

ANÁLISE FACIAL E PROTEÇÃO DE DADOS PESSOAIS

Facial analysis and personal data protection

Murilo Arakaki¹

SUMÁRIO

1. Introdução; 2. Direito de Imagem; 3. Biometria Facial; 4. Análise Facial; 5. Identificação Facial; 6. Discriminação Algorítmica; 7. Neurodireitos; 8. Conclusão; Referências Bibliográficas.

RESUMO

O presente artigo tem como objetivo explorar a atuação dos sistemas de análise facial para classificar indivíduos em categorias de gênero, faixa etária e humor, bem como sua implicação no campo de incidência da norma de proteção de dados pessoais. Ademais, apresenta-se a distinção em relação aos sistemas de reconhecimento facial, cujo propósito principal é a identificação ou a autenticação do indivíduo, e discute-se em que medida essa diferença pode ser relevante para a aplicação da norma jurídica. Por fim, abordam-se outras possíveis implicações acerca da utilização daqueles sistemas: a discriminação algorítmica e os neurodireitos.

Palavras-chave: Dados Pessoais. Dados Pessoais Sensíveis. Análise Facial. Categorização. Reconhecimento Facial. Identificação.

ABSTRACT

This article aims to verify the proceeding of facial analysis systems to classify individuals into categories such as gender, age group and mood, and its implication in the incidence of the personal data protection regulation. Furthermore, it presents the distinction with facial recognition systems, whose main purpose is the identification or authentication of the individual, and discusses the extent to which this difference may be relevant for the application of the legal norm. Finally, it adresses other possible implications of those systems: algorithmic discrimination and neurorights.

Keywords: Personal Data. Sensitive Personal Data. Facial Anaysis. Categorization. Facial Recognition. Identification.

1. INTRODUÇÃO

O desenvolvimento e a difusão de tecnologias digitais, como a inteligência artificial (IA), o *Big Data*, a internet das coisas (IoT), a computação em nuvem (*cloud computing*), a realidade aumentada (RA) e outras, têm transformado a vida das pessoas. Se por um lado, isso ocorre de forma veloz e impactante, sem paralelo comparável na história, por outro, dá-se de modo imperceptível ou naturalizado, no qual dados pessoais são fornecidos, coletados, observados, inferidos e tratados sem que os titulares se sintam necessariamente expostos, manipulados, prejudicados ou

¹ Assessor no Gabinete da Presidência da ARTESP Advogado, Especialista em Direito Público Municipal pela ESGCP do TCMSP, Especialista em Direito Digital e Inovação Tecnológica pela ESPGE/SP Engenheiro Eletrônico pela Unicamp. MBA em Tecnologia da Informação pela FIPECAFI.

abusados. Desse modo, as pessoas passam a existir no mundo real e no mundo digital, por vezes mais neste do que naquele, em termos de implicações e consequências.

A esse respeito, Teffé² explica que o ser humano tende a ter um prolongamento e uma projeção de si no ambiente digital em razão do fenômeno da datificação:

Vive-se intensamente, nos últimos tempos, o fenômeno da *datificação*: ato de datificar (pôr em dados) a vida e as relações de uma pessoa. As informações são formatadas de maneira que possam ser registradas, monitoradas e analisadas, permitindo a extração de mais informações e a análise preditiva dos sujeitos, o que facilita, sobremaneira, inferências de caráter sensível sobre eles.

Também externando preocupação similar, Rodotà³, em defesa da dignidade humana e redimensionamento de princípios fundamentais consolidados, criou a teoria do corpo eletrônico para proteger o ser humano da exploração abusiva de seus dados pessoais:

A dignidade é explicitamente referida no início do Código de proteção de dados pessoais (Decreto Legislativo 196/2003, art. 2º)⁴. O “corpo eletrônico”, o conjunto de informações que constroem a nossa identidade, é assim remetido ao corpo físico: a dignidade torna-se o liame forte para reconstruir a integridade da pessoa (Carta dos Direitos Fundamentais da União Europeia, art. 3º), para evitar que a pessoa seja considerada uma espécie de “mina a céu aberto” onde qualquer pessoa possa alcançar qualquer informação e, assim, criar perfis individuais, familiares e grupais, tornando a pessoa objeto de poderes externos, que podem falsificá-la, construí-la em formas consistentes com as necessidades de uma sociedade de vigilância, de seleção social, de cálculo econômico. A Carta dos Direitos Fundamentais da União Europeia reafirmou a proibição de fazer do corpo um objeto lucrativo. Previsto para o corpo físico, esse princípio pode ser estendido ao corpo eletrônico, como já fazem algumas normas, como as que preveem a autorização pública para tratar os chamados dados sensíveis, que dizem respeito aos aspectos mais íntimos da vida ou à posição social da pessoa. Aqui, o princípio da dignidade é combinado com o da igualdade, para evitar discriminações ou estigmatizações sociais.

² TEFFÉ, Chiara Spadaccini de. **Dados pessoais sensíveis**: qualificação, tratamento e boas práticas. Indaiatuba: Editora Foco, 2022, p. 68.

³ RODOTÀ, Stefano. A antropologia do homo dignus. Tradução de Maria Celina Bodin de Moraes. **Civilistica.com**, Rio de Janeiro, v. 6, n. 2, 2017. Disponível em: <https://www.jur.puc-rio.br/wp-content/uploads/2021/08/STEFANO-RODOTA-A-antropologia-do-homo-dignus.pdf>. Acesso em: 27 mar. 2026. p. 15.

⁴ BRASIL. Decreto Legislativo nº 196, de 2003. Aprova o texto da Convenção sobre o Cibercrime, celebrada em Budapeste, em 23 de novembro de 2001. **Diário Oficial da União**, Brasília, DF, 2003.

Nesse sentido, o aprimoramento das tecnologias de processamento digital de imagens faciais e a sua proliferação, viabilizada pelo crescente aumento da capacidade computacional e de armazenamento de dados, aliados ao barateamento e à disponibilidade, em escala global, de dispositivos de captura cada vez mais precisos e sensíveis, têm despertado grandes interesses, não apenas comerciais, mas também no campo do direito. Assim, discute-se a distinção entre sistemas de reconhecimento facial e de análise facial, bem como a eventual relevância jurídica dessa diferença.

Posto desse modo, o objetivo deste trabalho é avaliar em que medida essa distinção é relevante para o direito e em que extensão eventualmente afeta a aplicação da norma protetiva de dados pessoais. Ainda que se possa admitir que os sistemas de análise facial e de reconhecimento de emoções faciais não operam no campo da identificação ou da autenticação de indivíduos, pois tratam com dados impessoais ou anônimos, também se tem como objetivo explorar outras implicações jurídicas decorrentes desse tratamento, como eventuais condutas discriminatórias advindas de decisões automatizadas produzidas por esses sistemas, bem como o eventual alcance a outros campos do direito, como os neurodireitos.

2. DIREITO DE IMAGEM

A imagem facial humana é o principal objeto de tratamento dos sistemas de reconhecimento facial e de análise facial. Como será visto mais adiante, a distinção mais relevante entre esses sistemas consiste mais no propósito do tratamento ou no resultado do processamento dos dados faciais do que nas técnicas computacionais empregadas: ambos os sistemas partem da captura e da detecção da imagem facial para fins de identificação, autenticação ou avaliação do indivíduo. Assim sendo, importa inicialmente contextualizar a relevância jurídica da imagem facial humana, uma vez que se pretende confrontar a análise facial com a proteção de dados pessoais.

Basicamente, há dois aspectos aos quais a imagem humana pode ser associada: (i) à imagem como fotografia, ou ao registro das características físicas do indivíduo que o distinguem das demais pessoas; e (ii) à imagem como projeção social do indivíduo que o representa na sociedade. Assim, Diniz⁵ diferencia imagem-retrato e imagem-atributo da seguinte forma:

A imagem-retrato é a representação física da pessoa, como um todo ou em partes separadas do corpo (nariz, olhos, sorriso etc.) desde que identificáveis, implicando o reconhecimento de seu titular, por meio de fotografia, escultura, desenho, pintura, interpretação dramática, cinematografia, televisão, sites etc., que requer autorização do retratado (CF, art. 5º, X).

⁵ DINIZ, Maria H. **Curso de Direito Civil Brasileiro**: teoria geral do direito civil. São Paulo, SP: Saraiva, 2023, p. 53.

A imagem-atributo é o conjunto de caracteres ou qualidades cultivados pela pessoa, reconhecidos socialmente (CF, art. 5º, V), como habilidade, competência, lealdade, pontualidade etc. A imagem abrange também a reprodução, romaneada em livro, filme, ou novela, da vida de pessoa de notoriedade.

Assim sendo, o direito de imagem, insculpido no artigo 20 do Código Civil Brasileiro (CC)⁶, abarca adequadamente esses dois aspectos, impedindo a exposição ou a utilização comercial indevida da imagem-retrato do indivíduo, bem como a alteração não autorizada de sua imagem-atributo, que atinja sua reputação perante a sociedade:

Art. 20. Salvo se autorizadas, ou se necessárias à administração da justiça ou à manutenção da ordem pública, a divulgação de escritos, a transmissão da palavra, ou a publicação, a exposição ou a utilização da imagem de uma pessoa poderão ser proibidas, a seu requerimento e sem prejuízo da indenização que couber, se lhe atingirem a honra, a boa fama ou a respeitabilidade, ou se se destinarem a fins comerciais.

Vale observar que, apesar de os direitos à intimidade, à vida privada e à honra estarem usualmente relacionados ao direito à imagem, tratam-se de direitos autônomos, em que um não depende necessariamente do outro para o seu exercício e tutela. Assim, por exemplo, ainda que a divulgação indevida da imagem de alguém não viole sua intimidade, vida privada ou honra, subsiste o dever de reparação pela ausência de autorização, conforme entendimento sumulado do Superior Tribunal de Justiça (STJ): “Independente de prova do prejuízo a indenização pela publicação não autorizada de imagem de pessoa com fins econômicos ou comerciais”⁷.

Embora a autonomia desses institutos pareça inquestionável, até mesmo pelo texto constitucional do artigo 5º, X, colacionado a seguir, que os trata de modo destacado e independente, indaga-se acerca do objeto da autorização: a exposição ou a utilização da imagem, ou a mera captação desta.

Art. 5º [...]

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;⁸

⁶ BRASIL. **Lei nº 10.406, de 10 de janeiro de 2002**. Institui o Código Civil. Brasília, DF: Presidência da República, 2002. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/2002/110406compilada.htm. Acesso em: 27 mar. 2026.

⁷ BRASIL. Superior Tribunal de Justiça. **Súmula nº 403**. DJe 24 nov. 2009. Disponível em: https://www.stj.jus.br/docs_internet/revista/eletronica/stj-revista-sumulas-2014_38_capSumula403.pdf. Acesso em: 27 mar. 2026.

⁸ BRASIL. **Constituição da República Federativa do Brasil de 1988**. Brasília, DF: Presidência da República, 1988. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao_compilado.htm. Acesso em: 27 mar. 2026.

Nesse sentido, a inteligência do artigo 20, do CC, parece fundar-se na percepção utilitarista da imagem pessoal: a mera captação, sem o efetivo emprego ou a divulgação da imagem, não teria utilidade prática e, portanto, não haveria ofensa ao direito de imagem, uma vez que não há exposição da imagem-retrato e, tampouco, alteração da imagem-atributo, dispensando, assim, a autorização do indivíduo. Por outro lado, justamente por conta dessa aparente indissociabilidade de captação e de divulgação, Affonso⁹ entende que:

A ratio da codificação vigente é de que a mera captação já dependeria do consentimento do seu titular, porque haveria “uma *presumptio hominis* de que a fixação fotográfica da imagem destina-se à posterior reprodução. Por isso, deve ser deferido ao titular o direito de autorizar, e negar, a captação de sua imagem. A divulgação ou reprodução constitui extensão de uma lesão já ocorrida”. Assim, no atual estado da arte da doutrina, entende-se que o direito à imagem precede à sua divulgação, sendo protegida já a mera captação da imagem.

