sobre mecanismos de segurança para acesso aos sistemas	Não aprovado Situação: Arquivada

		Gomes (PSDB/TO)	e bancos de dados da Administração Pública Federal.	
“Reconhecimento facial”	PL nº 3372/2004	15/04/2004, Deputado Eduardo Paes (PSDB/RJ)	Dispõe sobre mecanismos de segurança para acesso aos sistemas e bancos de dados da Administração Pública Federal.	Em tramitação na Câmara (Casa Iniciadora) Situação: Arquivada
“Inteligência artificial”	PL nº 1153/2023	15/03/2023, Deputado Carlos Henrique Gaguim (UNIÃO/TO)	Dispõe sobre normas gerais para a pesquisa, o desenvolvimento e a aplicação da inteligência artificial - IA, e seu uso consciente e ético no âmbito da União, dos Estados, do Distrito Federal e dos Municípios.	Em tramitação na Câmara (Casa Iniciadora) Situação: Aguardando Despacho do Presidente da Câmara dos Deputados
“Inteligência artificial”	PL nº 791/2023	02/03/2023, Deputado Emanuel Pinheiro Neto (MDB/MT)	Estabelece procedimentos a serem adotados pela União em regime de colaboração com os Estados, Distrito Federal e Municípios em situação de riscos e desastres mediante o uso de Sistemas de Processamento de Dados e de Inteligência Artificial (IA), com objetivo na organização, solução e implementação integrada e dá outras providências.	Em tramitação na Câmara (Casa Iniciadora) Situação: Aguardando Despacho do Presidente da Câmara dos Deputados
“Inteligência artificial”	PL nº 759/2023	01/03/2023, Deputado Lebrão (UNIÃO/RO)	Regulamenta os sistemas de Inteligência Artificial, e dá outras providências.	Em tramitação na Câmara (Casa Iniciadora) Situação: Aguardando Despacho do Presidente da Câmara dos Deputados
“Inteligência artificial”	PL nº 3009/2022	15/12/2022, Deputado Alexis Fonteyne (NOVO/SP)	Dispõe sobre a reforma da Lei nº 9.784/99 (Lei de Processo Administrativo).	Em tramitação no Senado (Casa Iniciadora) Situação: Apensado ao PL 1732/2020
“Inteligência artificial”	PL nº 705/2022	24/03/2022, Deputado Helio Lopes (UNIÃO/RJ)	Dispõe sobre a compatibilização dos sistemas de Inteligência Artificial utilizados pela Administração Pública a	Em tramitação no Senado (Casa Iniciadora) Situação: Aguardando Designação de Relator na

			práticas da agenda ambiental, social e de governança.	Comissão de Constituição e Justiça e de Cidadania (CCJC)
"Inteligência artificial"	PL nº 872/2021	12/03/2021, Senador Veneziano Vital do Rêgo (MDB/PB)	Dispõe sobre o uso da Inteligência Artificial.	Em tramitação no Senado (Casa Iniciadora) Situação: Aguardando despacho
"Inteligência artificial"	PL nº 1969/2021	26/05/2021, Deputado Gustavo Fruet (PDT/PR)	Dispõe sobre os princípios, direitos e obrigações na utilização de sistemas de inteligência artificial.	Não aprovado Situação: Arquivada
"Inteligência artificial"	PL nº 21/2020	04/02/2021, Deputado Eduardo Bismarck (PDT/CE)	Estabelece fundamentos, princípios e diretrizes para o desenvolvimento e a aplicação da inteligência artificial no Brasil, e dá outras providências.	Em tramitação no Senado (Casa Revisora desde 30/09/2021) Situação: Aguardando despacho.
"Inteligência artificial"	PL nº 240/2020	11/02/2020, Deputado Léo Moraes (PODE/RO)	Cria a Lei da Inteligência Artificial, e dá outras providências.	Não aprovado pela Câmara (Casa Iniciadora) Situação: Arquivada
"Inteligência artificial"	PL nº 4513/2020	09/09/2020, Deputada Angela Amin (PP/SC)	Institui a Política Nacional de Educação Digital; altera as Leis nºs 9.394, de 20 de dezembro de 1996 (Lei de Diretrizes e Bases da Educação Nacional), 9.448, de 14 de março de 1997, 10.260, de 12 de julho de 2001, e 10.753, de 30 de outubro de 2003; e dá outras providências.	Aprovada pelo Congresso Sancionada com vetos Situação: Transformada na Lei Ordinária nº 14.533 de 11/01/2023
"Inteligência artificial"	PL nº 5051/2019	16/09/2019, Senador Styvenson Valentim (PODEMOS/ RN)	Estabelece os princípios para o uso da Inteligência Artificial no Brasil.	Em tramitação na Câmara (Casa Iniciadora) Situação: Aguardando despacho.
"Inteligência artificial"	PL nº 5691/2019	25/10/2019, Senador Styvenson Valentim (PODEMOS/ RN)	Institui a Política Nacional de Inteligência Artificial.	Em tramitação na Câmara (Casa Iniciadora) Situação: Aguardando designação do relator.

Fonte: elaborado pela autora com base nas matérias legislativas do Congresso Nacional, atualizado até março de 2023[291].

[291] BRASIL. **Congresso Nacional**, op. cit.

Conforme o Quadro 5, enquanto cinco projetos de lei foram "não aprovados", a maioria permanece "em tramitação" no Congresso Nacional para regular os temas procurados, sendo que grande parte não passou pela aprovação da casa legislativa em que o projeto foi apresentado (casa iniciadora).

Apenas quatro PLs evoluíram no processo de aprovação. O primeiro caso foi o PL nº 4513/2020[292] que foi aprovado pelo Congresso Nacional, sancionado pelo Presidente com vetos e transformado em lei, que entretanto, não será importante para fins do estudo desta dissertação, tendo em vista que deixou de considerar o termo "inteligência artificial" no texto aprovado[293].

Ademais, três PLs foram aprovados na casa iniciadora e estão em trâmite na casa revisora. O PL nº 676/2021[294], que "altera o Decreto-Lei nº 3.689, de 3 de outubro de 1941 (Código de Processo Penal), para disciplinar o reconhecimento fotográfico de pessoa", ou seja, o projeto altera as regras para o reconhecimento de pessoas acusadas por cometer crimes. O PL também não tem relevância para o presente estudo, já que não se trata de tecnologia de reconhecimento facial.

O segundo é o PL nº 7750/2010[295], que "altera a Lei nº 8.934, de 18 de novembro de 1994, e a Lei nº 10.406, de 10 de janeiro de 2002 (Código Civil), para atualizar a terminologia referente ao Registro Público de Empresas e Atividades Afins". Entretanto, o PL segue sem qualquer menção ao termo "dados biométricos" pelo qual foi encontrado, em conjunto com os apensos PL nº 4646/2012 e PL nº 3492/2012.

---

[292] BRASIL. Câmara dos Deputados. **Projeto de Lei nº 4.513, de 9 de setembro de 2020.** Institui a Política Nacional de Educação Digital; altera as Leis nºs 9.394, de 20 de dezembro de 1996 (Lei de Diretrizes e Bases da Educação Nacional), 9.448, de 14 de março de 1997, 10.260, de 12 de julho de 2001, e 10.753, de 30 de outubro de 2003; e dá outras providências. Brasília: Câmara dos Deputados, 2020. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2262422. Acesso em: 29 abr. 2023.

[293] Em um primeiro momento, o PL nº 4513/2020 foi apresentado na Câmara dos Deputados com a intenção de instituir uma política abrangente de educação digital no Brasil. Essa educação digital possuía a "pesquisa digital" como um dos eixos para atingir o propósito da política, cujo objetivo desse eixo seria promover um avanço significativo na utilização de "tecnologias digitais", ou seja, considerava a utilização das inteligências artificiais. Contudo, embora o PL tenha aparecido na busca pelo termo "inteligência artificial", ele foi para a casa revisora (Senado) com a mudança do texto e a supressão do termo "inteligência artificial". Portanto, apesar do PL ter sido aprovado, sancionado e convertido em Lei, a legislação não será importante para fins do estudo dessa dissertação de mestrado. Ibidem.

[294] Possui como apensados o PL nº 7213/2014 e o PL nº 1527/2021. BRASIL. Senado Federal. **Projeto de Lei nº 676, de 3 de março de 2021.** Altera o Decreto-Lei nº 3.689, de 3 de outubro de 1941 (Código de Processo Penal), para disciplinar o reconhecimento fotográfico de pessoa. Brasília: Senado Federal, 2021. Disponível em: https://www25.senado.leg.br/web/atividade/materias/-/materia/147134. Acesso em: 29 abr. 2023.

[295] Possui como apensados o PL nº 4646/2012 e o PL nº 3492/2012. BRASIL. Câmara dos Deputados. **Projeto de Lei nº 7.750, de 13 de agosto de 2010.** Estabelece fundamentos, princípios e diretrizes para o desenvolvimento e a aplicação da inteligência artificial no Brasil; e dá outras providências. Brasília: Câmara dos Deputados, 2010. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=484718. Acesso em: 29 abr. 2023.

Por último, o PL nº 21/2020[296], que "estabelece fundamentos, princípios e diretrizes para o desenvolvimento e a aplicação da inteligência artificial no Brasil e dá outras providências", isto é, está sendo criada a regulamentação para o desenvolvimento e uso da inteligência artificial pelo poder público e setor privado[297].

Portanto, dentre os três que avançaram no processo de tramitação bicameral, o que chama atenção para fins da presente pesquisa é este último, o PL nº 21/2020, que, se aprovado, afetará o uso de tecnologias de reconhecimento facial. Há, no legislativo, seis PLs que visam regular e estabelecer princípios para o uso da IA no Brasil, tais como: (i) o PL nº PL nº 759/2023[298]; (ii) o PL nº 872/2021[299]; (iii) o já mencionado PL nº 21/2020; (iv) o PL nº 240/2020[300]; (v) o nº PL 5.051/2019[301]; (vi) o PL nº 5.691/2019[302]. Essas tentativas iniciais de regulamentação demonstram que as instituições já começaram a se movimentar no sentido de criar um Marco Legal para o uso de IA no país. No entanto, apenas o PL nº 21/2020 possui o texto mais avançado sobre o tema - mesmo que apresente insuficiências expressivas, em amplo debate atualmente -, enquanto os outros PLs referidos enfrentam a temática de forma superficial.

O objetivo do PL nº 21/2020 é estabelecer princípios, direitos, deveres e instrumentos de governança para a IA, garantindo o respeito aos direitos humanos, valores democráticos, transparência e privacidade de dados. A proposta prevê a figura do agente de IA - agente de desenvolvimento ou de operação -, que terá deveres a cumprir, como responder legalmente

---

[296] BRASIL. Senado Federal. **Projeto de Lei nº 21, de 4 de fevereiro de 2020.** Altera a Lei nº 8.934, de 18 de novembro de 1994, e a Lei nº 10.406, de 10 de janeiro de 2002 (Código Civil), para atualizar a terminologia referente ao Registro Público de Empresas e Atividades Afins. Brasília: Senado Federal, 2020. Disponível em: https://www25.senado.leg.br/web/atividade/materias/-/materia/151547. Acesso em: 29 abr. 2023.

[297] CÂMARA DOS DEPUTADOS. Projeto cria marco legal para uso de inteligência artificial no Brasil. **Agência Câmara de Notícias**, 4 mar. 2020. Disponível em: https://www.camara.leg.br/noticias/641927-projeto-cria-marco-legal-para-uso-de-inteligencia-artificial-no-brasil/. Acesso em: 29 abr. 2023.

[298] BRASIL. Câmara dos Deputados. **Projeto de Lei nº 759, de 1 de março de 2023.** Regulamenta os sistemas de Inteligência Artificial, e dá outras providências. Brasília: Câmara dos Deputados, 2023. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2349685. Acesso em: 29 abr. 2023.

[299] BRASIL. Senado Federal. **Projeto de Lei nº 872, 12 de março de 2021.** Dispõe sobre o uso da Inteligência Artificial. Brasília: Senado Federal, 2021. Disponível em: https://www25.senado.leg.br/web/atividade/materias/-/materia/147434. Acesso em: 29 abr. 2023.

[300] BRASIL. Câmara dos Deputados. **Projeto de Lei nº 240, de 11 de fevereiro de 2020.** Cria a Lei da Inteligência Artificial, e dá outras providências. Brasília: Câmara dos Deputados, 2020. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2236943. Acesso em: 29 abr. 2023.

[301] BRASIL. Senado Federal. **Projeto de Lei nº 5.051, de 16 de setembro de 2019.** Estabelece os princípios para o uso da Inteligência Artificial no Brasil. Brasília: Senado Federal, 2019. Disponível em: https://www25.senado.leg.br/web/atividade/materias/-/materia/147434. Acesso em: 29 abr. 2023.

[302] BRASIL. Senado Federal. **Projeto de Lei nº 5.691, de 25 de outubro de 2019.** Institui a Política Nacional de Inteligência Artificial. Brasília: Senado Federal, 2019. Disponível em: https://www25.senado.leg.br/web/atividade/materias/-/materia/139586. Acesso em: 29 abr. 2023.

pelas decisões tomadas por um sistema de inteligência artificial, assegurar o respeito à LGPD e elaborar relatório de impacto de IA, para descrever a tecnologia e seus riscos[303].

Destaca-se também, para fins desta pesquisa, o PL nº 12/2015[304], que, em sua essência, busca dar proteção jurídica aos dados biométricos ao dispor "sobre a utilização de sistemas de verificação biométrica e dá outras providências". O texto propõe a criação de regras para usuários e administradores de sistemas de reconhecimento biométrico, tais como reconhecimento de impressões digitais, reconhecimento facial, identificação de íris, assinatura e geometria das mãos. O projeto garante o direito à proteção dos dados biométricos gerados no território nacional e estabelece sanções para infrações administrativas, como violação do sigilo, criação de dados fictícios e não fornecimento das informações ao titular. As infrações serão punidas com advertência, multa, suspensão da venda e fabricação do produto ou da atividade. A multa poderia chegar até dez milhões para quem a utilizar de forma irregular ou poderia haver pena de um a quatro anos de reclusão para os casos de inserção de dados falsos ou exclusão de dados corretos obtidos por meio da biometria com a finalidade de obter vantagens indevidas[305].