Entretanto, sistemas de análise facial ou de reconhecimento de emoções faciais procuram associar atributos faciais mensuráveis de imagens humanas capturadas a categorias como gênero, faixa etária e humor, em tese, sem qualquer propósito de divulgação ou exposição das imagens, até porque somente os dados dos atributos faciais são armazenados e processados. Dessa forma, parece que a lógica do artigo 20, c.c, poderia ser rompida nesse caso, tornando facultativo o prévio consentimento para a captura da imagem facial, desde que não ocorra a exposição ou a difusão desta. Esse aspecto utilitarista, que consistente na divulgação da imagem capturada, parece ser relevante para o exercício do direito de imagem, ainda que essa exposição se concretize por qualquer meio, seria imprescindível a sua ocorrência para caracterização de violação:

O direito à imagem consiste na prerrogativa que o sujeito tem de autorizar ou não a exposição, reprodução ou divulgação de sua imagem, que não se limita aos aspectos físicos, mas abrange a concretização da representação física, moral e psíquica do titular, a exteriorização da personalidade. Além de não se restringir à representação fotográfica, o direito à imagem engloba toda e qualquer representação plástica, gráfica ou fotográfica de uma pessoa ou de um objeto, ou, ainda, por qualquer outro meio de caracterização de seus atributos. Explica Adriano de Cupis que a imagem dos indivíduos é resguardada independente da forma ou meio como é representada, sendo indiferente a forma como é representada, sendo “certo é que o direito à

⁹ AFFONSO, Filipe José Medon. O direito à imagem na era das deep fakes. **Revista Brasileira de Direito Civil**, Rio de Janeiro, v. 27, n. 1, p. 251-277, 2021. Disponível em: <https://rbdcivil.ibdrcivil.org.br/rbdc/article/view/438>. Acesso em: 27 mar. 2026.

imagem assegura ao indivíduo a defesa contra este, como contra os outros modos de difusão de sua imagem”¹⁰.

Nessa ordem de pensamento, outra indagação aparentemente relevante se refere à necessidade de determinação do titular da imagem facial para que o direito de imagem possa ser exercido. Se o indivíduo for indeterminado, assim considerado uma pessoa desconhecida, e, simultaneamente, indeterminável, assim considerado aquela cujos dados disponíveis a seu respeito sejam insuficientes para reconhecê-la, parece não fazer sentido falar em direito de imagem, uma vez que não se identifica o seu titular e, portanto, torna-se impraticável a tutela de seus direitos.

Novamente, os sistemas de análise facial ou de reconhecimento de emoções faciais atuam no processamento de dados representativos de atributos faciais, como a forma e o posicionamento de sobrancelhas, olhos, narinas, lábios, formato do rosto e orelhas para estimar gênero, faixa etária e humor da imagem facial. Assim, além de a identificação do indivíduo não ser o propósito desses sistemas, os atributos faciais coletados, em regra, não são suficientes para identificá-lo. Conforme ressalva Loureiro¹¹, a relevância jurídica da imagem humana passa pela possibilidade de identificação do indivíduo:

Mas foi Walter Moraes quem nos apresentou uma definição verdadeiramente ampla de imagem, que vai além do caráter visual: “Toda expressão formal e sensível da personalidade de um homem é imagem para o Direito”. A imagem constitui um sinal sensível da personalidade: revela para o mundo exterior o ser imaterial da personalidade interior, delinea-a, dá-lhe forma. A ideia de imagem, para o direito, pressupõe figura humana. Não se refere somente à sua reprodução visual, mas também à imagem sonora da fonografia e da radiodifusão, às partes de corpo (boca, nariz, olhos etc., **desde que suficientes à identificação do indivíduo**), aos gestos e expressões dinâmicas da personalidade.

Por fim, ainda se indaga a respeito da autorização implícita do indivíduo que frequenta determinados ambientes para a captura de sua imagem e o consequente processamento de atributos faciais com a finalidade de classificação de gênero, faixa etária e humor, de forma a melhorar a assertividade no provimento de serviços individuais e coletivos. Se o indivíduo for adequadamente informado sobre as circunstâncias e as condições de captura e processamento de dados faciais, e

¹⁰ SIQUEIRA, Dirceu Pereira; VIEIRA, Ana Elisa Silva Fernandes. Os limites à reconstrução digital da imagem na sociedade tecnológica. **Revista Eletrônica do Curso de Direito da UFSM**, Santa Maria, v. 17, n. 3, e67299, 2022, p. 4. Disponível em: <https://periodicos.ufsm.br/revistadireito/article/view/67299>. Acesso em: 27 mar. 2026.

¹¹ LOUREIRO, Henrique Vergueiro. **Direito à imagem**. 2005. Dissertação (Mestrado em Direito) – Pontifícia Universidade Católica de São Paulo, São Paulo, 2005, p. 58. Disponível em: <https://repositorio.pucsp.br/jspui/handle/handle/5983>. Acesso em: 27 mar. 2026. grifo nosso.

demonstrar aceitá-las por permanecer e frequentar o ambiente monitorado, poderia se concluir pela autorização tácita, uma vez que o indivíduo não evidenciaria expectativa diversa. Nesse ponto, Affonso observa que, em determinadas situações, não se trata de consentimento tácito, mas de limitação ao direito de imagem em benefício do interesse público:

Fala-se, ainda, numa noção de consentimento tácito, que, no caso das fotografias, pode ser “tão usual quanto a celebração de termos por escrito, uma vez que a simples pose para foto já pode consistir em concordância para a sua captura”. Antonio Chaves, por exemplo, apontava como hipótese de consentimento presumido o caso de uma pessoa que comparece em público em companhia de uma pessoa famosa, passando, então, a sofrer uma limitação do seu direito à imagem decorrente de sua notoriedade. No mesmo sentido, Adriano de Cupis, para quem, àquele que “participa em um acontecimento ou em uma cerimônia de interesse público ou ocorrida em público, pode mesmo atribuir-se o consentimento tácito da reprodução da sua imagem, em várias cópias enquadradas nos ditos acontecimentos ou cerimônias. Objeta-se, contudo, que nessas situações não haveria consentimento tácito propriamente dito, mas, sim, uma série de limites impostos ao direito à imagem da pessoa pelo interesse público, o que tornaria desnecessária a autorização do titular. Tais limites se diferenciariam da autorização tácita, pois se se estivesse “tratando de autorização, ainda que implícita, haveria o poder de oposição do titular à publicação”¹².

Assim, de forma similar, se a análise facial ou o reconhecimento de emoções faciais, cujo propósito não é a identificação de indivíduos, mas a sua classificação em gênero, faixa etária e humor, for benéfica à coletividade, por exemplo mediante melhorias no provimento de serviços, parece razoável que o direito individualizado de imagem possa ser proporcionalmente atenuado ou limitado, de forma que o direito de um não prejudique em demasia o direito de muitos.

3. BIOMETRIA FACIAL

A imagem facial humana dispõe de inúmeros atributos biométricos que podem ser capturados e processados para diversas finalidades, como a identificação ou a autenticação do indivíduo por meio de sistemas de reconhecimento facial, bem como a avaliação ou a categorização do indivíduo utilizando-se sistemas de análise facial ou de reconhecimento de emoções faciais. No primeiro exemplo, dados biométricos do indivíduo são coletados e tratados com o objetivo de confirmar a sua identidade; portanto, trata-se de um conjunto de dados biométricos personalizados, individualizados e únicos, capaz de distinguir inequivocamente um indivíduo de

¹² AFFONSO, *op. cit.*, p. 255-256.

outro. Por outro lado, no segundo, o tratamento de dados biométricos do indivíduo se presta para classificá-lo em categorias como gênero, faixa etária e humor, mas não para identificá-lo.

Em que pese a diferenciação de propósitos, os sistemas de identificação ou autenticação facial e de análise ou reconhecimento de emoções faciais utilizam dados biométricos de indivíduos para atingir seus objetivos. Assim sendo, importa compreender a relevância jurídica dessa distinção, especialmente porque a Lei Geral de Proteção de Dados (LGPD) considera os dados biométricos como dados pessoais sensíveis, cujos requisitos ou bases legais autorizativas de tratamento são mais rígidos em relação àqueles dispensados para o tratamento de dados pessoais comuns ou não sensíveis:

Art. 5º Para os fins desta Lei, considera-se:

[...]

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 natural¹³;

Contudo, embora a LGPD aponte o dado biométrico como exemplo de dado pessoal sensível, a Lei não o define ou conceitua, deixando, aparentemente como técnica legislativa, a cargo da legislação, da doutrina e da jurisprudência essa tarefa, amoldando-se à casuística das demandas sociais. Nesse contexto, a Autoridade Nacional de Proteção de Dados (ANPD) tem canalizado esforços para debater, fiscalizar e regulamentar o tratamento de dados biométricos, como o estudo “Biometria de reconhecimento facial”, no Radar Tecnológico de 2024¹⁴; a inclusão do tratamento de dados biométricos na Agenda Regulatória da autarquia para o biênio 2025-2026¹⁵; a fiscalização do uso de sistemas de reconhecimento facial na venda

¹³ BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República, 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709compilado.htm. Acesso em: 27 mar. 2026. Grifo nosso.

¹⁴ AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD). **Radar Tecnológico nº 2 – Biometria e Reconhecimento Facial**. Brasília, DF: ANPD, 2024b. Disponível em: <https://www.gov.br/anpd/pt-br/centrais-de-conteudo/documentos-tecnicos-orientativos/>. Acesso em: 27 mar. 2026.

¹⁵ AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD). **Agenda Regulatória para o Biênio 2025-2026**. Brasília, DF: ANPD, 2024a. Disponível em: https://www.gov.br/anpd/pt-br/assuntos/processo_regulatorio/agenda-regulatoria-1. Acesso em: 27 mar. 2026.

de ingressos e na entrada de estádios de futebol¹⁶; e a tomada de subsídios sobre tratamento de dados biométricos¹⁷.

Tratam-se de iniciativas recentes nessa seara, em que a produção legislativa e jurisprudencial parece ainda incipiente. Entretanto, o conceito de dado biométrico deve considerar aspectos humanos para além da fisiologia. Nesse sentido, embora menos recente, o Decreto Federal nº 10.046/2019¹⁸, que dispõe sobre a governança no compartilhamento de dados, assim regulamenta:

Art. 2º Para fins deste Decreto, considera-se:

[...]

II - atributos biométricos - características biológicas e comportamentais mensuráveis da pessoa natural que podem ser coletadas para reconhecimento automatizado, tais como a palma da mão, as digitais dos dedos, a retina ou a íris dos olhos, o formato da face, a voz e a maneira de andar.

A partir dessa definição, percebe-se que os atributos ou dados biométricos não se restringem a características biológicas, mas abrangem também características comportamentais do indivíduo, desde que passíveis de mensuração. Dessa forma, no caso de dados faciais, o posicionamento e o formato dos olhos, do nariz, da boca, das orelhas e do rosto, bem como a forma de expressar emoções por meio da movimentação ou da articulação daqueles elementos faciais, são considerados dados biométricos por se tratarem de características mensuráveis da face de uma pessoa natural. Apesar desse esclarecimento, a norma não especifica o propósito da coleta de atributos biométricos, referindo-se apenas ao reconhecimento automatizado, o qual parece condizente com o objetivo primordial de identificação do indivíduo. Com efeito, segundo entendimento de Teffé¹⁹, tanto os atributos fisiológicos quanto os comportamentais mensurados teriam como objetivo o estabelecimento da identidade de alguém:

A biometria é a ciência de se estabelecer a identidade de alguém, a partir da medição e análise de seus atributos fisiológicos ou comportamentais

¹⁶ AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD). **ANPD fiscaliza uso de sistema de reconhecimento facial na venda de ingressos e na entrada de estádios por 23 clubes de futebol**. Brasília, DF: ANPD, 2025b. Disponível em: <https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-fiscaliza-uso-de-sistema-de-reconhecimento-facial-na-venda-de-ingressos-e-na-entrada-de-estadios-por-23-clubes-de-futebol>. Acesso em: 27 mar 2026.

¹⁷ AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD). **ANPD abre Tomada de Subsídios sobre Tratamento de Dados Biométricos**. Brasília, DF: ANPD, 2025a. Disponível em: <https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-abre-tomada-de-subsidios-sobre-tratamento-de-dados-biometricos>. Acesso em: 27 mar. 2026.

¹⁸ BRASIL. **Decreto nº 10.046, de 9 de outubro de 2019**. Dispõe sobre a governança no compartilhamento de dados no âmbito. Brasília, DF: Presidência da República, 2019. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/decreto/D10046.htm. Acesso em: 27 mar. 2026.

¹⁹ TEFFÉ, *op. cit.*, p. 149.

mensuráveis. No primeiro caso, são exemplos a impressão digital, o reconhecimento da íris, a identificação por retina, a definição dos traços do rosto, a arcada dentária, a geometria da mão e a altura da pessoa. As medidas fisiológicas geralmente oferecem o benefício de permanecer mais estáveis ao longo da vida de um indivíduo. No segundo caso, é possível mencionar: a forma como a pessoa digita, como anda, gestos característicos, dinâmica da assinatura (velocidade do movimento da caneta, acelerações, pressão exercida e inclinação), a altura que o indivíduo costuma segurar o celular, a forma com que ele movimenta o mouse do computador, a pressão que ele exerce no teclado ou na tela e, até mesmo, como corrige as palavras. Com o aprendizado de máquina e a inteligência artificial, é possível entender e analisar como uma pessoa se comporta no computador ou no celular, por exemplo.