O PL nº 1515/2022[306], encontrado na pesquisa, pretende criar a "Lei de Proteção de Dados Pessoais para fins exclusivos de segurança do Estado, de defesa nacional, de segurança pública, e de investigação e repressão de infrações penais". Apesar de ser destinado ao setor público e, por essa razão, não ser relevante para esta pesquisa, o PL será de grande importância para regulamentar o uso de dados biométricos por agentes públicos para as finalidades descritas.

Enquanto isso, os PLs nº 3715/2015[307] e nº 3492/2012[308] não se tratam de regulamentar as tecnologias em si, mas são destinados à implementação da coleta dos dados biométricos

---

[303] CÂMARA DOS DEPUTADOS. Projeto cria marco legal para uso de inteligência artificial no Brasil. **Agência Câmara de Notícias**, 4 mar. 2020. Disponível em: https://www.camara.leg.br/noticias/641927-projeto-cria-marco-legal-para-uso-de-inteligencia-artificial-no-brasil/. Acesso em: 29 abr. 2023.

[304] Possui como apensados o PL nº 4901/2019 e o PL nº 4612/2019. BRASIL. Câmara dos Deputados. **Projeto de Lei nº 12, de 2 de fevereiro de 2015.** Dispõe sobre a utilização de sistemas de verificação biométrica e dá outras providências. Brasília: Câmara dos Deputados, 2015. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=944254. Acesso em: 29 abr. 2023.

[305] CÂMARA DOS DEPUTADOS. Uso irregular de dados de biometria pode acarretar multa de até R$ 10 milhões. **Agência Câmara de Notícias**, 30 abr. 2015. Disponível em: https://www.camara.leg.br/noticias/457188-USO-IRREGULAR-DE-DADOS-DE-BIOMETRIA-PODE-ACARRETAR-MULTA-DE-ATE-R$-10-MILHOES. Acesso em: 29 abr. 2023.

[306] BRASIL. Câmara dos Deputados. **Projeto de Lei nº 1.515, de 7 de junho de 2022.** Lei de Proteção de Dados Pessoais para fins exclusivos de segurança do Estado, de defesa nacional, de segurança pública, e de investigação e repressão de infrações penais. Brasília: Câmara dos Deputados, 2022. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2326300. Acesso em: 29 abr. 2023.

[307] BRASIL. Câmara dos Deputados. **Projeto de Lei nº 3.715, de 19 de novembro de 2015.** Altera a Lei nº 7.116, de 29 de agosto de 2013, que assegura a validade nacional as Carteiras de Identidade e regula sua expedição e dá outras providências. Brasília: Câmara dos Deputados, 2015. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2056049. Acesso em: 29 abr. 2023.

[308] BRASIL. Câmara dos Deputados. **Projeto de Lei nº 3.492, de 21 de março de 2012.** Altera a Lei nº 8.934, de 18 de novembro de 1994, para tornar mais rigorosos os atos empresariais levados a registro nas Juntas Comerciais.

como mecanismo de combate às fraudes documentais, como em documentos de identidade e em registro de atos empresariais nas Juntas Comerciais, respectivamente. Essas iniciativas demonstram exemplos de situações em que as novas tecnologias, como o reconhecimento facial (uma das formas de coleta de dados biométricos), podem ser utilizadas de forma benéfica para a sociedade.

Destaca-se, ainda, o PL nº 2392/2022[309], que foi encontrado tanto pelo termo "dados biométricos" quanto pelo termo "reconhecimento facial". O PL, com apenas seis artigos, dispõe sobre o uso de tecnologias de reconhecimento facial tanto pelo setor público quanto pelo privado e condiciona o tratamento de dados biométricos ao cumprimento com as disposições da LGPD. O texto do projeto proíbe o compartilhamento desses dados com terceiros e considera nulo qualquer termo de consentimento para esse fim, bem como proíbe o uso de tecnologias de reconhecimento facial para fins de identificação sem que antes tenha sido conduzido um relatório de impacto à privacidade das pessoas, conforme previsto pela LGPD[310].

Por fim, outros três PLs merecem destaque em atenção à possibilidade de afetar alguns ramos do setor privado, se aprovados. O primeiro destaque é o PL n° 6299/2019[311], que "obriga os aplicativos de mobilidade urbana a cadastrar informações mínimas de seus usuários" e a implementar ferramentas de reconhecimento facial e de compartilhamento de rotas, para garantia da segurança de usuários e motoristas. Outro destaque diz respeito ao PL nº 2537/2019[312], que poderá impactar os estabelecimentos comerciais que utilizarem programas de reconhecimento facial, em razão de que deverão alertar os consumidores sobre essa prática com placas ou adesivos fixados na entrada do local. Por último, o PL nº 807/2022[313] dispõe que

---

Brasília: Câmara dos Deputados, 2012. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=538210. Acesso em: 29 abr. 2023.

[309] BRASIL. Câmara dos Deputados. **Projeto de Lei nº 2.392, de 31 de agosto de 2022.** Dispõe sobre o uso de tecnologias de reconhecimento facial nos setores público e privado. Brasília: Câmara dos Deputados, 2022. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2334803. Acesso em: 29 abr. 2023.

[310] CÂMARA DOS DEPUTADOS. Projeto condiciona uso de reconhecimento facial a inviabilidade de outros meios de identificação. **Agência Câmara de Notícias**, 6 out. 2022. Disponível em: https://www.camara.leg.br/noticias/911976-PROJETO-CONDICIONA-USO-DE-RECONHECIMENTO-FACIAL-A-INVIABILIDADE-DE-OUTROS-MEIOS-DE-IDENTIFICACAO. Acesso em: 29 abr. 2023.

[311] BRASIL. Senado Federal. **Projeto de Lei nº 6.299, de 4 de dezembro de 2019.** Altera a Lei nº 12.587, de 3 de janeiro de 2012, para disciplinar o cadastro de usuários, as informações a serem fornecidas a usuários e a motoristas e as ferramentas de segurança no transporte privado remunerado individual de passageiros. Brasília: Senado Federal, 2019. Disponível em: https://www25.senado.leg.br/web/atividade/materias/-/materia/140072. Acesso em: 29 abr. 2023.

[312] BRASIL. Câmara dos Deputados. **Projeto de Lei nº 2.537, de 25 de abril de 2019.** Obriga o aviso sobre o reconhecimento facial em estabelecimentos comerciais. Brasília: Câmara dos Deputados, 2019. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2199418. Acesso em: 29 abr. 2023.

[313] BRASIL. Câmara dos Deputados. **Projeto de Lei nº 807, de 4 de abril de 2022.** Estabelece medidas de prevenção e combate ao trabalho infantil em empresas de aplicativos de entregas ou transporte e dá outras

empresas de aplicativos de entrega serão obrigadas a adotar medidas de combate ao trabalho infantil por meio da implementação de cadastro biométrico ou de identificação facial dos trabalhadores e por meio da verificação periódica dos dados, que deverão ser disponibilizados para órgãos de fiscalização do trabalho.

Grande parte dos PLs que não foram explorados aqui no texto, mas que estão presentes na tabela, referem-se ao setor público. Contudo, em certa medida também são importantes para o setor privado que é o principal fornecedor de tecnologia para o setor público, de tal modo que qualquer proibição ou permissão de uso de sistemas de reconhecimento facial pelo setor público acaba afetando indiretamente as empresas, além de possivelmente apresentarem um termômetro para a regulamentação do uso privado.

Após as considerações feitas sobre os projetos de lei mapeados em tramitação no Congresso Nacional que dizem respeito a dados biométricos, reconhecimento facial e inteligência artificial, parte-se para a compreensão das disposições da LGPD que regulamentam os sistemas de reconhecimento facial no Brasil

3.3 A LEI GERAL DE PROTEÇÃO DE DADOS E OS DADOS BIOMÉTRICOS

Até 2018, não havia no Brasil uma lei específica destinada a tratar somente da proteção de dados pessoais que considerasse a segurança dos dados em todo o seu ciclo de operações: coleta, armazenamento, compartilhamento e descarte. Inspirada no GDPR, a LGPD entrou em vigor em setembro de 2020 e foi criada com o objetivo de garantir principalmente os direitos fundamentais da privacidade, da liberdade e do livre desenvolvimento da personalidade da pessoa natural (art. 1º, LGPD), para que as pessoas obtenham maior controle, segurança e privacidade sobre suas próprias informações. Para tanto, a Lei estabelece uma série de medidas para a proteção de dados, prevê sanções e criou a Autoridade Nacional de Proteção de Dados (ANPD)[314], responsável por zelar, implementar e fiscalizar o seu cumprimento (art. 5º, XIX, LGPD).

Os dados biométricos faciais coletados através das tecnologias de reconhecimento facial são considerados sensíveis pela LGPD, isso porque o seu art. 5º, inciso II, define esses tipos de

providências. Brasília: Câmara dos Deputados, 2022. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2319143. Acesso em: 29 abr. 2023.

[314] A Autoridade Nacional de Proteção de Dados é uma autarquia de natureza especial vinculada ao Ministério da Justiça e Segurança Pública, dotada de autonomia técnica e decisória, responsável por zelar pela proteção de dados pessoais e por implementar e fiscalizar o cumprimento da LGPD no Brasil. As principais competências da ANPD estão previstas no art. 55-J da LGPD.

dados como sendo: “dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural”[315]. Nesse sentido, o ordenamento jurídico brasileiro atribui proteção especial aos dados biométricos ao incluí-los na definição de dados pessoais sensíveis[316]. Em razão disso, o tratamento dos dados biométricos faciais deverá observar os requisitos específicos que a Lei estabeleceu.

Nesse momento, é importante ressaltar que o termo “tratamento”, a ser utilizado deste momento em diante, segue a definição disposta no art. 5º, inciso X, da LGPD, que considera tratamento toda e qualquer operação realizada com dados pessoais, como as que se referem a: “coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração”. Basicamente, sempre que houver um dado pessoal, sensível ou não, possivelmente haverá o tratamento desse dado.

Com relação às disposições da LGPD para o tratamento de dados sensíveis, estes deverão seguir a Seção II do Capítulo II, em que estão compreendidos os arts. 11 a 13, sem prejuízo da aplicação de outras determinações gerais, como garantia de direitos aos titulares[317] de dados e respeito aos princípios e às técnicas de segurança, aplicáveis a todos os tipos de dados pessoais.

A LGPD, em seu art. 4º e incisos, dispõe sobre algumas hipóteses de inaplicabilidade da própria Lei, que seriam os casos de tratamento de dados pessoais: (i) para fins exclusivamente particulares e não econômicos; (ii) para fins exclusivamente jornalístico e artísticos ou acadêmicos (aplicando-se a esta hipótese os arts. 7º e 11); (iii) para fins exclusivos de segurança pública, defesa nacional, segurança do Estado ou atividades de investigação e repressão de infrações penais, a serem regidos por legislação específica; 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

[315] BRASIL. Lei n. 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD), op. cit.
[316] A LGPD considera dados pessoais sensíveis aqueles que potencialmente podem ser utilizados para fins discriminatórios.
[317] Art. 5º, V, da LGPD: “titular: pessoa natural a quem se referem os dados pessoais que são objeto de tratamento”. BRASIL. Lei n. 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD), op. cit.

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[318].

Com relação ao terceiro ponto acima, as referidas hipóteses somente se aplicam ao setor público, de modo que é vedado que qualquer pessoa de direito privado realize tratamento de dados pessoais para estes fins, exceto em procedimentos sob tutela de pessoa jurídica de direito público, que deverão ser especificamente informados à ANPD (art. 4º, §2º, LGPD) e que deverão observar a limitação imposta pelo §4º do art. 4º da LGPD[319]. Nesse sentido, é evidente que o setor privado não pode tratar dados biométricos - e, portanto, utilizar tecnologia de reconhecimento facial -, com a finalidade de segurança pública, defesa nacional, segurança do Estado ou investigação e repressão de infrações penais.

Após essas considerações, se estiver configurada a incidência da LGPD ao tratamento de dados, então será preciso esforços para a adequação à Lei, o que envolve, no mínimo: (i) cumprimento com os princípios previstos no art. 6º da LGPD; (ii) garantia aos direitos dos titulares dos dados, previstos no arts. 18 e 20 da LGPD; (iii) mapeamento de dados pessoais, contendo, por exemplo, a indicação de todos os dados coletados, sua natureza (sensível ou não), suas finalidades, seu ciclo de vida e as respectivas hipóteses autorizadoras previstas pela Lei (bases legais); (iv) avaliação e mitigação dos riscos do tratamento de dados; (v) elaboração e divulgação de documentos, como política interna e externa de privacidade, termos de uso, guias internos de proteção de dados e de garantia aos direitos dos titulares, Política de Segurança da Informação (PSI)[320], Relatório de Impacto a Proteção de Dados (RIPD)[321] e cláusulas de

---

[318] Ibidem.

[319] Art. 4º, § 4º, da LGPD: "Em nenhum caso a totalidade dos dados pessoais de banco de dados de que trata o inciso III do caput deste artigo poderá ser tratada por pessoa de direito privado, salvo por aquela que possua capital integralmente constituído pelo poder público". Ibidem.

[320] LGPD, Art. 46: "Os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito. § 1º A autoridade nacional poderá dispor sobre padrões técnicos mínimos para tornar aplicável o disposto no caput deste artigo, considerados a natureza das informações tratadas, as características específicas do tratamento e o estado atual da tecnologia, especialmente no caso de dados pessoais sensíveis, assim como os princípios previstos no caput do art. 6º desta Lei. § 2º As medidas de que trata o caput deste artigo deverão ser observadas desde a fase de concepção do produto ou do serviço até a sua execução."
LGPD, Art. 47: "Os agentes de tratamento ou qualquer outra pessoa que intervenha em uma das fases do tratamento obriga-se a garantir a segurança da informação prevista nesta Lei em relação aos dados pessoais, mesmo após o seu término." BRASIL. Lei n. 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD), op. cit.