Nessa linha de raciocínio, considerando que o propósito dos sistemas de análise facial ou de reconhecimento de emoções faciais é a classificação de indivíduos em categorias como gênero, faixa etária e humor, mas não a sua identificação, as informações coletadas das faces não seriam consideradas dados biométricos, pelo menos na acepção empregada no âmbito da legislação de proteção de dados pessoais. Esse entendimento reforça a ideia de que o significado do termo “biometria” ou “dado biométrico”, a partir apenas de sua etimologia, não seria um caminho seguro e suficiente para compreender o sentido e o alcance da norma jurídica.

Nesse contexto, poderia se dividir ou classificar os dados biométricos de acordo com uma escala de força ou capacidade de identificar o indivíduo, na qual identificadores fortes possibilitariam a identificação unívoca de uma pessoa natural. Por outro lado, indicadores mais fracos não teriam essa habilidade, por não tratar pessoas de forma individualizada ou única, mas sim agrupadas em categorias que apresentam características biométricas comuns como gênero, faixa etária e humor, conforme apontam Wendehorst e Duller²⁰ em um estudo realizado acerca do reconhecimento biométrico e da detecção comportamental:

Biometrics may be divided in various ways, one of them being ‘strong’, ‘weak’, and ‘soft’ identifiers. Strong identifiers allow or confirm the unique identification of a natural person, e.g. fingerprints, iris, and retina. Weak biometrics are features that are ‘less unique’ or ‘less stable’, e.g. body shape, behavioural patterns, voice, and body sounds. Soft biometrics comprise features that are generic in nature and not uniquely associated with a person, e.g. gender or age.

²⁰ WENDEHORST, Christiane; DULLER, Yannic. **Biometric Recognition and behavioural detection**. Policy Department for Citizens' Rights and Constitutional Affairs, PE 696.968 , Aug. 2021, p. 13. Disponível em: [https://www.europarl.europa.eu/RegData/etudes/STUD/2021/696968/IPOL_STU\(2021\)696968_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2021/696968/IPOL_STU(2021)696968_EN.pdf). Acesso em: 27 mar. 2026.

Considerando essa classificação de dados biométricos, os sistemas de análise facial ou de reconhecimento de emoções faciais podem ser entendidos como técnicas de categorização, uma vez que os identificadores biométricos empregados por eles são adequados apenas para designar pessoas em categorias específicas, e não para identificá-las individualmente. Entretanto, vale ressaltar que, se uma pessoa for designada em diferentes categorias de forma cumulativa e, dependendo das circunstâncias, como o número e a granularidade de categorias, a identidade do indivíduo poderá ser obtida ou confirmada:

Biometric techniques can, in the light of their primary function, be divided into techniques of biometric authentication or identification, categorisation, and detection. [...] Biometric categorisation is a term that is less common than biometric identification, also because the rise of biometric categorisation techniques has only come with the increasing use of 'soft' or 'weak' biometrics. Data that are as such not (or not necessarily) suited for the unique identification of a natural person may nevertheless be suited for assigning natural persons to specific categories, such as sex, age, ethnic origin or health. Needless to say, where a particular natural person is assigned to several different categories, the cumulative assignment may, depending on circumstances such as number and granularity of categories, allow or confirm the identification of that natural person²¹.

Ainda que pareça inicialmente contraintuitivo, o processamento de dados biométricos faciais e a sua finalidade, seja a identificação ou a categorização, são aspectos relevantes ao enquadramento desses dados como pessoais ou sensíveis, ao menos para fins de aplicação da norma jurídica. Ao observar a imagem facial de um indivíduo, qualquer pessoa de juízo mediano seria capaz de identificá-lo, se for conhecido, e de determinar, com razoável acurácia, seu gênero, faixa etária e humor: a imagem facial carrega todas essas informações biométricas e, portanto, a sua simples captura já parece constituir a em dado pessoal comum e sensível. Contudo, deve-se considerar que o cérebro humano, instantaneamente, observa, captura, processa e reage diante da imagem facial de forma indissociável, o que se mostra inviável para sistemas computacionais. Nesse sentido, ensina Teffé²² que:

De acordo com o Information Commissioner's Office (ICO), se você processar fotografias digitais de pessoas, esses dados não serão automaticamente biométricos, mesmo que sejam usados para fins de identificação. Embora uma imagem digital possa permitir a identificação por meio de características físicas, ela só se tornará um dado biométrico se você realizar um "processamento técnico específico". Normalmente, isso envolve

²¹ *Ibid.*, p. 20-21.

²² TEFFÉ, *op. cit.*, p. 150.

o uso dos dados da imagem para criar um modelo digital individual ou perfil, que, por sua vez, você usará para correspondência automática de imagens e identificação.

Na mesma direção, o Considerando 51 do Regulamento Geral sobre a Proteção de Dados (General Data Protection Regulation – GDPR) também observa que o processamento, por meios técnicos específicos que permitam a identificação ou autenticação do indivíduo, é requisito para o enquadramento do tratamento de categorias especiais de dados pessoais²³:

Considerando 51 do GDPR. [...] O tratamento de fotografias não deverá ser considerado sistematicamente um tratamento de categorias especiais de dados pessoais, uma vez que são apenas abrangidas pela definição de dados biométricos quando forem processadas por meios técnicos específicos que permitam a identificação inequívoca ou a autenticação de uma pessoa singular.

A propósito, se os dados faciais capturados para fins de análise facial ou de reconhecimento de emoções faciais forem ineficazes para a identificação do indivíduo, sequer seriam considerados dados pessoais, na medida em que, embora se refiram à pessoa natural, não se trata de um indivíduo determinado ou determinável. Assim, a possibilidade de identificação pessoal é o requisito essencial e, em regra, imprescindível, não somente para a determinação de dados biométricos, mas também para a assunção do dado como pessoal.

Com efeito, o Article 29 Data Protection Working Party da Comissão Europeia²⁴ emitiu o Opinativo nº 02/2012 a respeito do reconhecimento facial e do dado pessoal, para esclarecer que um conjunto de atributos distintivos usado somente em um sistema de categorização não conteria, em regra, informação suficiente para identificar um indivíduo, mas apenas para realizar a categorização, por exemplo, masculino ou feminino, e, nesse caso, não seria considerado dado pessoal:

4.1. Digital images as personal data. When a digital image contains an individual's face which is clearly visible and allows for that individual to be identified it would be considered personal data. A template or set of distinctive features used only in a categorisation system would not, in general, contain sufficient information to identify an individual. It should only

²³ 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*, 4 maio 2016. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32016R0679>. Acesso em: 27 mar. 2026.

²⁴ EUROPEAN COMMISSION. ARTICLE 29 DATA PROTECTION WORKING PARTY. **Opinion 2/2012 on the concept of personal data**. Bruxelas, 2012. Disponível em: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/index_en.htm. Acesso em: 27 mar. 2026.

contain sufficient information to perform the categorisation (e.g. male or female). In this case it would not be personal data provided the template (or the result) is not associated with an individual's record, profile or the original image (which will still be considered personal data).

Apesar disso, assim como o propósito da aplicação distingue os sistemas de identificação ou autenticação facial dos sistemas de análise ou reconhecimento de emoções faciais, a repercussão pessoal do tratamento de dados relativos à pessoa natural, ainda que indeterminada ou indeterminável, pode ser um critério distintivo entre dado pessoal e dado não pessoal ou anônimo. Em outros termos, o dado poderá ser considerado pessoal, mesmo que não se relacione com uma pessoa natural identificada ou identificável, desde que o seu tratamento possa interferir no âmbito pessoal de alguém, embora desconhecido, como se verá mais adiante.

Por fim, no âmbito do enquadramento dos dados faciais biométricos, vale indagar acerca da relação entre o dado pessoal e o dado pessoal sensível. A partir da primeira interpretação dos incisos I e II do artigo 5º da LGPD, parece tratar-se de relação de qualificação, em que o dado pessoal sensível é espécie do gênero dado pessoal²⁵:

Art. 5º Para os fins desta Lei, considera-se:

I - **dado pessoal**: informação relacionada a pessoa natural identificada ou identificável;

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;

Em defesa por uma tutela ampliada das informações pessoais, Teffé²⁶ também parece entender que os dados pessoais sensíveis são espécies de dados pessoais:

A LGPD em seu Art. 5º, inciso II, trouxe **espécies** de dados pessoais considerados sensíveis: “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”. Todavia, não esclareceu o que seriam dados sensíveis em termos conceituais, não definiu suas **espécies** nem se posicionou quanto à qualidade de seu rol: se taxativo ou exemplificativo.

²⁵ BRASIL, **Lei nº 13.709, de 14 de agosto de 2018**, *op. cit.*, grifo nosso.

²⁶ TEFFÉ, *op. cit.*, p. 22, grifo nosso.

Inicialmente, essa colocação parece fazer sentido, porque há de se reconhecer a existência de uma classe especial de dados pessoais, cujo tratamento potencializa condutas ilícitas ou discriminatórias. Entretanto, Teffé²⁷ observa que a distinção entre dado pessoal geral e dado sensível “torna-se cada vez mais fluída, pois aparentemente qualquer dado pode se tornar sensível, se for encontrada uma maneira de, a partir dele, serem inferidas informações sobre atributos assim protegidos”. Dessa forma, pode-se concluir que não é necessariamente a natureza do dado pessoal, comum ou sensível, que conduz ao comportamento ou à decisão automatizada ilícita ou discriminatória, mas o tratamento desse dado pessoal. A esse respeito, Teffé²⁸ alerta sobre o tratamento sensível de dados pessoais comuns:

Entende-se que, além de se realizar uma proteção mais ampla dos dados sensíveis, tal proteção também deverá ser observada nos casos em que houver tratamento sensível de dados pessoais. Isso porque, com base estritamente em considerações a respeito da natureza dos dados tratados, nem sempre será possível prever os efeitos que o tratamento poderá causar em seu titular ou em interesses coletivos lato sensu. Inferências e conclusões geradoras de informações sensíveis bem como tratamentos sensíveis de informações que apresentem claro viés discriminatório ilícito ou abusivo deverão, por consequência, receber proteções ampliadas. Recomenda-se, então, que sejam verificadas, entre outras questões apontadas neste livro, as intenções do controlador e se, a partir do tratamento realizado, era previsível que os dados poderiam revelar informações sensíveis.

Essa lógica também poderia ser aplicada ao tratamento de dados não pessoais ou anônimos. Considerando que os dados biométricos faciais capturados por sistemas de análise facial ou de reconhecimento de emoções faciais são insuficientes para a identificação dos titulares, tratam-se, então, de dados não pessoais ou anônimos. Contudo, ainda assim, o tratamento pode ser potencialmente sensível, na medida em que decisões automatizadas decorrentes desse tratamento podem se revelar ilícitas por viés ou discriminação algorítmica.

4. ANÁLISE FACIAL

A análise facial, no contexto do processamento automatizado de características da face humana, pode ser conceituada como a categorização de atributos faciais mensuráveis em classes previamente determinadas, as quais expressam condições ou circunstâncias humanas, como faixa etária, gênero e humor. Embora o fluxo de

²⁷ *Ibid.*, p. 67.

²⁸ *Ibid.*, p. 62-63.

processamento de dados da análise facial seja razoavelmente similar ao do reconhecimento facial, as duas tecnologias não devem ser consideradas idênticas ou intercambiáveis, seja porque têm propósitos distintos, seja porque têm repercussões jurídicas próprias, a depender das aplicações em casos concretos.

De acordo com estudos de Li e Jain²⁹, geralmente, “um sistema de reconhecimento facial consiste em quatro módulos: detecção, alinhamento, extração de atributos e comparação”³⁰. A detecção facial segmenta áreas da face, distinguindo-as da imagem de fundo. O alinhamento facial tem como objetivo a localização mais precisa e a estimativa da escala da face detectada. Os componentes faciais, como olhos, nariz, boca e contorno facial, são localizados com base nesses pontos de localização; em seguida, a imagem da face é então normalizada em relação às propriedades geométricas, como tamanho e posição, e às propriedades fotométricas, como iluminação e escala de cinza. Depois que a face é normalizada, a extração de atributos é executada para se obter informações efetivamente úteis, a fim de distinguir faces de diferentes pessoas. No módulo de comparação, o conjunto de atributos extraídos da face é comparado com os registrados no banco de dados, assim, a identidade da face é indicada pelo sistema quando a comparação atinge um nível razoável de confiança, ou, caso contrário, indica uma face desconhecida.