[321] LGDP, Art. 38: "A autoridade nacional poderá determinar ao controlador que elabore relatório de impacto à proteção de dados pessoais, inclusive de dados sensíveis, referente a suas operações de tratamento de dados, nos termos de regulamento, observados os segredos comercial e industrial.
Parágrafo único. Observado o disposto no caput deste artigo, o relatório deverá conter, no mínimo, a descrição dos tipos de dados coletados, a metodologia utilizada para a coleta e para a garantia da segurança das informações e a análise do controlador com relação a medidas, salvaguardas e mecanismos de mitigação de risco adotados." Ibidem.

proteção de dados para parceiros comerciais; (vi) indicação de um Encarregado (*Data Protection Officer* - DPO) pelo tratamento de dados pessoais[322] e disponibilização de um canal de comunicação com os titulares de dados; e (vii) treinamentos internos de colaboradores a respeito da LGPD. A responsabilidade de adequação é algo vivo, ou seja, exige atualizações periódicas do mapeamento, das análises de risco, da documentação e dos treinamentos, conforme ocorrem mudanças nas operações de tratamento.

3.3.1 Bases legais

Nesse sentido, de acordo com a LGPD, as operações de tratamento dos dados biométricos, necessariamente, deverão estar fundamentadas em uma das hipóteses legais previstas pelo art. 11 da LGPD, também chamadas de bases legais, a seguir expostas:

> Seção II
> Do Tratamento de Dados Pessoais Sensíveis
> Art. 11. O tratamento de dados pessoais sensíveis somente poderá ocorrer nas seguintes hipóteses:
> I - quando o titular ou seu responsável legal consentir, de forma específica e destacada, para finalidades específicas;
> II - sem fornecimento de consentimento do titular, nas hipóteses em que for indispensável para:
> a) cumprimento de obrigação legal ou regulatória pelo controlador;
> b) tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos;
> c) realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais sensíveis;
> d) exercício regular de direitos, inclusive em contrato e em processo judicial, administrativo e arbitral, este último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem);
> e) proteção da vida ou da incolumidade física do titular ou de terceiro;
> f) tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; ou
> g) garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos, resguardados os direitos mencionados no art. 9º desta Lei e exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais.

[322] O Encarregado, ou DPO, é uma pessoa indicada para atuar como um canal de comunicação entre o agente de tratamento de dados (controlador ou operador), os titulares dos dados e a ANPD (arts. 5º, VIII, e 41, LGPD). A ANPD, por meio da Resolução CD/ANPD nº 2/2022, indica hipótese de dispensa da necessidade de sua indicação, conforme a natureza e o porte da entidade ou o volume de operações de tratamento de dados (art. 41, §3º, LGPD). Assim, no art. 11 da Resolução, a ANPD isenta dessa obrigação os agentes de pequeno porte. Contudo, ainda que não indiquem, devem disponibilizar um canal de comunicação com o titular de dados. AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. Ministério da Justiça e Segurança Pública. Resolução CD/ANPD nº 2, de 27 de janeiro de 2022. Aprova o Regulamento de aplicação da Lei nº 13.709, de 14 de agosto de 2018, Lei Geral de Proteção de Dados Pessoais (LGPD), para agentes de tratamento de pequeno porte. **Diário Oficial da União**: Brasília, DF. 28 jan. 2022. Disponível em: https://www.in.gov.br/web/dou/-/resolucao-cd/anpd-n-2-de-27-de-janeiro-de-2022-376562019. Acesso em: 15 mar. 2023.

> § 1º Aplica-se o disposto neste artigo a qualquer tratamento de dados pessoais que revele dados pessoais sensíveis e que possa causar dano ao titular, ressalvado o disposto em legislação específica. (...)

Nestes termos, os dados biométricos poderão ser tratados quando (i) o titular dos dados ou seu responsável legal der o consentimento, de forma específica e destacada, para finalidades específicas[323], ou quando necessário para: (ii) cumprimento de obrigação legal ou regulatória; (iii) compartilhado de dados necessários à execução de políticas públicas, pela administração pública; (vi) realização de estudos por órgão de pesquisa; (v) exercício regular de direitos, inclusive em contrato e em processo judicial, administrativo e arbitral; (vi) proteção da vida ou da incolumidade física do titular ou de terceiro; (vii) tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; (viii) prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular[324].

Em comparação com os dados pessoais não sensíveis, cujo tratamento é autorizado pelas bases legais previstas no art. 7º da LGPD, os dados sensíveis não poderão ser tratados em caso de: (i) execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados; (ii) necessidade para atender aos interesses legítimos do controlador ou de terceiros; e de (iii) proteção do crédito[325].

Além da especial proteção aos dados sensíveis por meio das hipóteses que autorizam o seu tratamento, a LGPD também aborda de forma especial o tratamento de dados pessoais das crianças e adolescentes[326] (Capítulo II, Seção III, art. 14). Nos termos da Lei, as operações com

---

[323] O consentimento é, por definição em lei, a manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada (art. 5º, XII, LGPD). Para dados sensíveis, contudo, exige-se ainda que o consentimento seja dado de forma específica e destacada, para finalidades específicas. O consentimento será: (i) livre quando dado de forma espontânea e sem qualquer tipo de repressão ou coação; (ii) informado quando dado após o titular obter informações claras e precisas, com linguagem acessível e facilmente compreendida; (iii) inequívoco quando o modo de manifestação for possível de comprovar, sem ambiguidades e confusões; (iv) específico quando for minucioso e detalhado, bem como garantir a separação clara de informações relacionadas à obtenção de consentimento obtido. O consentimento deverá ser fornecido por escrito ou por outro meio que demonstre a manifestação de vontade do titular dos dados pessoais (art. 8º, LGPD). Caso o consentimento seja fornecido por escrito, esse deverá constar de cláusula destacada das demais cláusulas contratuais (art. 8º, §1º, LGPD). Além disso, o consentimento deverá referir-se a finalidades determinadas, sendo que as autorizações genéricas para o tratamento de dados pessoais serão nulas (art. 8º, §4º, LGPD). LGPD, Art. 5º, V: "titular: pessoa natural a quem se referem os dados pessoais que são objeto de tratamento". BRASIL. Lei n. 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD), op. cit.

[324] Ibidem.

[325] Ibidem.

[326] De acordo com o art. 2º do Estatuto da Criança e do Adolescente (ECA), "considera-se criança, para os efeitos desta Lei, a pessoa até doze anos de idade incompletos, e adolescente aquela entre doze e dezoito anos de idade." BRASIL. Lei n. 8.069, de 13 de julho de 1990. Dispõe sobre o Estatuto da Criança e do Adolescente e dá outras

esses dados devem ser realizadas de acordo com o melhor interesse das crianças e adolescentes, mediante consentimento específico e destacado dado por pelo menos um dos pais ou pelo responsável legal.

De forma excepcional, a lei dispensa o consentimento dos responsáveis em duas hipóteses (art. 14, § 2º), quais sejam: (i) quando a coleta do dado for necessária para contatar os pais ou responsável legal; ou (ii) para a própria proteção da criança ou do adolescente. Contudo, o Enunciado 684[327], da IX Jornada de Direito Civil que ocorreu em maio de 2022, dispôs que as demais bases legais (além da base legal do consentimento), se cabível, poderão autorizar o tratamento de dados pessoais de crianças e adolescentes, desde que seja observado o melhor interesse da criança. Assim, o tratamento de dados pessoais de crianças e adolescentes poderá ser realizado quando ocorrer, por exemplo, em razão da tutela da saúde, do exercício regular de direitos, e/ou de obrigação regulatória, conforme o melhor interesse.

As bases legais previstas na LGPD, em um primeiro momento, passam a percepção de que os processos de tratamento de dados pessoais, principalmente os de natureza sensível, somente serão autorizados em algumas situações pré-determinadas, de certa forma, limitando a atuação dos agentes de tratamento. Na realidade, as hipóteses acima previstas contemplam muitas situações na prática, de modo que, através delas, a LGPD viabiliza o uso dos dados biométricos se o agente de tratamento seguir os itens de conformidade à Lei. Sempre será possível adequar as operações com dados pessoais à alguma das bases legais previstas, entretanto, se for preciso fundamentar o tratamento através do consentimento do titular ou do responsável, isso pode ser trabalhoso a ponto de inviabilizá-lo na prática. Por exemplo, seria impraticável coletar o consentimento de todos os afetados pelas câmeras que possuem reconhecimento facial e que são instaladas em lugares de ampla circulação de pessoas.

3.3.2 Princípios

Além da adequação às bases legais, as operações de tratamento de dados pessoais (sensíveis ou não) deverão observar a boa-fé e os dez princípios previstos no art. 6º da LGPD, que representam um conjunto de valores e boas práticas a serem seguidas obrigatoriamente

---

providências. **Diário Oficial da União**: Brasília, DF, 13 jul. 1990. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l8069.htm. Acesso em: 15 mar. 2023.

[327] BRASIL. IX Jornada de Direito Civil. Enunciado nº 684. Coordenador Geral Ministro Jorge Mussi. **Conselho da Justiça Federal**: Brasília, DF, 2022. Disponível em: https://www.cjf.jus.br/enunciados/enunciado/1823. Acesso em: 15 mar. 2023.

pelos agentes de tratamento de dados. Segundo Eduardo Tomasevicius Filho[328], os princípios previstos no art. 6º da LGPD, no fundo, são desdobramentos dos deveres da boa-fé, que acabam representando hipóteses de comportamentos corretos a serem perseguidos.

O princípio da boa-fé, notadamente um princípio geral do direito, tem o objetivo de estabelecer, nas atividades de tratamento de dados, os seus deveres de coerência, de informação e de cooperação. Nesse sentido, a boa-fé visa o estabelecimento de uma relação de confiança, cuidado e honestidade com os titulares, de modo que o tratamento de dados pessoais deve ser capaz de atender a legítima expectativa dos titulares. Por este princípio, "proíbe-se a mentira, o abuso, o oportunismo, a falta de consideração e a incoerência de comportamento, e impõem-se a transparência e a preservação da confiança legitimamente despertada"[329].

De acordo com o princípio da finalidade (art. 6º, I, LGPD), o tratamento somente pode ser realizado para propósitos (finalidades) legítimos (conforme bom senso, legalidade, bons costumes e boa-fé), específicos (objetivo, determinado e relevante), explícitos (não admitindo ambiguidade) e devem ser estritamente informados ao titular dos dados pessoais, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades. O princípio da adequação (art. 6º, II, LGPD) determina que o tratamento de dados pessoais deve ser compatível "com as finalidades informadas ao titular, em acordo com o contexto do tratamento"[330]. Além disso, pelo princípio da necessidade (art. 6º, III, LGPD), deverá haver limites que respeitem o mínimo necessário para satisfação da finalidade, apenas abrangendo dados pertinentes, proporcionais e não excessivos.

O princípio do livre acesso (art. 6º, IV, LGPD) dispõe sobre o dever de garantir aos titulares a possibilidade de "consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais"[331]. Por sua vez, o princípio da qualidade dos dados (art. 6º, V, LGPD) assegura aos titulares que seus dados sejam tratados com "exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento"[332].

O princípio da transparência (art. 6º, VI, LGPD) estabelece que os titulares devem ter o acesso facilitado a "informações claras, precisas e facilmente acessíveis sobre a realização do

---

[328] TOMASEVICIUS FILHO, Eduardo. O princípio da boa-fé na Lei Geral de Proteção de Dados. **Jusbrasil**, 2022. Disponível em: https://www.jusbrasil.com.br/artigos/o-principio-da-boa-fe-na-lei-geral-de-protecao-de-dados/1252511524. Acesso em: 14 ago. 2023.
[329] Ibidem.
[330] BRASIL. Lei n. 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD), op. cit.
[331] Ibidem.
[332] Ibidem.

tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial"[333].

Ademais, em respeito ao princípio da segurança (art. 6º, VII, LGPD), deve-se empregar "medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão"[334]. Já o princípio da prevenção (art. 6º, VIII, LGPD) representa a base da Segurança da Informação, que consiste na busca da antecipação de eventualidades, com a "adoção de medidas para prevenir a ocorrência de danos em razão do tratamento de dados pessoais"[335].

A Lei ainda prevê o princípio da não discriminação (art. 6º, IX, LGPD), proibindo expressamente a "realização do tratamento para fins discriminatórios ilícitos ou abusivos"[336]. Por último, pelo princípio da responsabilização e prestação de contas (art. 6º, X, LGPD), espera-se que os agentes de tratamento de dados demonstrem todas as medidas eficazes e capazes de comprovar o cumprimento da lei e a eficácia das medidas aplicadas.

3.3.3 Direito dos titulares dos dados

O titular dos dados pode exercer os direitos abaixo em relação aos seus dados tratados, a qualquer momento e mediante requisição ao responsável pelo tratamento (art. 18, LGPD) ou mediante movimentação do Judiciário pelo direito de petição.

Pelo direito de ser informado (arts. 9º e 18, VII, da LGPD)[337], a lei confere ao titular o direito de acesso facilitado, disponibilizado de forma clara, adequada e ostensiva a informações como: (i) finalidade, forma e duração do tratamento - ressalvados os segredos comercial e industrial -; (ii) identificação e informações de contato responsável pelo tratamento; (iii) informações acerca do compartilhamento dos seus dados, finalidade desse compartilhamento e responsabilidades dos agentes de tratamento envolvidos e (iv) como exercer outros direitos previstos na Lei, com menção explícita aos direitos do art. 18 da LGPD.

O direito de confirmação e o direito de acesso (art. 18, I e II, da LGPD)[338] asseguram ao titular o direito de ter a confirmação sobre a existência de tratamento dos seus dados pessoais, assim como poderá solicitar acesso aos dados sob tratamento, se for o caso.

---

[333] Ibidem.
[334] Ibidem.
[335] BRASIL. Lei n. 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD), op. cit.
[336] Ibidem.
[337] Ibidem.
[338] Ibidem.

O direito à retificação (art. 18, III, da LGPD)[339], fundamentado no princípio da qualidade dos dados, que garante o tratamento de dados exatos, claros e atualizados, permite ao titular a correção de dados incompletos, inexatos ou desatualizados.

A Lei garante ao titular o direito de requerer ao agente de tratamento que ele anonimize, bloqueie ou elimine (art. 18, IV, da LGPD)[340] seus dados pessoais sempre que essas informações processadas sejam desnecessárias, excessivas ou tratadas em desconformidade com a LGPD.