Usualmente, as aplicações mais difundidas e conhecidas dos sistemas de reconhecimento facial são a verificação ou autenticação facial e a identificação facial. Segundo Zuk³¹, a verificação facial é o processo de determinação de que alguém é quem declara ser. Tal processo é chamado de comparação um-para-um (1:1). Por exemplo, quando um usuário tenta desbloquear seu telefone celular com o seu rosto, o algoritmo compara a face do usuário com a imagem armazenada do proprietário; se a pontuação de similaridade for elevada o suficiente, a identidade do usuário é confirmada e o é celular desbloqueado. Outras aplicações incluem o embarque em voos e a autorização de pagamentos. De fato, não são as imagens das faces efetivamente comparadas, mas os seus atributos.

Por outro lado, a identificação facial compara uma face desconhecida com um banco de dados de imagens. Esse tipo de comparação é chamado de um-para-muitos (1:N). Por exemplo, algoritmos de identificação facial podem checar a face capturada por uma câmera de vigilância com uma base de dados contendo faces de criminosos procurados. Assim, a identificação facial compreende um desafio computacional mais elaborado, pois o algoritmo deve “vasculhar” toda a base de dados em busca da identidade da face a ser reconhecida, com grau de confiança

²⁹ LI, Sant Z.; JAIN, Anil K. **Handbook of face recognition**. New York: Springer, 2005. p. 2-3.

³⁰ Tradução livre do original: “A face recognition system generally consists of four modules [...]: detection, alignment, feature extraction, and matching [...]”.

³¹ ZUK, Ofir. The State of Facial Recognition Today. **Datagen.tech**, 2024. Disponível em: <https://datagen.tech/blog/the-state-of-facial-recognition-today/>. Acesso em: 12 fev. 2024.

aceitável. Mesmo admitindo essa diferença computacional, a verificação ou autenticação facial e a identificação facial atuam com um propósito comum: identificar o titular dos atributos faciais capturados.

Nesse sentido, a análise facial se diferencia do reconhecimento facial de modo estrito, uma vez que não há interesse na identificação do titular dos atributos faciais, mas no significado de suas expressões faciais, conforme explica Bastos e Esteves³²:

Em sentido estrito, as tecnologias de reconhecimento facial tratam o rosto apenas como um index de identidade, desconsiderando sua expressiva capacidade de comunicação e interação social. Estabelecem seu marco de identidade para então ligar o rosto coletado (input) com a sua identidade no mundo real (output). Procuram responder a seguinte problemática: “A qual pessoa pertence esse rosto coletado”? É o que se denomina de reconhecimento facial em sentido estrito, ou seja, o reconhecimento apenas da identidade. Por outro lado, a análise automatizada de expressão facial tenta controlar os diversos significados que uma face individual pode transmitir para identificar sinais afetivos, expressões, emoções, humor, etc. Mesmo com objetivos finais diferentes, os primeiros passos da análise automatizada de expressão facial são os mesmos do reconhecimento facial em sentido estrito: detectar uma face e a extração de características.

Enquanto o reconhecimento facial utiliza dados únicos e específicos de uma pessoa para responder a questões como “quem é você?”, no caso de identificação facial, ou “você realmente é quem diz ser?”, no caso de verificação ou autenticação facial, a análise facial ou o reconhecimento de emoção facial (*facial emotion recognition* – FER) é o processo de mapeamento de expressões faciais com o objetivo de identificar emoções, como aversão, alegria, raiva, surpresa, medo e tristeza, em uma face humana, por meio de *software* de processamento de imagem. Assim, a interpretação das emoções humanas se diferencia do reconhecimento facial, o qual visa identificar uma pessoa, e não uma emoção³³.

Apesar da incapacidade de identificar pessoas, os sistemas de análise facial visam agrupar indivíduos em classes previamente determinadas, de acordo com atributos faciais mensuráveis que expressam condições ou circunstâncias humanas, como faixa etária, gênero e humor. Esse agrupamento de indivíduos, segundo critérios que os unem, como mesma faixa etária, mesmo gênero ou mesmo humor, pode ser considerado a formação de perfil comportamental a que se refere o art. 12, § 2º,

³² BASTOS, Elísio Augusto Velloso; ESTEVES, Vitória Barros. Tecnologias de reconhecimento facial: um estudo a partir do contexto de vigilância digital e sutil. **Revista Direitos Democráticos & Estado Moderno**, São Paulo, n. 3, p. 216-240, jul./dez. 2021. Disponível em: <https://revistas.pucsp.br/index.php/DDEM/article/view/53875/38321>. Acesso em: 27 mar. 2026.

³³ THALES. **Facial recognition: top 7 trends (tech, vendors, use cases)**. 2021. Disponível em: <https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/biometrics/facial-recognition>. Acesso em: 27 mar. 2026.

da LGPD. Assim sendo, se o perfil de determinada classe for a base para a tomada de alguma decisão que possa interferir no âmbito pessoal de alguém, então os atributos faciais coletados serão considerados dados pessoais, mesmo sem necessariamente identificar o titular desses dados.

Trata-se da análise consequencialista trazida por Bioni³⁴, segundo a qual, o conceito de dado pessoal deve ser compreendido não apenas a partir do atributo da identificabilidade, mas também do seu desdobramento na esfera pessoal:

Muitas vezes, processos de decisões automatizados valem-se desses perfis que não necessariamente identificam uma pessoa em específico, mas um grupo – grouping. É pelo fato de ela estar catalogada, inserida, referenciada ou estratificada nesse grupo que uma série de decisões serão tomadas a seu respeito, ainda que sem individualizá-la diretamente a priori. Como já apontado no início deste subcapítulo, essa é uma metodologia bastante comum em muitos modelos de negócios que se valem de dados estatísticos de grupos para o direcionamento de conteúdo e publicidade, ainda que não seja possível identificar as pessoas que compõem aquela massa.

Desse modo, sempre que a análise facial implicar repercussão no âmbito pessoal de alguém, haverá a incidência protetiva da LGPD e, portanto, os atributos faciais assim tratados serão considerados dados pessoais, ainda que não se possa identificar o seu titular individualmente. Por outro lado, em sentido oposto, se nenhum interesse pessoal for afetado com as decisões tomadas a partir da análise facial, então os atributos faciais processados não serão dados pessoais e, consequentemente, estarão fora do alcance da LGPD.

5. IDENTIFICAÇÃO FACIAL

A identificação a partir da imagem facial do titular é um elemento relevante e indispensável no contexto do direito à proteção de dados pessoais. Segundo a LGPD³⁵, dado pessoal é “informação relacionada a pessoa natural identificada ou identificável”; assim, percebe-se que o ordenamento pátrio adota o conceito amplo de identificação do titular do dado pessoal, não se restringindo à pessoa natural identificada, mas alcançando também a pessoa natural passível de identificação por qualquer meio, bastando ser identificável. Nesse sentido, a imagem facial que se relaciona à pessoa natural identificada ou identificável é um dado pessoal, caso contrário, em tese, não.

³⁴ BIONI, Bruno Ricardo. **Proteção de dados pessoais: a função e os limites do consentimento**. São Paulo: Grupo GEN, 2021, p. 77.

³⁵ BRASIL, **Lei nº 13.709, de 14 de agosto de 2018**, *op. cit.*

Pelo menos para fins de incidência da LGPD, um dado não poderá ser considerado pessoal se não puder ser relacionado à pessoa natural ou, mesmo relacionado, se essa pessoa não for identificada nem puder ser identificada por qualquer meio. Assim sendo, um dado não pessoal ou um dado impessoal é a informação que não se refere a uma pessoa natural em particular ou se refere a uma pessoa natural anônima (não identificada nem identificável).

Parece fazer sentido que informações dessa natureza sejam expurgadas do campo de incidência da LGPD, na medida em que o objeto da proteção imposta pela norma jurídica não é o dado em si, mas os direitos de liberdade do seu titular. Afinal, segundo Teffé³⁶:

O oferecimento aos cidadãos de instrumentos que lhes garantam assumir efetivamente controle acerca do uso e da integridade de suas informações representa garantia de tutela da própria dignidade da pessoa humana, tendo em vista o papel predominante da informação para as escolhas do indivíduo.

Assim, se não há um titular específico ou se o titular é anônimo, em tese, não haveria de se falar em ameaça ou lesão aos direitos ou liberdades fundamentais. Por exemplo, o número de inscrição no Cadastro de Pessoas Físicas (CPF) do Ministério da Fazenda pode ser considerado um dado pessoal, uma vez que o seu titular pode ter interesse em que o tratamento dessa informação esteja sob o seu controle e seja realizado de acordo com sua disposição ou autorização, em conformidade com as disposições legais, de forma a proteger seus direitos e liberdades. Por outro lado, se determinado número de CPF for inválido³⁷, ou mesmo válido e ainda não tiver sido atribuído a alguém³⁸, ou ainda se estiver associado a uma pessoa desconhecida, o tratamento isolado desse dado poderá não representar ameaça ou lesão a direitos, seja porque não há um titular (número inválido ou não atribuído) ou o titular é anônimo (pessoa desconhecida).

Pensamento similar pode ser aplicado à imagem facial humana. Se uma imagem facial não estiver relacionada a uma pessoa natural ou estiver relacionada a uma pessoa natural indeterminada e indeterminável, a princípio, essa imagem não deve ser

³⁶ TEFFÉ, *op. cit.*, p. 40.

³⁷ Para fins deste exemplo, considera-se válido o número de CPF que atenda aos critérios da fórmula em Javascript disponibilizados pela Secretaria da Receita Federal do Brasil (SRFB). Isso não significa que a situação cadastral de inscrição esteja regular junto à SRFB.

³⁸ O número de CPF é único para cada pessoa natural: não é possível que a mesma pessoa tenha mais de um número de CPF, assim como não é possível que o mesmo número de CPF esteja associado a mais de uma pessoa natural. Em razão dessa natureza unívoca, o número de CPF é amplamente utilizado como atributo-chave em banco de dados para distinguir registros de pessoas naturais distintas. Na fase de teste de desenvolvimento de softwares, é comum a utilização de geradores randômicos de números válidos de CPF pelos programadores, assim, é possível que números válidos, ainda não atribuídos a qualquer pessoa natural pela SRFB, estejam sendo gerados e processados.

considerada dado pessoal, em termos de aplicação da LGPD. Uma imagem facial surpreendentemente realista de uma pessoa que não existe pode ser criada por algoritmo de inteligência artificial: segundo o *website*, o “Unreal Person” é um gerador de imagem treinado por bilhões de faces humanas com o objetivo de produzir uma face completamente nova de alguém que não existe³⁹; portanto, não se trata de dado pessoal, pois o titular não existe no mundo real. Pela outra via, se a imagem facial se relacionar a uma pessoa natural anônima, igualmente não se trata de dado pessoal, pois o titular é desconhecido.

Em contrapartida, considerando o raciocínio protetivo disciplinado pela LGPD, em que a tutela é direcionada aos direitos e liberdades da pessoa natural, e não aos seus dados em si, se excepcionalmente o tratamento da imagem facial anônima repercutir em sua esfera pessoal, haverá incidência da LGPD por via reflexa. Nesse caso, restará prejudicada ou esvaziada a discussão sobre se, nesse caso, a imagem facial anônima é um dado pessoal ou não, para fins de aplicação da LGPD, pois a afetação do interesse pessoal já é causa bastante para invocar a proteção normativa. Contudo, apesar desse esvaziamento, para se manter a coerência com o objeto de manejo da norma, nessa situação, ainda que anônima, a imagem facial será considerada um dado pessoal.

A esse respeito, um caso emblemático ocorreu em São Paulo (SP), envolvendo a então loja conceito chamada “Hering Experience”, em que o Departamento de Proteção e Defesa do Consumidor (DPDC) instaurou um processo administrativo⁴⁰ em face da Cia Hering (representada), em razão de coleta e do processamento indevido de dados pessoais de clientes por meio de recursos tecnológicos de reconhecimento facial. Sustentava a representada que a tecnologia de detecção facial (*video analytics*) empregada não poderia ser confundida com reconhecimento facial e, portanto, não haveria possibilidade de identificação do consumidor, mas somente o diagnóstico estimado de gênero, faixa etária e humor, para gestão de mídia direcionada no interior do ambiente da loja, afastando, assim, qualquer violação legal, por não se tratar de dados pessoais.

Nesse caso, além das infrações consumeristas, o IDEC também apontou violações a preceitos da LGPD, sustentando que a diferenciação entre detecção e reconhecimento facial seria mera distinção de nomenclatura, havendo efetivamente tratamento não autorizado de dados pessoais. Apesar disso, a Secretaria Nacional do Consumidor (Senacon) considerou prejudicada essa questão, uma vez que, embora publicada, à época dos fatos, a LGPD ainda não estava em vigor, e concluiu pela violação aos preceitos do Código de Defesa do Consumidor (CDC) e aos

³⁹ UNREAL PERSON. **This person does not exist**. [S. l.]: Unreal Person, 2023. Disponível em: <https://www.unrealperson.com/>. Acesso em: 27 mar. 2026.

⁴⁰ SEI nº 08012.001387/2019-11 do Ministério da Justiça e Segurança Pública.

direitos de personalidade e imagem dos consumidores, aplicando uma multa de R\$ 58.767,00 à representada.

Apesar de a controvérsia acerca da caracterização de dado pessoal ter sido relativizada para fins de decisão da Senacon nessa situação, à luz do presente estudo, talvez a argumentação da representada pudesse se enquadrar no âmbito da análise facial, e a captação e o processamento de dados faciais tratados como dados genuinamente anônimos desde a origem, e não anonimizados posteriormente. Contudo, como visto anteriormente, mesmo o anonimato não seria argumento suficiente para afastar a incidência da LGPD e, portanto, por outras vias, a violação aos direitos restaria comprovada, se a esfera pessoal dos consumidores fosse atingida.

Questão relevante que se coloca é a que trata do anonimato absoluto ou relativo do titular da informação. Se a imagem facial estiver associada a pessoa natural inicialmente indeterminada, mas determinável, ou seja, passível de identificação do titular por qualquer meio, então estar-se-á diante de um autêntico dado pessoal, o qual reclamaria a incidência da LGPD. Assim sendo, o anonimato relativo não seria suficiente para afastar a proteção disciplinada pela LGPD, mas somente o anonimato absoluto seria capaz de descaracterizar a imagem facial como dado pessoal, salvo se, excepcionalmente, o seu tratamento puder repercutir na esfera pessoal de seu titular. Entretanto, essa avaliação não pode ser conduzida apenas no campo teórico, pois, em tese, se a imagem facial se refere a uma pessoa natural que existe, ou existiu, no mundo real, então o seu titular poderá ser identificado de algum modo; portanto, se assim fosse, qualquer informação relacionada a uma pessoa natural seria considerada como um dado pessoal, pois qualquer pessoa é abstratamente passível de identificação, com maior ou menor grau de dificuldade.

Desse modo, a aferição da possibilidade ou não de identificação do titular, a partir do processamento de atributos extraídos da imagem facial, deve ser conduzida dentro do contexto em que se encontra o responsável pelo tratamento desses dados, considerando fatores como custo, tempo e tecnologia, razoavelmente disponíveis e ao seu alcance:

A análise do potencial de identificação de certa informação pelo agente de tratamento ou por outro sujeito – conforme a orientação objetiva – não pode ser feita em abstrato apenas, como se bastasse uma possibilidade puramente hipotética. No direito europeu, desde a Diretiva 95/46/CE vigora o critério dos meios suscetíveis de ser razoavelmente utilizados, que busca ser balizado por fatores objetivos como custos e tempo de trabalho exigidos para a identificação, o estado da arte da tecnologia existente no período de duração do tratamento e os riscos de falhas técnicas, por exemplo. Trata-se de critério dependente de aspectos contextuais – v. g., estágio de desenvolvimento das tecnologias de rastreamento de comportamento online e

de algoritmos de aprendizado de máquina – que, em última análise, faz da caracterização como dado pessoal um estado dinâmico.⁴¹

Essa possibilidade razoável de identificação ou não do titular deve ser aferida não apenas em relação ao agente de tratamento de dados faciais, mas também em relação a qualquer outro agente. Assim, não é imprescindível que os dados necessários para a identificação do titular estejam sob controle ou na posse do mesmo agente de tratamento, bastando que os dados efetivamente existam e possam ser processados por qualquer meio razoavelmente aceitável para que o titular seja considerado uma pessoa natural identificável, ainda que o responsável pelo tratamento de dados faciais não disponha isoladamente de todos os dados necessários à identificação.

Apesar de adotar expressamente o conceito amplo de identificação do titular do dado pessoal, ao não se restringir à pessoa natural identificada, mas também incluir a pessoa natural identificável, a LGPD, ao menos de forma expressa, não indica os critérios e as balizas que possibilitam considerar uma pessoa natural identificável. Não obstante, o princípio da razoabilidade é expressamente invocado pela Lei em inúmeras passagens, inclusive para dispor acerca de meios técnicos e esforços razoáveis, além de trazer fatores objetivos para a determinação do que seja razoável: tempo, custo e tecnologia, muito em linha com os preceitos do GDPR da União Europeia, a partir dos quais a legislação brasileira buscou inspiração. A propósito, o Considerando 26 do GDPR esclarece os critérios aplicáveis para identificação da pessoa natural, os quais podem ser adotados no país para interpretação normativa:

[...] Para determinar se uma pessoa singular é identificável, importa considerar todos os meios suscetíveis de ser razoavelmente utilizados, tais como a seleção, quer pelo responsável pelo tratamento quer por outra pessoa, para identificar direta ou indiretamente a pessoa singular. Para determinar se há uma probabilidade razoável de os meios serem utilizados para identificar a pessoa singular, importa considerar todos os fatores objetivos, como os custos e o tempo necessário para a identificação, tendo em conta a tecnologia disponível à data do tratamento dos dados e a evolução tecnológica. [...] ⁴²

Sendo assim, o agente de tratamento de dados que conduz o processamento de análise facial, e não de reconhecimento facial, apesar de não pretender coletar informações que visem à identificação do titular, não escapa do campo de incidência da LGPD, se a identificação, ainda que não pretendida, seja razoavelmente possível

⁴¹ MACHADO, Diego. Considerações iniciais sobre o conceito de dado pessoal no ordenamento jurídico brasileiro. *Civilistica*, [S. l.], v. 12 n. 1, 2023, p. 11. Disponível em: https://www.researchgate.net/publication/371577468_Consideracoes_iniciais_sobre_o_conceito_de_dado_pessoal_no_ordenamento_juridico_brasileiro. Acesso em: 27 mar. 2026.

⁴² UNIÃO EUROPEIA, *op. cit.*

por qualquer meio ou agente, nas circunstâncias concretas em que ocorre o tratamento de dados. Mesmo que a efetiva identificação se mostre inviável, no contexto do processamento de dados faciais e, portanto, em regra, não se trate de dados pessoais, nos termos da LGPD, não significa necessariamente que o tratamento desses dados seja absolutamente livre, uma vez que o regime protetivo da dignidade humana não se restringe a uma norma específica, mas conta com todo o ordenamento jurídico, interpretado sistemicamente.

6. DISCRIMINAÇÃO ALGORÍTMICA

A expressão facial humana é um poderoso veículo de comunicação não verbal e de relacionamento interpessoal. Essa capacidade reflete a própria complexidade dos agrupamentos sociais e, nesse sentido, discute-se a invariabilidade e a universalidade das expressões faciais da emoção através das culturas. Além disso, emergem novos desafios quando se analisam as pesquisas sobre a relação entre emoção e comportamento facial, que apontam principalmente para a consideração de dialetos emocionais específicos de cada cultura e para a influência dos aspectos sociais e comunicativos no comportamento facial, para além da emoção⁴³. Dessa forma, a expressão ou comportamento facial é uma aproximação da emoção humana, que pode ser modulado por reações involuntárias ou intencionais, a depender de aspectos culturais e circunstanciais em que o indivíduo está inserido.

Algumas emoções humanas podem ser mais facilmente reconhecidas por expressões ou comportamentos faciais, como a alegria e a surpresa. Entretanto, outras podem ser mais complexas, como a surpresa feliz e a surpresa triste, justamente em razão da combinação de expressões faciais comuns. Estudos sobre as expressões faciais da emoção, conduzidos por Du, Tao e Martinez⁴⁴, demonstram que as emoções podem ser classificadas em dois grupos. O primeiro se refere à categoria de emoções básicas, que inclui alegria, surpresa, raiva, tristeza, medo e aversão. Apesar de se empregar o termo “básico”, isso não significa que se tratem de emoções mais básicas do que outras, mas que se referem a categorias que não podem ser decompostas em termos semanticamente menores, além de serem prevalentes na literatura especializada. Por outro lado, o segundo grupo corresponde às emoções compostas, no sentido de que as categorias são construídas a partir da combinação de duas categorias de emoções básicas; nem todas as combinações fazem necessariamente sentido, mas,

⁴³ SOUSA, Cristina de. Emoção e expressão facial: novos desafios. **Psicologia**, Lisboa, v. 24, n. 2, p. 17-41, 2010. Disponível em: <https://revista.appsicologia.org/index.php/rpsicologia/article/view/303/65>. Acesso em: 27 mar. 2026.

⁴⁴ DU, Shichuan; TAO, Young; MARTINEZ, Aleix M. Compound facial expression of emotion. **Proceedings of the National Academy of Sciences**, Washington, v. 111, n. 15, p. E1454-E1462, 2014, p. 1454. Disponível em: <https://www.pnas.org/doi/epdf/10.1073/pnas.1322355111>. Acesso em: 27 mar. 2026.

além das seis básicas, outras 15 categorias foram identificadas como típicas e distintas entre si, totalizando 21 expressões faciais da emoção, sem contar a expressão neutra.

Considerando esses desafios, a análise facial computacional procura classificar ou associar as inúmeras expressões ou comportamentos faciais, a partir da identificação de atributos físicos capturados das imagens digitais, a emoções ou sentimentos humanos. Segundo Vemou e Horvath⁴⁵, o reconhecimento de emoções faciais opera por meio de três etapas: (i) a detecção facial; (ii) a detecção de expressões faciais; e (iii) a classificação dessas expressões em estados emocionais. A detecção de emoções é baseada na análise de pontos de referência da face humana (como ponta do nariz, sobrancelhas etc.). Além disso, em vídeos, variações desses pontos também são analisadas, com o objetivo de identificar contrações em grupos de músculos faciais e, dependendo do algoritmo, as expressões faciais podem ser classificadas em emoções básicas ou emoções compostas e, em outros casos, podem ser relacionadas a estados mentais ou psicológicos (como cansaço ou tédio). Em razão do uso de dados biométricos e de tecnologias de inteligência artificial, o reconhecimento de emoções faciais compartilha alguns dos riscos do uso de sistemas de reconhecimento facial e dessas tecnologias: apesar de a identificação do indivíduo não ser o objetivo primordial, riscos relacionados à precisão da interpretação da emoção são relevantes.

Nesse sentido, a imprecisão da interpretação da emoção pode advir de diversos fatores: se o comportamento facial é uma aproximação do estado emocional humano, então pode ocorrer a situação em que determinada expressão facial de um indivíduo não corresponda à sua emoção naquele momento, seja porque intencionalmente consegue modificar sua expressão por meio do controle de alguns músculos faciais, ou, a revés, alguma anomalia o impede de movimentá-los, ou até mesmo por questões culturais, em que expressões de sentido comum em alguns grupos sociais podem não ter o mesmo significado em outros. Também a imprecisão pode decorrer de erro na identificação de atributos físicos da face digitalizada, ou na classificação equivocada pelo algoritmo, caso em que a categoria não representa o humor do indivíduo naquele momento. Essas imprecisões não se restringem ao reconhecimento automatizado de emoções humanas, mas também podem ocorrer na categorização de gênero e faixa etária, uma vez que atributos físicos faciais podem não ser suficientes em quantidade e qualidade para prevenir desvios de generalização.

Por outro lado, não seria razoável exigir a precisão absoluta como parâmetro de aceitação ou rejeição de um sistema automatizado de análise facial, seja para o reconhecimento de emoções, seja para o reconhecimento de características demográficas, como gênero e idade. Em algumas circunstâncias, o algoritmo poderia não apresentar uma resposta adequada, mas, se esses casos forem estatisticamente

⁴⁵ VEMOU, Konstantina; HORVATH, Anna. Facial Emotion Recognition. **TechDispatch**, v. 1, p. 1-5, 2021. Disponível em: https://www.edps.europa.eu/system/files/2021-05/21-05-26_techdispatch-facial-emotion-recognition_ref_en.pdf. Acesso em: 27 mar. 2026.

desprezíveis, poder-se-ia afirmar que, dentro de determinada margem de erro aceitável ou de confiança razoável, o algoritmo de análise facial seria suficientemente preciso para a aplicação que se pretenda.