Pelo direito de revogação do consentimento (art. 18, IX, da LGPD)[341] deve ser garantido ao titular a possibilidade de, a qualquer momento, revogar seu consentimento de forma gratuita e facilitada. Deve estar claro que a base legal autorizadora do tratamento seja o consentimento, de modo que, em caso de outra base legal, pela lógica, não há possibilidade de revogação. Além disso, o titular tem o direito de pedir a eliminação dos dados tratados mediante o consentimento anteriormente concedido (art. 18, VI, da LGPD)[342].

O responsável pelo tratamento deve garantir que o titular possa exercer seu direito de oposição (art. 18, §2º, da LGPD)[343] ao tratamento realizado com fundamento em alguma base legal que não a do consentimento, já que nesta o tratamento só se inicia com a concordância do titular e a ele é concedido o direito de revogação. Contudo, vale lembrar que esse direito somente pode ser exercido caso tenha havido um descumprimento da LGPD.

O titular tem o direito de solicitar que seus dados sejam transmitidos, gratuitamente, para outros fornecedores de serviço ou produto, a depender do seu interesse, observados os segredos comercial e industrial (art. 18, V, LGPD)[344].

Por fim, considerado importante para o tema da presente pesquisa, no caso de tomada de decisões baseadas unicamente no tratamento automatizado de dados pessoais (como, por exemplo, tomadas de decisão com base em sistemas de reconhecimento facial sem supervisão humana), o titular tem o direito de requerer revisão da decisão automatizada (art. 20 da LGPD)[345], caso essa afete seus interesses, bem como esclarecimentos sobre os critérios e procedimentos usados. Esse direito de explicação impõe que as informações sejam prestadas de uma forma facilmente acessível, observados os segredos comercial e industrial, tornando compreensível para o titular a lógica do procedimento automatizado de dados pessoais e os

---

339 Ibidem.
340 Ibidem.
341 BRASIL. Lei n. 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD), op. cit.
342 Ibidem.
343 Ibidem.
344 Ibidem.
345 Ibidem.

critérios utilizados. O texto da lei deixa claro que, em caso de não oferecimento das informações baseado na observância de segredo comercial e industrial, a ANPD poderá "realizar auditoria para verificação de aspectos discriminatórios em tratamento automatizado de dados pessoais"[346].

3.3.4 Relatório de Impacto a Proteção de Dados (RIPD)

Além da garantia aos direitos dos titulares previstos pela LGPD, as empresas devem estar atentas para a condução de um Relatório de Impacto a Proteção de Dados (RIPD), conforme previsto no art. 5º, XVII, da LGPD[347]. O RIPD, baseado no *Data Protection Impact Assessment* - "DPIA", é um documento que deve ser elaborado pelo controlador com a finalidade de descrever os processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais dos titulares de dados tratados, além de conter informações sobre as medidas, salvaguardas e mecanismos de mitigação implementados para reduzir os riscos previamente identificados.

O art. 38, parágrafo único, da LGPD[348], apresenta o conteúdo mínimo do RIPD, que engloba: (i) a descrição dos tipos de dados coletados; (ii) o ciclo de vida dos dados pessoais cujo tratamento pode gerar riscos aos seus titulares; (iii) as medidas de mitigação implementadas para os riscos mapeados e (iv) uma avaliação das medidas acerca da sua capacidade de efetivamente mitigar ou eliminar tais riscos.

Embora a LGPD não informe quais situações específicas que implicam em riscos às liberdades civis e aos direitos fundamentais dos titulares, que determinaria a elaboração do relatório, a ANPD, na recente Resolução CD/ANPD nº 4/2023[349], ao fornecer critérios para mensurar a gravidade das infrações (art. 8º), dispõe, no art. 8º, §2º, que uma infração será considerada média quando

> puder afetar significativamente interesses e direitos fundamentais dos titulares de dados pessoais, caracterizada nas situações em que a atividade de tratamento puder impedir ou limitar, de maneira significativa, o exercício de direitos ou a utilização de um serviço, assim como ocasionar danos materiais ou morais aos titulares, tais como

---

[346] Ibidem.
[347] BRASIL. Lei n. 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD), op. cit.
[348] Ibidem.
[349] AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. Ministério da Justiça e Segurança Pública. Resolução CD/ANPD nº 4/2023, 27 de fevereiro de 2023. Aprova o Regulamento de Dosimetria e Aplicação de Sanções Administrativas. **Diário Oficial da União**: Brasília, DF, 27 fev. 2023. Disponível em: https://www.in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-4-de-24-de-fevereiro-de-2023-466146077. Acesso em: 29 abr. 2023.

> discriminação; violação à integridade física; ao direito à imagem e à reputação; fraudes financeiras ou uso indevido de identidade, desde que não seja classificada como grave[350].

Ademais, por meio da Resolução nº 2/2022, a ANPD apresenta o que se entende por "alto risco" e, portanto, ensejaria a produção do RIPD. Segundo o art. 4º da Resolução CD/ANPD nº 2/2022, o tratamento de dados pessoais será considerado de alto risco quando preenchidos, cumulativamente, ao menos um dos critérios gerais e um dos critérios específicos. O mesmo artigo dispões que os critérios gerais são: (i) tratamento de dados pessoais em larga escala, assim considerados quando apresentam número significativo de titulares, alto volume de dados envolvidos e grande ou alta duração, frequência e extensão geográfica; (ii) tratamento de dados pessoais que possa afetar significativamente interesses e direitos fundamentais dos titulares, ou seja, quando impedir o exercício de direitos ou a utilização de um serviço, ocasionar danos materiais ou morais aos titulares, gerar discriminação, gerar violação à integridade física, ao direito de imagem e à reputação do titular e/ou gerar fraudes financeiras ou roubo de identidade. Enquanto que os critérios específicos são definidos como: (a) uso de tecnologias emergentes ou inovadoras; (b) vigilância ou controle de zonas acessíveis ao público; (c) decisões tomadas unicamente com base em tratamento automatizado; (d) tratamento de dados pessoais sensíveis, de crianças, adolescentes e/ou idosos[351].

Uma vez que algumas dessas situações apresentadas pela ANPD estejam presentes no tratamento de dados pessoais, será possível afirmar que a atividade conduzida se revela como um risco às liberdades civis e aos direitos fundamentais dos titulares e, portanto, necessariamente deve ser conduzido um Relatório de Impacto. Considerando os riscos intrínsecos aos sistemas de reconhecimento facial, já discutidos no primeiro tópico desta dissertação, e considerando o tratamento de dados sensíveis do tipo biometria facial, mostra-se evidente a obrigatoriedade de elaboração de um RIPD nestes casos.

3.3.5 Segurança da Informação e *privacy by design*

No Brasil, a LGPD regulamenta os dados biométricos em razão de estarem listados na definição de dados sensíveis, sem dar-lhes uma definição ou qualquer regulamentação

---

[350] Ibidem.

[351] AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. Ministério da Justiça e Segurança Pública. Resolução CD/ANPD nº 2/2023, 27 de janeiro de 2022. Aprova o Regulamento de aplicação da Lei nº 13.709, de 14 de agosto de 2018, Lei Geral de Proteção de Dados Pessoais (LGPD), para agentes de tratamento de pequeno porte. **Diário Oficial da União**: Brasília, DF, 27 jan. 2022. Disponível em: https://www.in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-2-de-27-de-janeiro-de-2022-376562019#wrapper. Acesso em: 29 abr. 2023.

específica que determine técnicas especializadas para sua proteção, por exemplo, a obrigatoriedade de implementação de criptografia para os conjuntos de dados para se evitar qualquer invasão de terceiros ou vazamentos indesejados, embora isso seja visto como uma medida de segurança apropriada para o caso.

Portanto, espera-se que as empresas, ao tratarem dados biométricos, adotem as melhores práticas em proteção de dados pretendidas pela LGPD, o que inclui medidas adequadas de segurança da informação, conforme dispõe o art. 47 da LGPD: "os agentes de tratamento ou qualquer outra pessoa que intervenha em uma das fases do tratamento obriga-se a garantir a segurança da informação prevista nesta Lei em relação aos dados pessoais, mesmo após o seu término"[352].

Como visto anteriormente, a segurança dos dados foi enunciada na LGPD como um princípio, de modo que se entende por segurança a "utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão"[353], conforme art. 6º, VII, da LGPD. Apesar da LGPD não definir o que se entende por medidas técnicas e administrativas, a Lei expressou que a ANPD poderá dispor sobre esses padrões para que se tornem aplicáveis.

Como pontuou Ricardo Villas Bôas Cueva, "a segurança da informação é indissociável da proteção de dados pessoais. É um pré-requisito, uma condição de possibilidade para que se tutelem efetivamente os direitos dos titulares dos dados pessoais"[354].

Além da proteção aos titulares, as medidas de segurança também são necessárias para a proteção das próprias empresas, que podem ter altos impactos financeiros e reputacionais nos seus negócios ao terem informações vazadas, por exemplo, por sofrer ataques cibernéticos[355].

Somado às duas importâncias referidas acima, o tratamento de dados pessoais será considerado irregular se não for realizado conforme os termos da Lei e deixar de fornecer a segurança esperada pelo titular dos dados, considerando o modo de tratamento, o resultado e os

---

[352] BRASIL. Lei n. 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD), op. cit.
[353] Ibidem.
[354] CUEVA, Ricardo Villas Bôas. Segurança da Informação e Proteção de Dados Pessoais. *In*: FRANCOSKI, Denise; TASSO, Fernando. **A Lei Geral de Proteção de Dados Pessoais:** Aspectos Práticos e Teóricos Relevantes no Setor Público e Privado. São Paulo: Editora Revista dos Tribunais, 2021. Disponível em: https://www.jusbrasil.com.br/doutrina/secao/capitulo-20-seguranca-da-informacao-e-protecao-de-dados-pessoais-parte-i-a-lei-geral-de-protecao-de-dados-pessoais-no-setor-publico/1279975775#a-263118669. Acesso em: 30 abr. 2023.
[355] PRADO, Viviane Muller; DUTRA, Marcos Galileu Lorena. Compliance de Dados e Governança Corporativa. *In*: FRAZÃO, Ana; CUEVA, Ricardo. **Compliance e Políticas de Proteção de Dados**. São Paulo: Editora Revista dos Tribunais, 2022. Disponível em: https://www.jusbrasil.com.br/doutrina/compliance-e-politicas-de-protecao-de-dados/1506551345. Acesso em: 30 abr. 2023.

riscos razoavelmente esperados e as técnicas disponíveis à época (art. 44 da LGPD[356]). Portanto, o responsável pelo tratamento dos dados responde pelos danos causados pela violação da segurança dos dados[357].

Nesse sentido, a adequação à LGPD exige a implementação de uma Política de Segurança da Informação (PSI) bem delimitada na condução das atividades da empresa, cujo objetivo é garantir a confidencialidade, integridade, disponibilidade das informações, por meio de um conjunto de práticas de (i) armazenamento e utilização de dados adequada, (ii) descarte seguro de informações e documentos, (iii) uso de serviços em nuvem protegido, (iv) sistemas seguros, (v) restrições de acesso e uso, (vi) pseudonimização e anonimização[358], (vii) conscientização contínua de pessoal, (viii) monitoramento e auditoria periódica do cumprimento com a Política, (ix) gestão e resposta a incidentes de segurança da informação, entre outros.

Mais que isso, as medidas de segurança para os dados "deverão ser observadas desde a fase de concepção do produto ou do serviço até a sua execução" (art. 46, §2º, da LGPD)[359]. Isto significa que as ações deverão estar "alinhadas à lógica do *privacy by design* – que preconiza que a privacidade e a proteção de dados devem ser consideradas desde a concepção e durante todo o ciclo de vida do projeto, sistema, serviço, produto ou processo – [...]"[360]. Essa abordagem assegura que a privacidade e os dados pessoais sejam protegidos de forma integrada e automática aos sistemas, por padrão (*by default*).

Na prática, portanto, os procedimentos de segurança da informação devem ser seguidos e incorporados, desde o início das operações de tratamento, não só para a proteção de dados pessoais e da própria empresa, como também para a prevenção da concretização de danos, de acordo com o princípio da prevenção (art. 6º, VIII, da LGPD)[361].

3.4 *Compliance*, governança e boas práticas no uso de tecnologias de reconhecimento facial

[356] BRASIL. Lei n. 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD), op. cit.
[357] LGPD, Art. 44, parágrafo único: "Responde pelos danos decorrentes da violação da segurança dos dados o controlador ou o operador que, ao deixar de adotar as medidas de segurança previstas no art. 46 desta Lei, der causa ao dano". Ibidem.
[358] LGPD, Art. 11, §3º: "A autoridade nacional poderá dispor sobre padrões e técnicas utilizados em processos de anonimização e realizar verificações acerca de sua segurança, ouvido o Conselho Nacional de Proteção de Dados Pessoais". Ibidem.
[359] Ibidem.
[360] TEFFÉ, op. cit.
[361] BRASIL. Lei n. 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD), op. cit.

Ana Frazão[362] escreveu a definição simplificada de *compliance* como "um conjunto de ações a serem adotadas no ambiente corporativo para que se reforce a anuência da empresa à legislação vigente, de modo a prevenir a ocorrência de infrações ou, já tendo ocorrido o ilícito, propiciar o imediato retorno ao contexto de normalidade e legalidade"[363]. Além disso, a autora complementa que o termo não se resume somente nessa definição simplificada de observância às leis, já que, mais do que isso,

> o *compliance* também tem por objetivo criar, difundir e consolidar uma cultura e uma prática de respeito às normas jurídicas e éticas, razão pela qual comumente é baseado em códigos de ética ou princípios, cuja finalidade é mostrar como os objetivos empresariais de cada agente econômico podem e devem ser buscados de forma compatível com a preservação dos valores defendidos pela organização[364].

Portanto, o *compliance* de uma empresa em relação a proteção de dados pessoais deve ir além do mero cumprimento com as disposições da LGPD, mas também ser voltado para esclarecer, no ambiente empresarial, a real importância de cumprimento com as regras e de se conferir proteção aos dados pessoais, de modo que "além de ser fundamental para a tutela dos importantes objetivos previstos pela legislação, ainda pode criar valor para a empresa, tornando-se importante vetor de reputação, competitividade e posicionamento no mercado"[365].