Entretanto, justamente por não objetivar a identificação do indivíduo, mas a sua classificação em grupos previamente definidos, como humor (alegria, surpresa, raiva, tristeza, medo, aversão), gênero (masculino, feminino) e faixa etária (jovem, adulto, idoso), e por estar sujeito a erros estatísticos, sistemas automatizados de análise facial estão mais intensamente sujeitos à discriminação algorítmica do que os de reconhecimento facial. Embora a identificação e a autenticação de indivíduos a partir de atributos físicos faciais mensuráveis sejam passíveis de erros estatísticos, muitas vezes decorrentes de vieses algorítmicos oriundos de bases de dados de treinamento insuficientes ou pouco representativas, o reconhecimento facial usualmente não opera com generalizações de atributos ou agregação de indivíduos em classes ou categorias.

Embora o termo viés algorítmico, em diversas circunstâncias, possa ser empregado de forma intercambiável com o termo discriminação algorítmica, não sem razão, pois o comportamento tendencioso do algoritmo pode não raramente produzir resultados discriminatórios; a distinção é relevante em razão de objetivos diferentes dos sistemas de reconhecimento facial e de análise facial, conforme apontado anteriormente. Segundo Alves e Andrade⁴⁶, o viés algorítmico decorre do comprometimento da neutralidade do sistema em razão do “treinamento incorreto do algoritmo ou por desdobramentos inesperados do aprendizado de máquina”, em que tendências refletem a “predileção humana por determinados valores, devido a fatores sociais e culturais preexistentes à programação e que circundam os projetistas”. Assim sendo, falhas dos sistemas de reconhecimento facial estariam mais associadas a vieses algorítmicos.

Por outro lado, os sistemas de análise facial não estariam expostos apenas ao comprometimento da neutralidade, mas também ao fato de, genericamente, associarem indivíduos a categorias de estados emocionais e demográficos incompatíveis com a realidade, por ignorar características e convicções individualizadas. Nesse sentido, o conceito de discriminação algorítmica proposto por Mattiuzzo e Mendes⁴⁷ parece mais adequado para retratar os riscos dos algoritmos de análise facial:

⁴⁶ ALVES, Marco Antonio Sousa; ANDRADE, Otávio Morato de. Da “caixa-preta” à “caixa de vidro”: o uso da explainable artificial intelligence (XAI) para reduzir a opacidade e enfrentar o enviesamento em modelos algorítmicos. **Direito Público**, Brasília, v. 18, n. 100, 2022, p. 355. Disponível em: <https://www.portaldeperiodicos.idp.edu.br/direitopublico/article/view/5973>. Acesso em: 27 mar. 2026.

⁴⁷ MATTIUZZO, Marcela; MENDES, Laura Schertel. Discriminação algorítmica: conceito, fundamento legal e tipologia. **Revista Direito Público**, Porto Alegre, v. 16, n. 90, p. 39-64, nov./dez. 2019, p. 51. Disponível em: <https://www.portaldeperiodicos.idp.edu.br/direitopublico/article/view/3766/Schertel%20Mendes%3B%20Mattiuzzo%2C%202019>. Acesso em: 27 mar. 2026.

Feitas essas observações, vale esclarecer que o termo “discriminação algorítmica” é utilizado, neste artigo, para englobar tanto cenários que envolvem afirmações estatisticamente inconsistentes quanto cenários em que as afirmações, embora estatisticamente lógicas, de alguma forma tomam os indivíduos que dela são objeto não de forma efetivamente individualizada, mas apenas como parte de um grupo. Isso porque, a nosso ver, uma classificação, ainda que consistente sob o ponto de vista estatístico, pode em alguns casos se mostrar injusta.

Em termos de tipologia, as autoras sugerem a sistematização em quatro tipos principais de discriminação algorítmica: (i) a discriminação por erro estatístico; (ii) a discriminação por generalização; (iii) a discriminação pelo uso de informações sensíveis; e (iv) a discriminação limitadora do exercício de direitos. Apesar de a tipologia se revelar um poderoso instrumento para a mitigação de riscos e o desenvolvimento de salvaguardas, na medida em que especifica o potencial discriminatório em cada situação, importa ressaltar que, enquanto a primeira categoria se aproxima do viés algorítmico, por se tratar basicamente de erro de projeto do algoritmo ou de base de dados tendenciosa de treinamento, as demais categorias se referem ao potencial tratamento discriminatório em razão da decisão automatizada decorrente do enquadramento do indivíduo em determinada classe ou grupo que não o representa adequadamente.

Nesse sentido, por exemplo, se um sistema de análise facial operar com precisão estatística satisfatória para determinado agrupamento social, em detrimento de outros, em razão da tendenciosidade da base de dados de treinamento, é possível que o algoritmo classifique o comportamento facial de um indivíduo como alegria ou satisfação, quando na realidade sua emoção é neutra ou de aversão e, como consequência, tome decisões inadequadas na oferta de produtos ou provimento de serviços. Seria o caso de tratamento discriminatório, uma vez que indivíduos em situações similares são tratados de modo distinto por viés algorítmico, e não por razões isonômicas.

Em outra situação exemplificativa, o algoritmo de análise facial procura classificar o indivíduo em categorias de gênero previamente estabelecidas, possivelmente masculino e feminino, a partir do processamento de atributos faciais mensuráveis, para tomar decisões automatizadas. Sabe-se que a identificação de gênero não se restringe aos aspectos fisionômicos do indivíduo, tornando-se impraticável determinar o gênero de alguém apenas observando a pessoa, sem interagir com ela, conforme Silva⁴⁸:

⁴⁸ SILVA, Heloísa Helena. Algoritmos de reconhecimento facial e as discriminações contra pessoas transexuais. *Revista InternetLab*, São Paulo, v. 2, n. 2, dez. 2021. Disponível em: <https://revista.internetlab.org.br/algoritmos-de-reconhecimento-facial-e-as-discriminacoes-contras-pessoas-transexuais/>. Acesso em: 27 mar. 2026.

O pesquisador Keyes assim definiu a problemática da questão “identificar o gênero de alguém olhando para uma pessoa e não falando com ela é como perguntar qual o sabor do cheiro do azul”, ou seja, a questão não é nem tanto o erro ou o acerto da resposta, mas sim entender que a pergunta em si não faz nenhum sentido. A conformação física é apenas um dos marcadores de gênero e não o único, e os algoritmos de reconhecimento facial, no estágio em que estão hoje, ainda não estão aptos a dar um passo além da aparência como fator determinante para indicação de gênero. A União Europeia, inclusive, já conta com um movimento que intenta o banimento do reconhecimento automatizado de gênero e de orientação sexual, visando a proteção desses dados sensíveis e da população LGBTQ+, vulnerável à discriminação sob esse aspecto.

Nesse caso, não se trata de vies algorítmico, mas da limitação do modelo binário de categorização de gênero, em que o indivíduo é classificado em desacordo com sua identificação de gênero ou com sua orientação sexual, produzindo um resultado automatizado potencialmente discriminatório. Aqui, especificamente, a situação tende a ser ainda mais grave, uma vez que a atitude discriminatória recai sobre grupos historicamente mais vulneráveis e a decisão automatizada tende a reforçar essas desigualdades.

Por fim, pode também ocorrer a situação em que não há vies algorítmico e o sistema de análise facial associa a expressão facial do indivíduo a uma determinada classe ou categoria de acordo com sua emoção ou sentimento, entretanto, contra a sua vontade. É possível admitir que há indivíduos capazes de simular ou representar comportamentos faciais que não condizem necessariamente com suas emoções, por exemplo, no caso de artistas ou atores profissionais. Por outro lado, há também reações faciais involuntárias que representam de forma fidedigna emoções ou sentimentos que, por razões de foro íntimo, o indivíduo não tenha intenção de revelar em determinadas situações. É o caso, por exemplo, da pessoa que tem a sua satisfação ou aversão revelada por sua expressão facial e capturada por um algoritmo de análise facial diante de determinada situação, mas contrária às suas convicções ideológicas e, portanto, isso pode representar uma violação à sua honra subjetiva. Trata-se, enfim, de invasão à privacidade ou à intimidade mental.

7. NEURODIREITOS

A face mais alarmante da insuficiência normativa para a “proteção jurídica da mente”, expressão cunhada por Pintarelli⁴⁹, está associada aos avanços da neurociência e da neurotecnologia, que podem ser assim compreendidas:

⁴⁹ PINTARELLI, Camila. A proteção jurídica da mente. **Revista de Direito da Saúde Comparado**, São Paulo, v. 1, n. 1, 2022, p.104. Disponível em: <https://periodicos.unisa.br/index.php/direitosaude/article/view/396/458>. Acesso em: 27 mar. 2026.

A neurociência é o campo da ciência responsável por estudar o cérebro humano e o sistema nervoso, como eles funcionam. Enquanto a neurotecnologia é um ramo da neurociência, no qual tecnologias são aplicadas ou usadas para registrar e interpretar informações da atividade cerebral. Se a neurociência tenta entender, por exemplo, as causas por trás do Parkinson, a neurotecnologia busca a aplicação de tecnologias no cérebro que ajudem a superar ou prevenir essa doença⁵⁰.

Em termos de categorização, as neurotecnologias podem ser classificadas em invasivas e não-invasivas, cujo critério principal de diferenciação é a localização dos sensores que monitoram a atividade do cérebro. Assim, dispositivos invasivos são aqueles inseridos dentro do corpo do indivíduo para interagir diretamente com os impulsos neurais. Por outro lado, os dispositivos não-invasivos buscam viabilizar a leitura de atividades neurais sem a necessidade de implantes cerebrais.⁵¹

Os riscos e as preocupações surgem com a ampliação da produção desses dados neurais, associada ao desenvolvimento de tecnologias correlatas, como a inteligência artificial, o *Big Data*, a internet das coisas, a computação em nuvem e a realidade aumentada. Não se trata apenas da proteção de dados pessoais, mas do acesso e da interferência alheia em informações que dizem respeito à mais íntima cognição humana, à autodeterminação, ao autodesenvolvimento e, portanto, trata-se da proteção da própria dignidade humana.

A lacuna normativa deverá ser preenchida, ou integrada, enquanto não houver legislação própria, mas sem deixar de reconhecer os benefícios trazidos por esses avanços tecnológicos e menos ainda impedir o seu contínuo desenvolvimento. Entretanto, a tutela jurídica, em boa medida, é necessária para proteger o homem de si mesmo:

Vimos que o intenso desenvolvimento da neurotecnologia, com a evolução das técnicas de interface conectiva entre o cérebro e a máquina, estão expandindo as fronteiras da ação humana, gerando esperança e expectativa sobre seus impactos positivos na economia e, na área da saúde, no tratamento e na cura de doenças. Embora sejam avanços que devam ser celebrados, não podemos perder de vista os limites éticos envolvidos em tais procedimentos, pois trata-se de escalada evolutiva que diz respeito à própria integridade psíquica do ser humano, no que inserimos, também,

⁵⁰ BARROSO, Eliana. Os neurodireitos diante dos avanços da neurociência e da neurotecnologia. **Jusbrasil**, 13 mar. 2023. Disponível em: <https://www.jusbrasil.com.br/artigos/os-neurodireitos-diante-dos-avancos-da-neurociencia-e-da-neurotecnologia/1778772576>. Acesso em: 1 mar. 2024.

⁵¹ POSSA, Alisson Alexsandro. **A concretização da dignidade humana na era das neurotecnologias: o direito à liberdade cognitiva como neurodireito na ordem constitucional brasileira**. 2022. Dissertação (Mestrado Acadêmico em Direito) – Instituto Brasileiro de Ensino, Desenvolvimento e Pesquisa, Brasília, 2022, p.15-16. Disponível em: <https://repositorio.idp.edu.br/handle/123456789/4688>. Acesso em: 27 mar. 2026.

as preocupações relativas à sedimentação dos processos automatizados de tomada de decisão via interação algorítmica, que também impactam a mente humana e demandam tutela jurídica específica.⁵²

Nesse contexto, no âmbito das iniciativas de proteção de neurodireitos, discute-se quais seriam esses direitos e, ainda, se, de fato, se tratariam de novos direitos não abarcados pela ordem jurídica estabelecida. Não se pretende aqui explorar essa discussão, uma vez que, embora relevante, escapa do objetivo desta investigação. Contudo, vale mencionar que o direito à privacidade mental tem sido invariavelmente considerado nas diversas propostas legislativas de neurodireitos, os quais, em linhas gerais, podem ser entendidos como o direito à proteção da segurança e da privacidade de dados neurais obtidos por neurotecnologias e, eventualmente, potencializados quando associados a tecnologias de inteligência artificial⁵³.