Ressalta-se, pois, que seguir as normas e regulamentos é apenas um aspecto da conformidade regulatória. O setor privado deve estar atento a todo o arcabouço regulatório pertinente à sua atividade, o que inclui leis, regulamentos, diretrizes e práticas recomendadas aplicáveis ao setor em que atua, entre as quais destacam-se a LGPD, as orientações da ANPD e, no que couber, as melhores práticas internacionais. Em complementação, a criação de normas internas, como códigos de ética e conduta, é uma forma de reforçar o cumprimento das normas regulatórias do setor, bem como prevenir comportamentos negativos, desvios de conduta e outras ilegalidades dentro do ambiente empresarial e laboral. Essas diligências ainda contribuem com o alinhamento de mentalidade dos envolvidos - interna e externamente -, conduzindo para uma governança corporativa em proteção de dados.

---

[362] FRAZÃO, Ana. 1. Propósitos, Desafios e Parâmetros Gerais dos Programas de Compliance e das Políticas de Proteção de Dados. *In:* FRAZÃO, Ana; CUEVA, Ricardo. **Compliance e Políticas de Proteção de Dados**. São Paulo: Editora Revista dos Tribunais, 2022. Disponível em: https://www.jusbrasil.com.br/doutrina/compliance-e-politicas-de-protecao-de-dados/1506551345. Acesso em: 29 abr. 2023

[363] Ibidem.

[364] Ibidem.

[365] Ibidem.

Nesse sentido, art. 50 da LGPD[366] menciona a possibilidade de criação e implementação de regras de boas práticas e governança que estabeleçam (i) as condições de organização, (ii) o regime de funcionamento, (iii) os procedimentos, incluindo reclamações e petições de titulares, (iv) as normas de segurança, (v) os padrões técnicos, (vi) as obrigações específicas para os diversos envolvidos no tratamento, (vii) as ações educativas, (viii) os mecanismos internos de supervisão e de mitigação de riscos, além de outros aspectos relacionados ao tratamento de dados pessoais. Observa-se que há liberdade de criação para a empresa ponderar essas regras de acordo com a natureza, escopo, finalidade e probabilidade e gravidade dos riscos e dos benefícios decorrentes de tratamento de dados pessoais[367].

Todos os esforços podem "evitar os riscos associados à não conformidade regulatória, por exemplo, multas, restrições, perda da confiança do consumidor e de clientes e diminuição de oportunidades de negócios"[368]. Desde fevereiro de 2023, a ANPD pode aplicar sanções com base no novo Regulamento de Dosimetria e Aplicação de Sanções Administrativas publicado (Resolução CD/ANPD nº 4/2023[369]). A elaboração desse regulamento tem base nos arts. 52 e 53 da LGPD[370] e no art. 51 do Regimento Interno da ANPD (Portaria nº 1/2021[371]) e complementa os art. 32, 55 e 62 da Resolução CD/ANPD nº 1/2021[372], que aprovou o Regulamento do Processo de Fiscalização e do Processo Administrativo Sancionador no âmbito da ANPD. Portanto, a ANPD pode efetivamente impor sanções administrativas (advertência, multa simples, multa diária, publicização da infração e bloqueio, eliminação, suspensão ou proibição das operações com dados) a empresas que não estejam cumprindo a LGPD e as melhores práticas em privacidade e proteção de dados.

Como foi visto no decorrer do presente trabalho, diversos atores ao redor do mundo têm trabalhado para desenvolver boas práticas no uso de tecnologias de reconhecimento facial. Embora os modelos regulatórios possam variar consideravelmente, é possível extrair

---

366 BRASIL. Lei n. 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD), op. cit.
367 Ibidem.
368 TEFFÉ, op. cit.
369 AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. Ministério da Justiça e Segurança Pública. Resolução CD/ANPD nº 4/2023, 27 de fevereiro de 2023, op. cit.
370 BRASIL. Lei n. 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD), op. cit.
371 AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. Ministério da Justiça e Segurança Pública. Portaria nº 1, de 8 de março de 2021. Estabelece o Regimento Interno da Autoridade Nacional de Proteção de Dados - ANPD. **Diário Oficial da União**: Brasília, DF, 8 mar. 2021. Disponível em: https://www.in.gov.br/en/web/dou/-/portaria-n-1-de-8-de-marco-de-2021-307463618. Acesso em: 30 abr. 2023.
372 AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. Ministério da Justiça e Segurança Pública. Resolução CD/ANPD nº 1, de 28 de outubro de 2021. Aprova o Regulamento do Processo de Fiscalização e do Processo Administrativo Sancionador no âmbito da Autoridade Nacional de Proteção de Dados. **Diário Oficial da União**: Brasília, DF, 28 out. 2021. Disponível em: https://in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-1-de-28-de-outubro-de-2021-355817513. Acesso em: 30 abr. 2023.

convergência no entendimento do que consiste a adequação com boas práticas em relação à proteção dos dados pessoais sensíveis de biometria facial ao adotar tecnologias de reconhecimento facial nas atividades do setor privado.

Fábio L. B. Pereira e Cecília A. C. Silva[373] recomendam como melhores práticas, em caso de coleta de dados biométricos: (i) obter o consentimento prévio dos titulares antes da utilização da tecnologia de reconhecimento facial, assim como documentar todo o processo de tratamento, explicando claramente as razões para a utilização da tecnologia; (ii) avisar as pessoas, de forma clara e visível, a respeito da utilização de reconhecimento facial e do seu objetivo; (iii) explicar, de forma clara, todas as capacidades e limitações da tecnologia para todas as partes envolvidas no tratamento dos dados; (iv) informar previamente os titulares dos dados quando a tecnologia de reconhecimento facial for utilizada em ambientes públicos ou comerciais; (v) elaborar relatório de impacto sobre a proteção de dados pessoais; e (vi) adotar todos os esforços técnicos e medidas de segurança da informação para que não ocorram vazamentos de dados ou violações dos direitos dos titulares.

O IDEC e o Internetlab[374], em parceria, estabeleceram nove condutas de boas práticas para empresas que oferecem produtos e serviços com base em tecnologias de reconhecimento facial. Assim, ressaltam que (i) seja feita uma análise prévia para (a) avaliar a proporcionalidade e a necessidade de uso da tecnologia em consideração a outras maneiras menos invasivas à privacidade, bem como para (b) verificar se a implementação da tecnologia está de acordo com os princípios da matéria, principalmente da LGPD. A segunda proposta de conduta é para que as empresas (ii) sejam transparentes e prestem informações completas e precisas, assim as pessoas serão capazes de tomar suas próprias decisões conscientemente. Nesse sentido, as informações devem conter

> a utilização de dispositivos de coleta de imagens; quais dados são coletados, sua forma de tratamento e as finalidades para as quais este é realizado; o prazo e as condições de armazenamento e descarte, como as medidas de segurança adotadas para a sua proteção; as hipóteses de compartilhamento com terceiros; os direitos dos titulares sobre seus dados e, finalmente; os riscos envolvidos neste tratamento de dados[375].

O IDEC e o Internetlab também consideraram como boa prática a (iii) "transparência pública", que "incluem (mas não se limitam a) ferramentas como o Relatório de Impacto à Proteção de Dados Pessoais, práticas de transparência contínua e a instituição de órgãos internos

[373] PEREIRA; SILVA, op. cit.
[374] SIMÃO; FRAGOSO; ROBERTO, op. cit.
[375] Ibidem, p. 54.

independentes"[376]. Recomendam também a (iv) obtenção, antes da captura de imagens, de consentimento livre, expresso, informado e, por se tratar de dados sensíveis, de forma específica e em destaque[377]. Além disso, (v) a instalação de câmeras deve ocorrer em locais que possibilitem o consentimento prévio dos titulares, mas este não deverá ser condição para acesso a serviços.

A sexta proposta de conduta, segundo o IDEC e o Internetlab, é para que as empresas (vi) implementem medidas antidiscriminatórias, por exemplo, as tecnologias de reconhecimento facial "não devem ser utilizadas, direta ou indiretamente, e sob qualquer hipótese, para a negação de bens ou serviços, variação de preços ou oferecimento de condições desvantajosas"[378]. Sugere-se, ainda, que (vii) o armazenamento dos dados biométricos ocorra pelo menor prazo possível, em locais seguros e criptografados, idealmente sempre *offline* ou com conexão criptografada. Ainda neste item, a responsabilização e prestação de contas (*accountability*) são consideradas boas práticas que devem ser cumpridas por meio de auditorias independentes e regulares nos sistemas da empresa, bem como por meio da publicação dos resultados. As recomendações também são no sentido de que os dados biométricos não devem ser compartilhados para outras finalidades além daquelas que foram consentidas pelos titulares e, em nenhuma hipótese, para fins de vigilância e segurança pública em geral[379].

O IDEC e o Internetlab compreendem que (viii) o reconhecimento facial de crianças e adolescentes somente é permitido com o consentimento específico dos pais ou responsável legal dado antes do alcance das câmeras, conforme interpretação da lei. O consentimento "abarcará somente a captura da imagem e sua posterior exclusão, não podendo envolver o uso de dados pessoais de crianças e adolescentes para finalidades comerciais, especialmente para direcionamento de publicidade"[380].

---

[376] Ibidem, p. 55.

[377] O consentimento será: (i) livre quando dado de forma espontânea e sem qualquer tipo de repressão ou coação; (ii) informado quando dado após o titular obter informações claras e precisas, com linguagem acessível e facilmente compreendida; (iii) inequívoco quando o modo de manifestação for possível de comprovar, sem ambiguidades e confusões; (iv) específico quando for minucioso e detalhado, bem como garantir a separação clara de informações relacionadas à obtenção de consentimento obtido. O consentimento deverá ser fornecido por escrito ou por outro meio que demonstre a manifestação de vontade do titular dos dados pessoais (art. 8º, LGPD). Caso o consentimento seja fornecido por escrito, esse deverá constar de cláusula destacada das demais cláusulas contratuais (art. 8º, §1º, LGPD). Além disso, o consentimento deverá referir-se a finalidades determinadas, sendo que as autorizações genéricas para o tratamento de dados pessoais serão nulas (art. 8º, §4º, LGPD). LGPD, Art. 5º, V: "titular: pessoa natural a quem se referem os dados pessoais que são objeto de tratamento". BRASIL. Lei n. 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD), op. cit.

[378] SIMÃO; FRAGOSO; ROBERTO, op. cit., p. 59.

[379] Ibidem, p. 61-62.

[380] Segundo o IDEC e o Internetlab, "dados pessoais sobre crianças e adolescentes não poderão ser utilizados para quaisquer finalidades comerciais, incluindo qualquer forma de pesquisa de mercado, direcionamento de publicidade ou inteligência de negócios", conforme art. 37, §2º, do Código de Defesa do Consumidor, Resolução nº 163/2014 do Conanda e art. 14, *caput*, da LGPD. Ibidem, p. 63.

Por fim, o IDEC e o Internetlab estabelecem que todo e qualquer (ix) incidente de segurança deve ser investigado, eliminado ou minimizado e informado para as autoridades públicas, sociedade civil e titulares dos dados - especialmente se acarretar risco ou dano relevante nos termos do art. 48 da LGPD[381].

O Quadro 6 a seguir faz um resumo do que se pode considerar como regras e boas práticas a serem seguidas para a implementação de sistemas de reconhecimento facial de modo a proteger os dados pessoais biométricos faciais.

Quadro 6 - Boas práticas em proteção de dados biométricos no uso de tecnologias de reconhecimento facial

Recomendação	Justificativa legal (LGPD)
Ter uma finalidade específica, explícita e legítima	Adequação ao princípio da finalidade (art. 6º)
Verificar se é necessário para cumprir a finalidade ou se existem meios alternativos mais seguros para isso	Adequação ao princípio da necessidade e adequação (art. 6º)
Manter registro dos processos de tratamento de dados conduzido	Adequação ao princípio da responsabilização e prestação de contas (art. 6º)
Identificar uma base legal específica para a finalidade desempenhada e cumprir com seus requisitos	Adequação ao art. 11 e, quando se tratar de dados de crianças e adolescentes, art. 14.
Identificar as condições de tratamento de dados biométricos	Adequação ao princípio da transparência (art. 6º)
Garantir que o sistema seja tecnicamente eficaz e suficientemente preciso estatisticamente	Adequação ao princípio da segurança (arts. 6º e 46 a 49)
Fornecer informações claras e acessíveis sobre o tratamento dos dados pessoais	Adequação ao princípio da transparência (art. 6º)
Cumprir com os princípios de proteção de dados	Adequação ao art. 6º
Garantir os direitos dos titulares	Adequação aos arts. 18 a 22
Conduzir Relatório de Impacto para avaliação de riscos aos direitos e liberdades dos titulares dos dados e implementação de medidas de mitigação	Adequação aos arts. 5º e 38

[381] Ibidem, p 64.

Adotar uma Política de Segurança da Informação	Adequação aos arts. 46 a 51
Adotar *Privacy by design and by default*	Adequação aos arts. 46 a 51
Implementar código de ética e conduta sobre proteção de dados	Adequação à toda LGPD

Fonte: elaborado pela autora.

4 CONCLUSÃO

A pesquisa demonstrou que os sistemas de reconhecimento facial exigem reflexões tanto em termos do funcionamento da técnica da tecnologia na prática quanto na finalidade pretendida na sua implementação por uma empresa. Isso porque, a depender do contexto, os riscos aos direitos e liberdades fundamentais serão em maior ou menor quantidade e grau. Por exemplo, um sistema de reconhecimento facial destinado à autenticação de pessoas está atrelado a um ambiente possivelmente mais controlado em relação àquele que é destinado à identificação de pessoas a partir de um banco de dados de rostos. Além disso, o oferecimento de um serviço de sistema de reconhecimento facial por uma empresa para seus clientes também é uma situação diferente da implementação desse sistema para a segurança privada da própria empresa, já que são finalidades e expectativas distintas.