Exemplo concreto dessa produção legislativa é a aprovação da emenda constitucional (Reforma Constitucional nº 21.383) que introduziu formalmente a neuroproteção no âmbito do direito à vida e à integridade física e psíquica da pessoa, na Constituição do Chile⁵⁴. Outro é a EC nº 85/2023, que alterou o parágrafo único do art. 235 da Constituição Estadual do Rio Grande do Sul⁵⁵, para incorporar a integridade mental do ser humano como pressuposto da política e da pesquisa científica e tecnológica no Estado.

Ainda em termos de atividade legislativa brasileira, a PEC 29/2023, em tramitação no Senado Federal, pode ser considerada um marco ao propor a alteração da Constituição Federal para incluir, entre os direitos e garantias fundamentais, a proteção à integridade mental e à transparência algorítmica⁵⁶. Outras iniciativas estão em curso no parlamento brasileiro, como o PL 522/2022, que busca modificar a LGPD para conceituar dado neural e regulamentar a sua proteção⁵⁷;

⁵² PINTARELLI, *op. cit.*, p. 117-118.

⁵³ LOPES, Ana Maria D'Ávila. Neurotecnologia: quando a tecnologia ameaça a dignidade humana. In: LOPES, Ana Maria D'Ávila *et al.* (org.). **Neurodireito, neurotecnologia e direitos humanos**. Porto Alegre: Livraria do Advogado, 2022, p. 21. Disponível em: https://www.researchgate.net/publication/368128401_Neurodireito_Neurotecnologia_e_Direitos_Humanos. Acesso em: 27 mar. 2026.

⁵⁴ CHILE. **Constitución Política de La República de Chile**. Santiago: Cámara de Diputadas y Diputados, 1980. Disponível em: https://www.camara.cl/camara/doc/leyes_normas/constitucion.pdf. Acesso em: 27 mar. 2026.

⁵⁵ RIO GRANDE DO SUL. **Constituição do Estado do Rio Grande do Sul**. Porto Alegre: Assembleia Legislativa do Estado do Rio Grande do Sul, 1989. Disponível em: <https://ww2.al.rs.gov.br/dal/LinkClick.aspx?fileticket=AixRs5bbgtw%3d&tabid=3683&mid=5359>. Acesso em: 27 mar. 2026.

⁵⁶ BRASIL. **Proposta de Emenda à Constituição nº 29, de 2023**. Brasília, DF: Senado Federal, 2023b. Disponível em: https://legis.senado.leg.br/sdleg-getter/documento?dm=9386685&ts=1733680966436&rendition_principal=S&disposition=inline. Acesso em: 27 mar. 2026.

⁵⁷ BRASIL. **Projeto de Lei nº 522, de 2022**. Brasília, DF: Câmara dos Deputados, 2022. Disponível em: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codeor=2146384&filename=PL%20522/2022. Acesso em: 27 mar. 2026.

o PL 2174/2023, que propõe lei específica para estabelecer normas e princípios para a proteção dos direitos fundamentais relacionados ao cérebro e ao sistema nervoso humano, objetivando garantir a proteção e a promoção de neurodireitos dos indivíduos⁵⁸; e o PL 4/2025, que pretende atualizar o Código Civil, inclusive dispondo de capítulo dedicado à pessoa no ambiente digital, abordando neurodireitos como parte indissociável da personalidade⁵⁹.

Feita essa breve contextualização, embora os sistemas de análise facial ou de reconhecimento de emoções faciais não sejam propriamente classificados como neurotecnologias, não há como negar que são capazes de registrar e interpretar informações da atividade cerebral por meio de uma interface homem-máquina não intrusiva: a imagem da face humana. Essa interface remota de captação da atividade mental tem potencial de disseminação similar ao do reconhecimento facial sobre tecnologias concorrentes, como o reconhecimento de íris e o de impressão digital para identificação ou autenticação pessoal.

Nesse sentido, é possível identificar inúmeras situações em que o comportamento facial pode significar, com acurácia, a atividade mental, muitas vezes de forma involuntária, e que se refere exclusivamente à privacidade mental do indivíduo, o qual não cogita que seja livremente revelada a terceiros, por se tratar de matéria do foro íntimo, ou por divergir de sua imagem perante a sociedade, ou por qualquer outra razão individual. Por exemplo, em uma entrevista de emprego, o candidato pode ser exposto intencionalmente a uma situação de segregação racial e, a pretexto de gravar em vídeo a dinâmica da reunião, o algoritmo de reconhecimento de emoções faciais pode captar, registrar e revelar suas convicções mais íntimas, ainda que contrárias à sua postura social e afirmações conscientes. Nesse caso, não parece razoável que a devassa mental seja mais relevante que a sua conduta para qualquer decisão que lhe diga respeito.

Em outra situação hipotética, poderia o algoritmo de reconhecimento de emoções faciais captar, registrar e revelar a satisfação mental de determinada auto-ridade religiosa, ainda que em lapso insignificante de tempo, diante de uma cena acidental de nudez infantil, ou de repulsa ou de aversão ao presenciar idosos desamparados em condições degradantes. Pode ocorrer ainda a revelação da orientação ou da preferência sexual do indivíduo, a partir da interpretação da reação facial involuntária, que sequer tenha consciência plena dessa condição ou, mesmo a tendo, cuja revelação seja contrária à sua vontade. Vale ressaltar que, em todas as situações

⁵⁸ BRASIL. **Projeto de Lei nº 2174, de 2023**. Brasília, DF: Câmara dos Deputados, 2023a. Disponível em: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=2264479&filename=PL%202174/2023. Acesso em: 27 mar. 2026.

⁵⁹ BRASIL. **Projeto de Lei nº 4, de 2025**. Brasília, DF: Senado Federal, 2025. Disponível em: https://legis.senado.leg.br/sdleg-getter/documento?dm=9889374&ts=1770318618932&rendition_principal=S&disposition=inline. Acesso em: 27 mar. 2026.

exemplificadas, considera-se revelação o mero acesso não autorizado a informação mental, sendo irrelevante a inexistência de divulgação ou propagação.

Dessa forma, percebe-se que a discussão acerca do tratamento de dados por sistemas de análise facial ou reconhecimento de emoções faciais não se restringe ao âmbito da proteção de dados pessoais, mas alcança o direito à proteção da privacidade mental, não apenas no sentido de impedir o uso indevido de informações representativas da atividade neural, obtidas por sensores implantados dentro ou fora do corpo humano, mas também e, principalmente, no que se refere à intimidade mental. Portanto, parece fazer mais sentido que o debate e a produção legislativa a respeito de neurodireitos sejam desvinculados ou ao menos expandidos para além da neurociência e das neurotecnologias, a fim de propiciar a efetiva tutela da integridade mental, impedindo ameaça ou lesão a direitos e liberdades fundamentais, independentemente da técnica ou dos recursos tecnológicos empregados.

8. CONCLUSÃO

A LGPD refere-se à titularidade da pessoa natural quanto aos dados pessoais que lhe dizem respeito, e não à do agente de tratamento desses dados, ainda que o tratamento seja realizado de acordo com a anuência daquele. Nesse sentido, a titularidade não se transfere, mas apenas a possibilidade temporária de tratamento de dados pessoais, com o objetivo de assegurar ao titular o controle de seus dados.

Esse controle se mostra cada vez mais relevante à medida em que os dados pessoais mais intensamente representam o seu titular e expressam a sua personalidade, muitas vezes para além do que se deseja ou de que se tenha consciência, diante de fenômenos como a datificação e de teorias como a do corpo eletrônico. Assim sendo, a LGPD não visa à proteção de dados pessoais em si, mas os utiliza como via ou instrumento de proteção de seu titular, uma vez que o manejo desses dados afeta direitos da personalidade e alcança a dignidade da pessoa humana.

Por esse raciocínio, a LGPD não inova no campo dos direitos e liberdades fundamentais, mas procura materializar ou dar concretude a fundamentos já lançados constitucionalmente e utiliza meios e instrumentos para atingir esse intento. Um deles é a tipologia ou a classificação de dados em: pessoais, pessoais sensíveis e impessoais; trata-se de tentativa, ainda que sujeita a falhas, de estabelecer balizas ou parâmetros objetivos para viabilizar a aplicação da norma em situações concretas, a fim de tutelar direitos assegurados em abstrato.

No bojo dessa tentativa, surge o argumento de que os sistemas automatizados de análise facial e de reconhecimento de emoções faciais operam em aparente lacuna ou à margem das balizas estabelecidas. Enquanto os algoritmos de reconhecimento facial utilizam atributos da face humana para identificar ou autenticar o seu titular, aqueles sistemas extraem atributos faciais para categorizar o seu titular em classes ou grupos representativos de gênero, faixa etária e humor, em que a

identificação individual, além de não ser um propósito, não seria viável a partir dos atributos coletados. Assim, em interpretação restritiva da LGPD, a impossibilidade de identificação do indivíduo seria argumento suficiente para descaracterizar o atributo facial como dado pessoal ou dado pessoal sensível, uma vez que se trataria de pessoa natural indeterminada e indeterminável, por qualquer meio e agente razoavelmente considerados.

Além disso, a captura não autorizada da face do indivíduo, para fins de análise facial e de reconhecimento de emoções faciais, não representaria necessariamente uma violação ao direito de imagem, porque a *presumptio hominis* de que a captação se destina à posterior divulgação ou à reprodução não se confirmaria nesse caso, esvaziando a lógica civilista. E mais, a impossibilidade de identificação individual tornaria inviável o exercício do direito de imagem e afastaria a necessidade de anuência individualizada, uma vez que eventual oposição pontual cederia ao interesse coletivo, se assim demonstrado pelo uso dessas tecnologias.

No entanto, isso não significa que o tratamento de dados pessoais anônimos seja livremente permitido por algoritmos de análise facial e de reconhecimento de emoções faciais. Ao revés, justamente por operar com a generalização de atributos faciais ou agregação de indivíduos em classes ou categorias, essas tecnologias estão mais intensamente sujeitas à discriminação algorítmica do que as de reconhecimento facial e, portanto, merecem atenção. A propósito, o reconhecimento da existência de uma classe especial de dados pessoais, os dados pessoais sensíveis, insere-se na tentativa de desenvolver salvaguardas antidiscriminatórias aplicáveis ao tratamento dessa espécie de dados pessoais. Desse modo, a desclassificação do dado, como burla instrumental, não pode ser motivo suficiente e legítimo para afastar o objetivo pretendido pela norma.

Também nessa linha de pensamento, o argumento de que os atributos faciais anônimos tratados por sistemas de análise facial e de reconhecimento de emoções faciais não seriam dados pessoais, com o intuito de afastar a incidência da LGPD, não deve prosperar, sem que se considere a repercussão desse tratamento na esfera pessoal de alguém. Nesse sentido, a informação relacionada a uma pessoa natural identificada ou identificável goza de presunção absoluta de afetação da esfera pessoal, portanto, trata-se de dado pessoal por definição e insere-se no campo de incidência da norma. Por outro lado, no caso de informação relacionada a uma pessoa natural anônima, a presunção de afetação da esfera pessoal é relativa, pois, somente diante do caso concreto, será possível aferir se há lesão ou ameaça a direitos e liberdades fundamentais; contudo, se confirmada, o tratamento de atributos faciais anônimos será disciplinado pela LGPD e esses dados anônimos serão considerados pessoais.

Ademais disso, ainda que não se possam classificar como neurotecnologias, os sistemas de análise facial e de reconhecimento de emoções faciais podem captar e registrar remotamente, mesmo que limitadamente, atividades neurais que são expressas nos comportamentos faciais, com a vantagem, ou não, de dispensar o uso

de sensores invasivos ou não-invasivos. Mesmo que anônimos, o tratamento desses dados alcança o direito à proteção da intimidade mental, atingindo outro campo da tutela jurídica, situação em que o anonimato não parece ser o critério mais seguro para dispensar a aplicação da norma.

Em suma, a LGPD desenvolveu um arcabouço normativo para regular o tratamento de dados pessoais, como meio para atingir o objetivo de proteger direitos e liberdades fundamentais de seus titulares. Ainda que se possa legitimamente discutir o enquadramento legal do tratamento de dados dispensado pelos sistemas de análise facial e de reconhecimento de emoções faciais, não se poderá renunciar àquele objetivo, apenas pela desclassificação do dado, que também conta com a tutela de todo o ordenamento jurídico, e não apenas de uma norma, que deve ser interpretada sistemicamente.