A pesquisa também mostrou que, na UE, nos EUA e no Brasil, as legislações sobre privacidade e proteção de dados, como o GDPR (UE), CCPA (CA, EUA), BIPA (IL, EUA), ESHB (WA, EUA), BUS&COM (TX, EUA) e LGPD (BR), são, até o momento, a base da regulamentação da implementação de tecnologias de reconhecimento facial pelas empresas em cada uma dessas localidades. Contudo, existem movimentações legislativas, na UE, nos EUA e no Brasil, para que essa regulamentação seja específica e preencha as lacunas deixadas pelas leis de privacidade e proteção de dados, tanto em relação aos dados biométricos quanto em relação às inteligências artificiais.

No Brasil, foram mapeados (Quadro 5) 42 (quarenta e dois) Projetos de Leis relacionados ao reconhecimento facial, dados biométricos e inteligência artificial, sendo a maioria destinada ao seu uso pelo setor público. Entretanto, em certa medida também são importantes para o setor privado que é o principal fornecedor dessa tecnologia para o setor público, de tal modo que qualquer proibição, restrição ou permissão de uso de sistemas de reconhecimento facial pelo setor público acaba afetando indiretamente as empresas, além de possivelmente apresentarem um termômetro para a regulamentação no uso privado. Ademais, os PLs nº 12/2015 e nº 21/2020 foram os grandes destaques, embora ainda estejam em debate. O PL nº 12/2015 propõe a criação de regras para usuários e administradores de sistemas de reconhecimento biométrico, incluindo o facial. Por sua vez, o objetivo do PL nº 21/2020 é estabelecer princípios, direitos, deveres e instrumentos de governança para a IA, garantindo o respeito aos direitos humanos, valores democráticos, transparência e privacidade de dados.

Proibições para o uso de sistemas de reconhecimento facial foram encontradas em legislações de cidades dos EUA (São Francisco, Boston e Minnesota), contudo tais restrições

se destinam aos casos de uso pelo setor público, além de não serem absolutas, havendo hipóteses permitidas com autorização das autoridades. A partir dessas três experiências, é possível identificar a diferença de rigor e exigências entre as legislações, bem como extrair os conteúdos mínimos de documentações exigidas, como de relatórios e de políticas de impacto de tecnologias de vigilância (Quadro 4).

Mesmo diante da ausência de regulamentação específica no Brasil, a pesquisa demonstrou que a adequação de uma empresa às melhores práticas em proteção de dados biométricos não é uma tarefa trivial. A prática demanda árduo e longo trabalho, bem como exige o envolvimento de todos os cargos e setores de uma empresa (por exemplo, diretoria, informática, comercial) e de diferentes profissionais em vários campos de atuação (por exemplo, advogados, DPO, técnicos de informática). A dificuldade também reside nas diferentes possibilidades para a tecnologia, considerando a técnica e as finalidades, em conjunto com a significativa quantidade de medidas impostas para o tratamento de dados sensíveis, como adequação aos princípios, definição de base legal, garantia aos direitos dos titulares de dados, condução e atualização de relatórios, documentos e políticas, sendo todas medidas primordiais de *compliance*, governança e boas práticas.

Por fim, a pesquisa demonstrou que as boas práticas em proteção de dados biométricos faciais se resumem a (Quadro 6): (i) ter uma finalidade específica, explícita e legítima; (ii) verificar se é necessário para cumprir a finalidade ou se existem meios alternativos mais seguros para isso; (iii) manter registro dos processos de tratamento de dados conduzido; (iv) identificar uma base legal específica para a finalidade desempenhada e cumprir com seus requisitos; (v) identificar as condições de tratamento de dados biométricos; (vi) garantir que o sistema seja tecnicamente eficaz e suficientemente preciso estatisticamente; (vii) fornecer informações claras e acessíveis sobre o tratamento dos dados pessoais; (viii) cumprir com os princípios de proteção de dados; (ix) garantir os direitos dos titulares; (x) condução de Relatório de Impacto para avaliação de riscos aos direitos e liberdades dos titulares dos dados e implementação de medidas de mitigação; (xi) adotar uma Política de de Segurança de Informação; (xii) adotar *privacy by design and by default*; (xiii) implementar código de ética e conduta sobre proteção de dados.

REFERÊNCIAS

ABELLO, Antonio A.; ARAÚJO, Rafael Will Macêdo de.; HIRATA JR., R. **Parecer InternetLab.** Mar, 2021. Disponível em: https://internetlab.org.br/wp-content/uploads/2022/03/Parecer-Metro-de-Sao-Paulo.-Reconhecimento-facial.pdf. Acesso em: 17 jan. 2023.

ALBUQUERQUE, Márcio Pontes de; CANER, Eugenio S.; MELLO, Aline Gesualdi. Análise de Imagens e Visão Computacional. **Centro Brasileiro de Pesquisas Físicas (CBPF),** 2012. Disponível em: https://mesonpi.cat.cbpf.br/e2012/arquivos/g06/CursoE2012-PI.pdf. Acesso em 20 jan. 2023.

AMAZON. Os fatos sobre a tecnologia de reconhecimento facial com inteligência artificial. **AWS**, c2023. Disponível em: https://aws.amazon.com/pt/rekognition/the-facts-on-facial-recognition-with-artificial-intelligence/. Acesso em: 30 abr. 2023.

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. Ministério da Justiça e Segurança Pública. Portaria nº 1, de 8 de março de 2021. Estabelece o Regimento Interno da Autoridade Nacional de Proteção de Dados - ANPD. **Diário Oficial da União**: Brasília, DF, 8 mar. 2021. Disponível em: https://www.in.gov.br/en/web/dou/-/portaria-n-1-de-8-de-marco-de-2021-307463618. Acesso em: 30 abr. 2023.

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. Ministério da Justiça e Segurança Pública. Resolução CD/ANPD nº 1, de 28 de outubro de 2021. Aprova o Regulamento do Processo de Fiscalização e do Processo Administrativo Sancionador no âmbito da Autoridade Nacional de Proteção de Dados. **Diário Oficial da União**: Brasília, DF, 28 out. 2021. Disponível em: https://in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-1-de-28-de-outubro-de-2021-355817513. Acesso em: 30 abr. 2023.

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. Ministério da Justiça e Segurança Pública. Resolução CD/ANPD nº 2/2023, 27 de janeiro de 2022. Aprova o Regulamento de aplicação da Lei nº 13.709, de 14 de agosto de 2018, Lei Geral de Proteção de Dados Pessoais (LGPD), para agentes de tratamento de pequeno porte. **Diário Oficial da União**: Brasília, DF, 27 jan. 2022. Disponível em: https://www.in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-2-de-27-de-janeiro-de-2022-376562019#wrapper. Acesso em: 29 abr. 2023.

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. Ministério da Justiça e Segurança Pública. Resolução CD/ANPD nº 4/2023, 27 de fevereiro de 2023. Aprova o Regulamento de Dosimetria e Aplicação de Sanções Administrativas. **Diário Oficial da União**: Brasília, DF, 27 fev. 2023. Disponível em: https://www.in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-4-de-24-de-fevereiro-de-2023-466146077. Acesso em: 29 abr. 2023.

BACCARIN, Cínthia; CANAVEZ, Luciana Lopes. Instrumentos de Proteção de Direitos Fundamentais na Lei Geral de Proteção de Dados: a finalidade no tratamento de dados pessoais e a inversão na lógica da fiscalização. **Revista Pensamento Jurídico**, São Paulo, v. 16, nº 2, p. 272-299, maio/ago, 2022. Disponível em: https://fadisp.com.br/revista/ojs/index.php/pensamentojuridico/article/view/356. Acesso em: 11 mar. 2023.

BIONI, Bruno Ricardo. **Proteção de dados pessoais:** a função e os limites do consentimento. 2. ed. Rio de Janeiro: Forense, 2020.

BIONI, Bruno Ricardo; RIELLI, Mariana; LUCIANO, Maria. Regulação de reconhecimento facial em São Francisco. **Jota**: *[s.l.]*, 2019. Disponível em: https://www.jota.info/opiniao-e-analise/colunas/agenda-da-privacidade-e-da-protecao-de-dados/regulacao-de-reconhecimento-facial-em-sao-francisco-25062019. Acesso em: 27 abr. 2023.

BOSTON. City of Boston Municipal Code. **American Legal Publishing**, *[s.l.]*, 2020. Disponível em: https://codelibrary.amlegal.com/codes/boston/latest/boston_ma/0-0-0-18988. Acesso em: 21 fev. 2023.

BRASIL. IX Jornada de Direito Civil. Enunciado nº 684. Coordenador Geral Ministro Jorge Mussi. **Conselho da Justiça Federal**: Brasília, DF, 2022. Disponível em: https://www.cjf.jus.br/enunciados/enunciado/1823. Acesso em: 15 mar. 2023.

BRASIL. Câmara dos Deputados. **Projeto de Lei nº 12, de 2 de fevereiro de 2015.** Dispõe sobre a utilização de sistemas de verificação biométrica e dá outras providências. Brasília: Câmara dos Deputados, 2015. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=944254. Acesso em: 29 abr. 2023.

BRASIL. Câmara dos Deputados. **Projeto de Lei nº 240, de 11 de fevereiro de 2020.** Cria a Lei da Inteligência Artificial, e dá outras providências. Brasília: Câmara dos Deputados, 2020. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2236943. Acesso em: 29 abr. 2023.

BRASIL. Câmara dos Deputados. **Projeto de Lei nº 759, de 1 de março de 2023.** Regulamenta os sistemas de Inteligência Artificial, e dá outras providências. Brasília: Câmara dos Deputados, 2023. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2349685. Acesso em: 29 abr. 2023.

BRASIL. Câmara dos Deputados. **Projeto de Lei nº 807, de 4 de abril de 2022.** Estabelece medidas de prevenção e combate ao trabalho infantil em empresas de aplicativos de entregas ou transporte e dá outras providências. Brasília: Câmara dos Deputados, 2022. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2319143. Acesso em: 29 abr. 2023.

BRASIL. Câmara dos Deputados. **Projeto de Lei nº 1.515, de 7 de junho de 2022.** Lei de Proteção de Dados Pessoais para fins exclusivos de segurança do Estado, de defesa nacional, de segurança pública, e de investigação e repressão de infrações penais. Brasília: Câmara dos Deputados, 2022. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2326300. Acesso em: 29 abr. 2023.

BRASIL. Câmara dos Deputados. **Projeto de Lei nº 2.392, de 31 de agosto de 2022.** Dispõe sobre o uso de tecnologias de reconhecimento facial nos setores público e privado. Brasília: Câmara dos Deputados, 2022. Disponível em:

https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2334803. Acesso em: 29 abr. 2023.

BRASIL. Câmara dos Deputados. **Projeto de Lei nº 2.537, de 25 de abril de 2019.** Obriga o aviso sobre o reconhecimento facial em estabelecimentos comerciais. Brasília: Câmara dos Deputados, 2019. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2199418. Acesso em: 29 abr. 2023.

BRASIL. Câmara dos Deputados. **Projeto de Lei nº 3.492, de 21 de março de 2012.** Altera a Lei nº 8.934, de 18 de novembro de 1994, para tornar mais rigorosos os atos empresariais levados a registro nas Juntas Comerciais. Brasília: Câmara dos Deputados, 2012. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=538210. Acesso em: 29 abr. 2023.

BRASIL. Câmara dos Deputados. **Projeto de Lei nº 3.715, de 19 de novembro de 2015.** Altera a Lei nº 7.116, de 29 de agosto de 2013, que assegura a validade nacional as Carteiras de Identidade e regula sua expedição e dá outras providências. Brasília: Câmara dos Deputados, 2015. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2056049. Acesso em: 29 abr. 2023.

BRASIL. Câmara dos Deputados. **Projeto de Lei nº 4.513, de 9 de setembro de 2020.** Institui a Política Nacional de Educação Digital; altera as Leis nºs 9.394, de 20 de dezembro de 1996 (Lei de Diretrizes e Bases da Educação Nacional), 9.448, de 14 de março de 1997, 10.260, de 12 de julho de 2001, e 10.753, de 30 de outubro de 2003; e dá outras providências. Brasília: Câmara dos Deputados, 2020. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2262422. Acesso em: 29 abr. 2023.

BRASIL. Câmara dos Deputados. **Projeto de Lei nº 7.750, de 13 de agosto de 2010.** Estabelece fundamentos, princípios e diretrizes para o desenvolvimento e a aplicação da inteligência artificial no Brasil; e dá outras providências. Brasília: Câmara dos Deputados, 2010. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=484718. Acesso em: 29 abr. 2023.

BRASIL. Constituição da República Federativa do Brasil, de 5 de outubro de 1988. **Diário Oficial da União**, Poder Legislativo, Brasília, DF, 5 out. 1988. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/ConstituicaoCompilado.htm. Acesso em: 30 jan. 2023.

BRASIL. **Congresso Nacional**. Praça dos Três Poderes, Brasília, DF. Disponível em: https://www.congressonacional.leg.br/. Acesso em: 17 mar. 2023.

BRASIL. Lei n. 8.069, de 13 de julho de 1990. Dispõe sobre o Estatuto da Criança e do Adolescente e dá outras providências. **Diário Oficial da União**: Brasília, DF, 13 jul. 1990. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l8069.htm. Acesso em: 15 mar. 2023.

BRASIL. Lei nº 8.078, de 11 de setembro de 1990. Dispõe sobre a proteção do consumidor e dá outras providências. **Diário Oficial da União:** Brasília, DF, 11 set. 1990. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l8078compilado.htm. Acesso em: 13 mar. 2023.

BRASIL. Lei nº 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 União:** Brasília, DF, 9 jun. 2011. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12414.htm. Acesso em: 13 mar. 2023.

BRASIL. Lei nº 12.527, de 18 de novembro de 2011. Regula o acesso a informações previsto no inciso XXXIII do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal; altera a Lei nº 8.112, de 11 de dezembro de 1990; revoga a Lei nº 11.111, de 5 de maio de 2005, e dispositivos da Lei nº 8.159, de 8 de janeiro de 1991; e dá outras providências. **Diário Oficial da União:** Brasília, DF, 18 nov. 2011. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm. Acesso em: 13 mar. 2023.

BRASIL. Lei nº 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. **Diário Oficial da União:** Brasília, DF, 23 abr. 2014. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 13 mar. 2023.

BRASIL. Lei n. 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). **Diário Oficial da União**, Poder Executivo, Brasília, DF, 14 ago. 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709compilado.htm. Acesso em: 18 jan. 2023.

BRASIL. Senado Federal. **Projeto de Lei nº 21, de 4 de fevereiro de 2020.** Altera a Lei nº 8.934, de 18 de novembro de 1994, e a Lei nº 10.406, de 10 de janeiro de 2002 (Código Civil), para atualizar a terminologia referente ao Registro Público de Empresas e Atividades Afins. Brasília: Senado Federal, 2020. Disponível em: https://www25.senado.leg.br/web/atividade/materias/-/materia/151547. Acesso em: 29 abr. 2023.

BRASIL. Senado Federal. **Projeto de Lei nº 676, de 3 de março de 2021.** Altera o Decreto-Lei nº 3.689, de 3 de outubro de 1941 (Código de Processo Penal), para disciplinar o reconhecimento fotográfico de pessoa. Brasília: Senado Federal, 2021. Disponível em: https://www25.senado.leg.br/web/atividade/materias/-/materia/147134. Acesso em: 29 abr. 2023.

BRASIL. Senado Federal. **Projeto de Lei nº 872, 12 de março de 2021.** Dispõe sobre o uso da Inteligência Artificial. Brasília: Senado Federal, 2021. Disponível em: https://www25.senado.leg.br/web/atividade/materias/-/materia/147434. Acesso em: 29 abr. 2023.

BRASIL. Senado Federal. **Projeto de Lei nº 5.051, de 16 de setembro de 2019.** Estabelece os princípios para o uso da Inteligência Artificial no Brasil. Brasília: Senado Federal, 2019. Disponível em: https://www25.senado.leg.br/web/atividade/materias/-/materia/147434. Acesso em: 29 abr. 2023.

BRASIL. Senado Federal. **Projeto de Lei nº 5.691, de 25 de outubro de 2019.** Institui a Política Nacional de Inteligência Artificial. Brasília: Senado Federal, 2019. Disponível em:https://www25.senado.leg.br/web/atividade/materias/-/materia/139586. Acesso em: 29 abr. 2023.

BRASIL. Senado Federal. **Projeto de Lei nº 6.299, de 4 de dezembro de 2019.** Altera a Lei nº 12.587, de 3 de janeiro de 2012, para disciplinar o cadastro de usuários, as informações a serem fornecidas a usuários e a motoristas e as ferramentas de segurança no transporte privado remunerado individual de passageiros. Brasília: Senado Federal, 2019. Disponível em: https://www25.senado.leg.br/web/atividade/materias/-/materia/140072. Acesso em: 29 abr. 2023.

BUX, Udo; MACIEJEWSKI, Mariusz. O ordenamento jurídico e os processos de tomada de decisão da União Europeia. **Parlamento Europeu**, jun. 2022. Disponível em: https://www.europarl.europa.eu/factsheets/pt/sheet/6/as-fontes-e-o-ambito-de-aplicacao-do-direito-da-uniao-europeia. Acesso em: 1º abr. 2023.

CALIFORNIA (State). California Consumer Privacy Act of 2018. **California Legislative Information**, 2018. Disponível em: https://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?division=3.&part=4.&lawCode=CIV&title=1.81.5. Acesso em: 27 abr. 2023.

CÂMARA DOS DEPUTADOS. Projeto condiciona uso de reconhecimento facial a inviabilidade de outros meios de identificação. **Agência Câmara de Notícias**, 6 out. 2022. Disponível em: https://www.camara.leg.br/noticias/911976-PROJETO-CONDICIONA-USO-DE-RECONHECIMENTO-FACIAL-A-INVIABILIDADE-DE-OUTROS-MEIOS-DE-IDENTIFICACAO. Acesso em: 29 abr. 2023

CÂMARA DOS DEPUTADOS. Projeto cria marco legal para uso de inteligência artificial no Brasil. **Agência Câmara de Notícias**, 4 mar. 2020. Disponível em: https://www.camara.leg.br/noticias/641927-projeto-cria-marco-legal-para-uso-de-inteligencia-artificial-no-brasil/. Acesso em: 29 abr. 2023.

CÂMARA DOS DEPUTADOS. Uso irregular de dados de biometria pode acarretar multa de até R$ 10 milhões. **Agência Câmara de Notícias**, 30 abr. 2015. Disponível em: https://www.camara.leg.br/noticias/457188-USO-IRREGULAR-DE-DADOS-DE-BIOMETRIA-PODE-ACARRETAR-MULTA-DE-ATE-R$-10-MILHOES. Acesso em: 29 abr. 2023.

CASTELLS, Manuel. **A sociedade em rede.** v. 1, 8. ed. São Paulo: Paz e Terra, 2005.

CLARK, Alisson. Why the U.S. needs federal regulation of facial recognition — and how to get it right. **University of Florida News**, 7 dec. 2020. Disponível em: https://news.ufl.edu/2020/12/facial-recognition/. Acesso em: 27 abr. 2023.

CNN BRASIL. Elon Musk compra Twitter por US $44 bilhões. **CNN Brasil**, 2022. Disponível em: https://www.cnnbrasil.com.br/business/elon-musk-compra-twitter-por-us-44-bilhoes/. Acesso em 16 jan. 2023.

COMISSÃO EUROPEIA. Orientações éticas para uma IA de confiança. **Comissão Europeia**, 2019. Disponível em: https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai. Acesso em: 25 jan. 2023.

COMISSÃO EUROPEIA. Livro Branco sobre a inteligência artificial: uma abordagem europeia virada para a excelência e a confiança. COM (2020) 65 final. **Comissão Europeia**: Bruxelas, 2020. Disponível em: https://commission.europa.eu/system/files/2020-03/commission-white-paper-artificial-intelligence-feb2020_pt.pdf. Acesso em: 26 abr. 2023.

COMISSÃO EUROPEIA. Uma Definição de IA: principais capacidades e disciplinas científicas. **Comissão Europeia,** 2019. Disponível em: https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai. Acesso em: 27 jan. 2023.

COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS. Reconnaissance faciale: pour un débat à la hauteur des enjeux. **Commission Nationale de l'Informatique et des Libertés (CNIL.)**, 2019. Disponível em: https://www.cnil.fr/fr/reconnaissance-faciale-pour-un-debat-la-hauteur-des-enjeux. Acesso em: 18 jan. 2023

COUNCIL OF EUROPE; EUROPEAN COURT OF HUMAN RIGHTS; EUROPEAN DATA PROTECTION SUPERVISOR; EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS. **Handbook on European data protection law**: 2018 edition. Publications Office of the European Union, 2019. Disponível em: https://data.europa.eu/doi/10.2811/343461. Acesso em 21 abr. 2023.

CUEVA, Ricardo Villas Bôas. Segurança da Informação e Proteção de Dados Pessoais. *In*: FRANCOSKI, Denise; TASSO, Fernando. **A Lei Geral de Proteção de Dados Pessoais:** Aspectos Práticos e Teóricos Relevantes no Setor Público e Privado. São Paulo: Editora Revista dos Tribunais, 2021. Disponível em: https://www.jusbrasil.com.br/doutrina/secao/capitulo-20-seguranca-da-informacao-e-protecao-de-dados-pessoais-parte-i-a-lei-geral-de-protecao-de-dados-pessoais-no-setor-publico/1279975775#a-263118669. Acesso em: 30 abr. 2023.

CUKIER, Kenneth; MAYER-SCHOENBERGER, Victor. The Rise of Big Data: how it's changing the way we think about the world. **Foreign Affairs,** [*S.l*], n. 3, v. 92, may/june 2013. Disponível em: https://www.foreignaffairs.com/articles/2013-04-03/rise-big-data. Acesso em: 9 fev. 2021.

DATA science and AI glossary. **The Alan Turing Institute**, London. Disponível em: https://www.turing.ac.uk/news/data-science-and-ai-glossary. Acesso em: 14 jan. 2023.

DUBALL, Joseph. The rise of US state-level BIPA: Illinois leads, others catching up. **International Association of Privacy Professionals (IAPP)**, 28 mar. 2023. Disponível em: https://iapp.org/news/a/the-rise-of-us-state-level-bipa-illinois-leads-others-catching-up/. Acesso em: 27 abr. 2023.

EUROPEAN COMMISSION. Proposal for a Regulation of the European Parliament and of the Council: Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts. 2021/0106 (COD). **European Commission**: Brussels, 2021. Disponível em: https://digital-

strategy.ec.europa.eu/en/library/proposal-regulation-laying-down-harmonised-rules-artificial-intelligence. Acesso em 26 abr. 2023.

EUROPEAN DATA PROTECTION BOARD; EUROPEAN DATA PROTECTION SUPERVISOR. EDPB-EDPS Joint Opinion 5/2021 on the proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act). **EDPB-EDPS**: Brussels, 2021. Disponível em: https://edps.europa.eu/system/files/2021-06/2021-06-18-edpb-edps_joint_opinion_ai_regulation_en.pdf. Acesso em 26 abr. 2023.

FAZLIOGLU, Müge. US Federal Privacy Legislation Tracker: Introduced in the 117th Congress (2021-2022). **International Association of Privacy Professionals (IAPP)**, dec., 2022. Disponível em: https://iapp.org/resources/article/us-federal-privacy-legislation-tracker/. Acesso em: 27 abr. 2023.

FEDERAL TRADE COMMISSION (FTC). 16 CFR Part 312. Children's Online Privacy Protection Act of 1998. **Electronic Code of Federal Regulations (eCFR)**, Federal Trade Commission, 17 jan. 2013. Disponível em: https://www.ecfr.gov/current/title-16/chapter-I/subchapter-C/part-312. Acesso em: 28 abr. 2023.

FERRASI, Faberson Augusto. **O uso de mídias locativas no universo da internet das coisas:** construindo uma prova de conceito. 53f. Dissertação (Mestrado) - Faculdade de Arquitetura, Artes e Comunicação, Universidade Estadual Paulista, Bauru, 2017. Disponível em: http://hdl.handle.net/11449/150785. Acesso em: 14 jan. 2023.

FRAZÃO, Ana. 1. Propósitos, Desafios e Parâmetros Gerais dos Programas de Compliance e das Políticas de Proteção de Dados. *In:* FRAZÃO, Ana; CUEVA, Ricardo. **Compliance e Políticas de Proteção de Dados**. São Paulo: Editora Revista dos Tribunais, 2022. Disponível em: https://www.jusbrasil.com.br/doutrina/compliance-e-politicas-de-protecao-de-dados/1506551345. Acesso em: 29 abr. 2023

G1. **Latam, Gol e Azul disponibilizam embarque com reconhecimento facial a partir desta terça-feira.** 9 ago. 2022. Disponível em: https://g1.globo.com/turismo-e-viagem/noticia/2022/08/09/gol-disponibiliza-embarque-com-reconhecimento-facial-a-partir-desta-terca-feira.ghtml. Acesso em: 9 jan. 2023.

G1. **A democracia que usa reconhecimento facial para registrar os rostos de seus cidadãos.** 8 ago. 2022. Disponível em: https://g1.globo.com/tecnologia/noticia/2022/08/08/a-democracia-que-usa-reconhecimento-facial-para-registrar-os-rostos-de-seus-cidadaos.ghtml. Acesso em: 9 jan. 2023.

G1. **Metrô de SP adota novo sistema de reconhecimento facial.** 21 nov. 2022. Disponível em: https://g1.globo.com/sp/sao-paulo/sp2/video/metro-de-sp-adota-novo-sistema-de-reconhecimento-facial-11144903.ghtml. Acesso em: 9 jan. 2023.

GARTNER. **Information Technology Glossary.** Disponível em: https://www.gartner.com/en/information-technology/glossary/big-data. Acesso em: 16 jan. 2023.

GLOBAL Privacy Law and DPA Directory. **International Association of Privacy Professionals (IAPP)**, c2023. Disponível em: https://iapp.org/resources/global-privacy-directory/. Acesso em: 13 mar. 2023.

GOLDMAN, Eric. An Introduction to the California Consumer Privacy Act (CCPA). **Santa Clara University School of Law Legal Studies Research Paper Series**, p. 1-7, 1 jul. 2020. Disponível em: http://dx.doi.org/10.2139/ssrn.3211013. Acesso em: 27 abr. 2023.

GROTHER, Patrick; NGAN, Mei; HANAOKA Kayee. Face Recognition Vendor Test (FRVT) Part 3: Demographic effects. **National Institute of Standards and Technology**, Tech. Rep. NISTIR 8280, 2019. Disponível em: https://doi.org/10.6028/NIST.IR.8280. Acesso em: 27 jan. 2023.

HARARI, Yuval Noah. **21 lições para o século 21**. Tradução Paulo Geiger. 1. ed. São Paulo: Companhia das Letras, 2018.

HARCOURT, Bernard E. The expository society. In: HARCOURT, Bernard E. **Exposed**: Desire and Disobedience in the Digital Age. Cambridge: Harvard University Press, 2015.

ILLINOIS (State). Civil liabilities (740 ILCS 14/) Biometric Information Privacy Act, of 3 oct. 2008. **Illinois General Assembly**, Springfield, 3 oct. 2008. Disponível em: https://www.ilga.gov/legislation/publicacts/fulltext.asp?Name=095-0994. Acesso em: 27 abr. 2023

INFORMATION COMMISSIONER'S OFFICE (ico.). Big data, artificial intelligence, machine learning and data protection. v. 2.2. **Information Commissioner's Office (ico.)**, [s/d]. Disponível em: https://ico.org.uk/media/for-organisations/documents/2013559/big-data-ai-ml-and-data-protection.pdf. Acesso em: 16 jan. 2023.

INFORMATION COMMISSIONER'S OFFICE. Guidance on video surveillance (including CCTV). **Information Commissioner's Office (ico.)**, 2022. Disponível em: https://ico.org.uk/media/for-organisations/guide-to-data-protection/key-dp-themes/guidance-on-video-surveillance-including-cctv-1-0.pdf. Acesso em: 16 jan. 2023.

INFORMATION COMMISSIONER'S OFFICE. Guide to the General Data Protection Regulation (GDPR). Special category data. **Information Commissioner's Office (ico.)**, 2022. Disponível em: https://ico.org.uk/media/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr-1-1.pdf. Acesso em: 21 abr. 2023.