REFERÊNCIAS BIBLIOGRÁFICAS

AFFONSO, Filipe José Medon. O direito à imagem na era das deep fakes. **Revista Brasileira de Direito Civil**, Rio de Janeiro, v. 27, n. 1, p. 251-277, 2021. Disponível em: <https://rbdcivil.ibdcivil.org.br/rbdc/article/view/438>. Acesso em: 27 mar. 2026.

ALVES, Marco Antonio Sousa; ANDRADE, Otávio Morato de. Da “caixa-preta” à “caixa de vidro”: o uso da explainable artificial intelligence (XAI) para reduzir a opacidade e enfrentar o enviesamento em modelos algorítmicos. **Direito Público**, Brasília, v. 18, n. 100, 2022. Disponível em: <https://www.portaldeperiodicos.idp.edu.br/direitopublico/article/view/5973>. Acesso em: 27 mar. 2026.

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD). **Agenda Regulatória para o Biênio 2025-2026**. Brasília, DF: ANPD, 2024a. Disponível em: https://www.gov.br/anpd/pt-br/assuntos/processo_regulatorio/agenda-regulatoria-1. Acesso em: 27 mar. 2026.

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD). **Radar Tecnológico nº 2 – Biometria e Reconhecimento Facial**. Brasília, DF: ANPD, 2024b. Disponível em: <https://www.gov.br/anpd/pt-br/centrais-de-conteudo/documentos-tecnicos-orientativos/>. Acesso em: 27 mar. 2026.

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD). **ANPD abre Tomada de Subsídios sobre Tratamento de Dados Biométricos**. Brasília, DF: ANPD, 2025a. Disponível em: <https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-abre-tomada-de-subsidios-sobre-tratamento-de-dados-biometricos>. Acesso em: 27 mar. 2026.

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD). **ANPD fiscaliza uso de sistema de reconhecimento facial na venda de ingressos e na entrada de estádios por 23 clubes de futebol**. Brasília, DF: ANPD, 2025b. Disponível em: <https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-fiscaliza-uso-de-sistema-de-reconhecimento-facial-na-venda-de-ingressos-e-na-entrada-de-estadios-por-23-clubes-de-futebol>. Acesso em: 27 mar 2026.

BARROSO, Eliana. Os neurodireitos diante dos avanços da neurociência e da neurotecnologia. **Jusbrasil**, 13 mar. 2023. Disponível em: <https://www.jusbrasil.com.br/artigos/os-neurodireitos-diante-dos-avancos-da-neurociencia-e-da-neurotecnologia/1778772576>. Acesso em: 1 mar. 2024.

BASTOS, Elísio Augusto Velloso; ESTEVES, Vitória Barros. Tecnologias de reconhecimento facial: um estudo a partir do contexto de vigilância digital e sutil. **Revista Direitos Democráticos & Estado Moderno**, São Paulo, n. 3, p. 216-240, jul./dez. 2021. Disponível em: <https://revistas.pucsp.br/index.php/DDEM/article/view/53875/38321>. Acesso em: 27 mar. 2026.

BIONI, Bruno Ricardo. **Proteção de dados pessoais: a função e os limites do consentimento**. São Paulo: Grupo GEN, 2021.

BRASIL. **Constituição da República Federativa do Brasil de 1988**. Brasília, DF: Presidência da República, 1988. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicaocompilado.htm. Acesso em: 27 mar. 2026.

BRASIL. **Decreto nº 10.046, de 9 de outubro de 2019**. Dispõe sobre a governança no compartilhamento de dados no âmbito. Brasília, DF: Presidência da República, 2019. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/decreto/D10046.htm. Acesso em: 27 mar. 2026.

BRASIL. Decreto Legislativo nº 196, de 2003. Aprova o texto da Convenção sobre o Cibercrime, celebrada em Budapeste, em 23 de novembro de 2001. **Diário Oficial da União**, Brasília, DF, 2003.

BRASIL. **Lei nº 10.406, de 10 de janeiro de 2002**. Institui o Código Civil. Brasília, DF: Presidência da República, 2002. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/2002/110406compilada.htm. Acesso em: 27 mar. 2026.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República, 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709compilado.htm. Acesso em: 27 mar. 2026.

BRASIL. **Projeto de Lei nº 522, de 2022**. Brasília, DF: Câmara dos Deputados, 2022. Disponível em: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=2146384&filename=PL%20522/2022. Acesso em: 27 mar. 2026.

BRASIL. **Projeto de Lei nº 2174, de 2023**. Brasília, DF: Câmara dos Deputados, 2023a. Disponível em: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=2264479&filename=PL%202174/2023. Acesso em: 27 mar. 2026.

BRASIL. **Projeto de Lei nº 4, de 2025**. Brasília, DF: Senado Federal, 2025. Disponível em: https://legis.senado.leg.br/sdleg-getter/documento?dm=9889374&ts=1770318618932&rendition_principal=5&disposition=inline. Acesso em: 27 mar. 2026.

BRASIL. **Proposta de Emenda à Constituição nº 29, de 2023**. Brasília, DF: Senado Federal, 2023b. Disponível em: https://legis.senado.leg.br/sdleg-getter/documento?dm=9386685&ts=1733680966436&rendition_principal=S&disposition=inline. Acesso em: 27 mar. 2026.

BRASIL. Superior Tribunal de Justiça. **Súmula nº 403**. DJe 24 nov. 2009. Disponível em: https://www.stj.jus.br/docs_internet/revista/eletronica/stj-revista-sumulas-2014_38_capSumula403.pdf. Acesso em: 27 mar. 2026.

CHILE. **Constitución Política de La República de Chile**. Santiago: Cámara de Diputadas y Diputados, 1980. Disponível em: https://www.camara.cl/camara/doc/leyes_normas/constitucion.pdf. Acesso em: 27 mar. 2026.

DINIZ, Maria H. **Curso de Direito Civil Brasileiro: teoria geral do direito civil**. São Paulo, SP: Saraiva, 2023.

DU, Shichuan; TAO, Young; MARTINEZ, Aleix M. Compound facial expression of emotion. **Proceedings of the National Academy of Sciences**, Washington, v. 111, n. 15, p. E1454-E1462, 2014. Disponível em: <https://www.pnas.org/doi/epdf/10.1073/pnas.1322355111>. Acesso em: 27 mar. 2026.

EUROPEAN COMMISSION. ARTICLE 29 DATA PROTECTION WORKING PARTY. **Opinion 2/2012 on the concept of personal data**. Bruxelas, 2012. Disponível em: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/index_en.htm. Acesso em: 27 mar. 2026.

LI, Sant Z.; JAIN, Anil K. **Handbook of face recognition**. New York: Springer, 2005.

LOPES, Ana Maria D'Ávila. Neurotecnologia: quando a tecnologia ameaça a dignidade humana. In: LOPES, Ana Maria D'Ávila *et al.* (org.). **Neurodireito, neurotecnologia e direitos humanos**. Porto Alegre: Livraria do Advogado, 2022. Disponível em: https://www.researchgate.net/publication/368128401_Neurodireito_Neurotecnologia_e_Direitos_Humanos. Acesso em: 27 mar. 2026.

LOUREIRO, Henrique Vergueiro. **Direito à imagem**. 2005. Dissertação (Mestrado em Direito) – Pontifícia Universidade Católica de São Paulo, São Paulo, 2005. Disponível em: <https://repositorio.pucsp.br/jspui/handle/handle/5983>. Acesso em: 27 mar. 2026.

MACHADO, Diego. Considerações iniciais sobre o conceito de dado pessoal no ordenamento jurídico brasileiro. **Civilistica**, [S. l.], v. 12 n. 1, 2023. Disponível em: https://www.researchgate.net/publication/371577468_Consideracoes_iniciais_sobre_o_conceito_de_dado_pessoal_no_ordenamento_juridico_brasileiro. Acesso em: 27 mar. 2026.

MATTIUZZO, Marcela; MENDES, Laura Schertel. Discriminação algorítmica: conceito, fundamento legal e tipologia. **Revista Direito Público**, Porto Alegre, v. 16, n. 90, p. 39-64, nov./dez. 2019. Disponível em: <https://www.portaldeperiodicos.idp.edu.br/direito-publico/article/view/3766/Schertel%20Mendes%3B%20Mattiuzzo%2C%202019>. Acesso em: 27 mar. 2026.

PINTARELLI, Camila. A proteção jurídica da mente. **Revista de Direito da Saúde Comparado**, São Paulo, v. 1, n. 1, 2022. Disponível em: <https://periodicos.unisa.br/index.php/direitosaude/article/view/396/458>. Acesso em: 27 mar. 2026.

POSSA, Alisson Alexandro. **A concretização da dignidade humana na era das neurotecnologias**: o direito à liberdade cognitiva como neurodireito na ordem constitucional brasileira. 2022. Dissertação (Mestrado Acadêmico em Direito) – Instituto Brasileiro de Ensino, Desenvolvimento e Pesquisa, Brasília, 2022. Disponível em: <https://repositorio.idp.edu.br/handle/123456789/4688>. Acesso em: 27 mar. 2026.

RIO GRANDE DO SUL. **Constituição do Estado do Rio Grande do Sul**. Porto Alegre: Assembleia Legislativa do Estado do Rio Grande do Sul, 1989. Disponível em: <https://ww2.al.rs.gov.br/dal/LinkClick.aspx?fileticket=AixRs5bbgtw%3d&tabid=3683&mid=5359>. Acesso em: 27 mar. 2026.

RODOTÀ, Stefano. A antropologia do homo dignus. Tradução de Maria Celina Bodin de Moraes. **Civilistica.com**, Rio de Janeiro, v. 6, n. 2, 2017. Disponível em: <https://www.jur.puc-rio.br/wp-content/uploads/2021/08/STEFANO-RODOTA-A-antropologia-do-homo-dignus.pdf>. Acesso em: 27 mar. 2026.

SILVA, Heloísa Helena. Algoritmos de reconhecimento facial e as discriminações contra pessoas transexuais. **Revista InternetLab**, São Paulo, v. 2, n. 2, dez. 2021. Disponível em: <https://revista.internetlab.org.br/algoritmos-de-reconhecimento-facial-e-as-discriminacoes-contr-pessoas-transexuais/>. Acesso em: 27 mar. 2026.

SIQUEIRA, Dirceu Pereira; VIEIRA, Ana Elisa Silva Fernandes. Os limites à reconstrução digital da imagem na sociedade tecnológica. **Revista Eletrônica do Curso de Direito da UFSM**, Santa Maria, v. 17, n. 3, e67299, 2022. Disponível em: <https://periodicos.ufsm.br/revistadireito/article/view/67299>. Acesso em: 27 mar. 2026.

SOUSA, Cristina de. Emoção e expressão facial: novos desafios. **Psicologia**, Lisboa, v. 24, n. 2, p. 17-41, 2010. Disponível em: <https://revista.appsicologia.org/index.php/rpsicologia/article/view/303/65>. Acesso em: 27 mar. 2026.

TEFFÉ, Chiara Spadaccini de. **Dados pessoais sensíveis**: qualificação, tratamento e boas práticas. Indaiatuba, SP: Editora Foco, 2022.

THALES. **Facial recognition**: top 7 trends (tech, vendors, use cases). 2021. Disponível em: <https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/biometrics/facial-recognition>. Acesso em: 27 mar. 2026.

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**, 4 maio 2016. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32016R0679>. Acesso em: 27 mar. 2026.

UNREAL PERSON. **This person does not exist**. [S. l.]: Unreal Person, 2023. Disponível em: <https://www.unrealperson.com/>. Acesso em: 27 mar. 2026.

VEMOU, Konstantina; HORVATH, Anna. Facial Emotion Recognition. **TechDispatch**, v. 1, p. 1-5, 2021. Disponível em: https://www.edps.europa.eu/system/files/2021-05/21-05-26_techdispatch-facial-emotion-recognition_ref_en.pdf. Acesso em: 27 mar. 2026.

WENDEHORST, Christiane; DULLER, Yannic. **Biometric Recognition and behavioural detection**. Policy Department for Citizens' Rights and Constitutional Affairs, PE 696.968 , Aug. 2021. Disponível em: [https://www.europarl.europa.eu/RegData/etudes/STUD/2021/696968/IPOL_STU\(2021\)696968_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2021/696968/IPOL_STU(2021)696968_EN.pdf). Acesso em: 27 mar. 2026.

ZUK, Ofir. **The State of Facial Recognition Today**. **Datagen.tech**, 2024. Disponível em: <https://datagen.tech/blog/the-state-of-facial-recognition-today/>. Acesso em: 12 fev. 2024.

Submetido em: 01/12/2024

Aprovado em: 26/09/2025