INFORMATION COMMISSIONER'S OFFICE. Information Commissioner's Opinion: The use of live facial recognition technology in public places. **Information Commissioner's Office (ico.)**, 2021. Disponível em: https://ico.org.uk/media/2619985/ico-opinion-the-use-of-lfr-in-public-places-20210618.pdf. Acesso em: 2 fev. 2023.

JILLSON, Elisa. Aiming for truth, fairness, and equity in your company's use of AI. **Federal Trade Commission**, 2021. Disponível em: https://www.ftc.gov/business-guidance/blog/2021/04/aiming-truth-fairness-equity-your-companys-use-ai. Acesso em: 27 abr. 2023.

LESLIE, David. Understanding bias in facial recognition technologies: an explainer. **The Alan Turing Institute**, 2020. Disponível em: https://doi.org/10.5281/zenodo.4050457. Acesso em: 16 jan. 2023.

LÉVY, Pierre. **O que é o virtual?** Tradução de Paulo Neves do original "Qu'est-ce le virtuel?". São Paulo: Editora 34, 2003.

MACHADO FILHO, Francisco. As tecnologias da informação e as novas estruturas sociais e econômicas. **Ciência Geográfica**, v. 16, n. 2, p. 155-167, 2012. Disponível em: http://hdl.handle.net/11449/134969. Acesso em: 14 jan. 2023.

MADIEGA, Tambiama; MILDEBRATH, Hendrik. Regulating facial recognition in the EU: in-depth analysis. **European Parliament**, Directorate-General for Parliamentary Research Services, 2022. Disponível em: https://data.europa.eu/doi/10.2861/140928. Acesso em: 25 mar. 2023.

MARZOCCHI, Ottavio. Proteção dos valores referidos no artigo 2.º do TUE na UE. **Parlamento Europeu**, maio de 2022. Disponível em: https://www.europarl.europa.eu/factsheets/pt/sheet/146/protecao-dos-valores-referidos-no-artigo-2.o-do-tue-na-ue. Acesso em: 1º abr. 2023.

MINNEAPOLIS (MN). Ordinance No. 2021-006. Amending Title 2, Chapter 41 of the Minneapolis Code of Ordinances relating to Administration: lnformation Governance. **City of Minneapolis**, 2021. Disponível em: https://lims.minneapolismn.gov/Download/MetaData/20406/2021-006_Id_20406.pdf. Acesso em: 21 fev. 2023.

MÜLLER, Leonardo. Aquisição do WhatsApp pelo Facebook foi finalmente concretizada. **Tecmundo**, 2014. Disponível em: https://www.tecmundo.com.br/whatsapp/64054-aquisicao-whatsapp-facebook-finalmente-concretizada.htm. Acesso em: 16 jan. 2023.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. **NIST Study Evaluates Effects of Race, Age, Sex on Face Recognition Software**. NIST, 2019. Disponível em: https://www.nist.gov/news-events/news/2019/12/nist-study-evaluates-effects-race-age-sex-face-recognition-software. Acesso em: 27 jan. 2023.

OLHAR DIGITAL. Mulher é detida no Rio por erro em câmera de reconhecimento facial. **Olhar Digital**, 10 jul. 2019. Disponível em: https://olhardigital.com.br/2019/07/10/seguranca/mulher-e-detida-no-rio-por-erro-em-camera-de-reconhecimento-facial/. Acesso em: 9 jan. 2023.

ORGANIZAÇÃO DAS NAÇÕES UNIDAS (ONU). **Declaração Universal dos Direitos Humanos**, 1948. Disponível em: https://brasil.un.org/pt-br/91601-declaracao-universal-dos-direitos-humanos. Acesso em: 11 mar. 2023.

O PANÓPTICO. Levantamento revela que 90,5% dos presos por monitoramento facial no Brasil são negros. **O Panóptico**, 21 nov. 2019. Disponível em: https://opanoptico.com.br/exclusivo-levantamento-revela-que-905-dos-presos-por-monitoramento-facial-no-brasil-sao-negros/. Acesso em 9 jan. 2023.

PANAHOV, Huseyn. Why the US Needs Federal Law on Facial Recognition Technology. **Intersect: The Stanford Journal of Science, Technology, and Society**, Stanford University, v. 15, n. 2, p. 1-9, april, 2022. Disponível em: https://ojs.stanford.edu/ojs/index.php/intersect/article/view/2168. Acesso em: 27 abr. 2023.

PEREIRA, Fábio Luiz Barbosa; SILVA, Cecília Alberton Coutinho. Capítulo 24. A Regulação do Reconhecimento Facial e Seus Impactos para os Setores Público e Privado no Brasil: Uma Análise Comparativa Internacional. *In:* FRANCOSKI, Denise; TASSO, Fernando. **A Lei Geral de Proteção de Dados Pessoais:** Lgpd: Aspectos Práticos e Teóricos Relevantes no Setor Público e Privado. São Paulo: Editora Revista dos Tribunais, 2021. Disponível em: https://thomsonreuters.jusbrasil.com.br/doutrina/secao/1279975781/capitulo-24-a-regulacao-do-reconhecimento-facial-e-seus-impactos-para-os-setores-publico-e-privado-no-brasil-uma-analise-comparativa-internacional#a-263118690. Acesso em: 37 abr. 2023.

PÉREZ, Montse Hidalgo. Quantas mensagens de WhatsApp são necessárias para nos identificar? Não muitas. **El País**, Madri, 2021. Disponível em: https://brasil.elpais.com/tecnologia/2021-08-31/quantas-mensagens-de-whatsapp-sao-necessarias-para-nos-identificar-nao-muitas.html?rel=buscador_noticias. Acesso em: 16 jan. 2023.

PESENTI, Jerome. Uma atualização sobre nosso uso de reconhecimento facial. **Meta**, 2021. Disponível em: https://about.fb.com/news/2021/11/update-on-use-of-face-recognition/. Acesso em: 31 jan. 2023.

PINHEIRO, Patrícia Peck. **Proteção de dados pessoais:** comentários à Lei n. 13.709/2018 (LGPD). São Paulo: Saraiva Educação, 2018.

PRADO, Viviane Muller; DUTRA, Marcos Galileu Lorena. Compliance de Dados e Governança Corporativa. *In*: FRAZÃO, Ana; CUEVA, Ricardo. **Compliance e Políticas de Proteção de Dados**. São Paulo: Editora Revista dos Tribunais, 2022. Disponível em: https://www.jusbrasil.com.br/doutrina/compliance-e-politicas-de-protecao-de-dados/1506551345. Acesso em: 30 abr. 2023.

REGULAR a Inteligência Artificial na UE: as propostas do Parlamento. **Parlamento Europeu**, 2023. Disponível em: https://www.europarl.europa.eu/news/pt/headlines/society/20201015STO89417/regular-a-inteligencia-artificial-na-ue-as-propostas-do-parlamento. Acesso em: 27 abr. 2023.

SÃO FRANCISCO. Código Administrativo de São Francisco. Chapter 19B: acquisition of surveillance technology. **American Legal Publishing**, *[s.l.]*, 14 jun. 2019. Disponível em: https://codelibrary.amlegal.com/codes/san_francisco/latest/sf_admin/0-0-0-47320. Acesso em: 21 fev. 2023.

SIMÃO, Bárbara; FRAGOSO, Nathalie; ROBERTO, Enrico. Reconhecimento Facial e o Setor Privado: Guia para a adoção de boas práticas. **InternetLab/IDEC**, São Paulo, 2020. Disponível em: https://idec.org.br/sites/default/files/reconhecimento_facial_diagramacao_digital_2.pdf. Acesso em: 12 jan. 2023.

SMITH, Brad. Reconhecimento facial: é hora de agir. **Microsoft**, 2018. Disponível em: https://blogs.microsoft.com/on-the-issues/2018/12/06/facial-recognition-its-time-for-action/. Acesso em: 31 jan. 2023.

SIMONITE, Tom. Congress Is Eyeing Face Recognition, and Companies Want a Say. **Wired**, New York, 23 nov. 2020. Disponível em: https://www.wired.com/story/congress-eyeing-face-recognition-companies-want-say/. Acesso em: 27 abr. 2023.

SUN, Chen; SHRIVASTAVA, Abhinav; SINGH, Saurabh; GUPTA, Abhinav. Revisiting Unreasonable Effectiveness of Data in Deep Learning Era. **Cornell University**, arXiv, 2. v., aug. 2017. Disponível em: https://doi.org/10.48550/arXiv.1707.02968. Acesso em: 01 fev. 2023.

TEFFÉ, Chiara Spadaccini de. 49. Compliance de Dados em Tecnologias de Segurança e Vigilância. In: FRAZÃO, Ana; CUEVA, Ricardo Villas Bôas. **Compliance e Políticas de Proteção de Dados.** São Paulo: Editora Revista dos Tribunais, 2022. Disponível em: https://thomsonreuters.jusbrasil.com.br/doutrina/secao/1506551452/49-compliance-de-dados-em-tecnologias-de-seguranca-e-vigilancia-parte-v-topicos-especiais-de-compliance-e-politica-de-protecao-de-dados#ftn.DTR.2021.47943-n1. Acesso em 11 mar. 2023

TEXAS. Business and Commerce Code. Chapter 503 Biometric Identifiers, of 1º apr. 2009. **Texas Constitution and Statutes**, Texas, 1º apr. 2009. Disponível em: https://statutes.capitol.texas.gov/Index.aspx. Acesso em: 28 abr. 2023.

THE ALAN TURING INSTITUTE. **Could AI solve your data problems?**. Disponível em: https://www.turing.ac.uk/events/could-ai-solve-your-data-problems. Acesso em: 14 jan. 2023.

THE ECONOMIST. The world's most valuable resource is no longer oil, but data. **The Economist**, 2017. Disponível em: https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data. Acesso em: 16 jan. 2023.

TOFFLER, Alvin. **A terceira onda.** Tradução João Távora. 29 ed. Rio de Janeiro: Record, 2007.

TOMASEVICIUS FILHO, Eduardo. O princípio da boa-fé na Lei Geral de Proteção de Dados. **Jusbrasil**, 2022. Disponível em: https://www.jusbrasil.com.br/artigos/o-principio-da-boa-fe-na-lei-geral-de-protecao-de-dados/1252511524. Acesso em: 14 ago. 2023.

TRIBUNAL SUPERIOR ELEITORAL (TSE). **Glossário Eleitoral.** Disponível em: https://www.tse.jus.br/servicos-eleitorais/glossario/termos-iniciados-com-a-letra-b. Acesso em: 23 jan. 2023.

UNIÃO EUROPEIA. Carta dos Direitos Fundamentais da União Europeia, de 26 de outubro de 2012. **Jornal Oficial da União Europeia**, 26 out. 2012. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX:12012P/TXT#document1. Acesso em: 25 mar. 2023.

UNIÃO EUROPEIA. Diretiva 95/46/CE do Parlamento Europeu e Conselho da União Europeia, de 24 de outubro de 1995. Relativa à protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados. **Jornal Oficial das**

Comunidades Europeias, Parlamento Europeu e Conselho da União Europeia, Luxemburgo, 24 out. 1995. Disponível em: http://data.europa.eu/eli/dir/1995/46/oj. Acesso em: 11 mar. 2023.

UNIÃO EUROPEIA. Regulamento (UE) nº 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016. Relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados). **Jornal Oficial da União Europeia**, Bruxelas, 27 abr. 2016. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX: 32016R0679 & from=PT. Acesso em: 23 jan. 2023.

UNIÃO EUROPEIA. Diretiva (UE) 2016/680 do Parlamento Europeu e do Conselho, de 27 de abril de 2016. Relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas autoridades competentes para efeitos de prevenção, investigação, deteção ou repressão de infrações penais ou execução de sanções penais, e à livre circulação desses dados e que revoga a Decisão-Quadro 2008/977/JAI do Conselho. **Jornal Oficial da União Europeia:** Bruxelas, 27 abr. 2016. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX:32016L0680. Acesso em: 26 mar. 2023.

US Federal Privacy. **International Association of Privacy Professionals (IAPP)**, *[s.d.]*. Disponível em: https://iapp.org/resources/topics/us-federal-privacy/. Acesso em: 27 abr. 2023.

US State Privacy. **International Association of Privacy Professionals (IAPP)**, 2023. Disponível em: https://iapp.org/resources/topics/us-state-privacy/. Acesso em: 27 abr. 2023.

VEMOU, Konstantina; HORVATH, Anna; ZERDICK, Thomas (ed.). EDPS TechDispatch: facial emotion recognition. Issue 1, 2021. **Publications Office of the European Union**, 2012. Disponível em: https://data.europa.eu/doi/10.2804/014217. Acesso em: 2 fev. 2023.

WASHINGTON. Engrossed Substitute House Bill 1493, of 23 jul. 2017. An act relating to biometric identifiers; and adding a new chapter to Title 19 RCW. **Washington State Legislature**, 65th Legislature, Washington, 23 jul. 2017. Disponível em: https://lawfilesext.leg.wa.gov/biennium/2017-18/Pdf/Bills/Session%20Laws/House/1493-S.sl.pdf. Acesso em: 28 abr. 2023.

WORKING PARTY. Article 29. **Parecer 02/2012 sobre reconhecimento facial em serviços online e móveis.** (WP 192). Bruxelas, 2012. Disponível em: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp192_en.pdf. Acesso em: 19 abr. 2023.

WORKING PARTY. Article 29. **Orientações relativas à Avaliação de Impacto sobre a Proteção de Dados (AIPD) e que determinam se o tratamento é «suscetível de resultar num elevado risco» para efeitos do Regulamento (UE) 2016/679** (WP 248 rev.01). Bruxelas, 2017. Disponível em: https://ec.europa.eu/newsroom/article29/items/611236/en. Acesso em: 24 abr. 2023.

WORKING PARTY. Article 29. **Orientações relativas à transparência na aceção do Regulamento 2016/679** (WP 260 rev.01). Bruxelas, 2017. Disponível em: https://ec.europa.eu/newsroom/article29/items/622227/en. Acesso em: 24 abr. 2023.

WORKING PARTY. Article 29. **Orientações sobre as decisões individuais automatizadas e a definição de perfis para efeitos do Regulamento (UE) 2016/679** (WP 251 rev.01). Bruxelas, 2017. Disponível em: https://ec.europa.eu/newsroom/article29/items/612053. Acesso em: 19 abr. 2023.